

Wissenschaftlicher Endbericht

RKD – Lösung für die Erzeugung und Verteilung von kryptografischen Schlüsseln auf Basis von Funkkanaleigenschaften

Dipl.-Ing. Dr. Ernst Piller

Jakob Heigl-Auer, BSc

insitu software gmbh, Heinrich Schneidmadlstr. 15, 3100 St. Pölten

St. Pölten, August 2025



 **Bundesministerium
Finanzen**



Das Projekt wurde im Rahmen des Sicherheitsforschungs-Förderprogramms KIRAS vom Bundesministerium für Finanzen finanziert

Literaturverzeichnis

| | | |
|----------|--|-----------|
| 1 | KURZFASSUNG | 4 |
| 2 | AUSGANGSLAGE | 6 |
| 2.1 | TERESTRISCHER BEREICH..... | 6 |
| 2.1.1 | <i>Physikalische Grundlagen der Zufälligkeit</i> | 7 |
| 2.1.2 | <i>Dynamikanforderungen</i> | 8 |
| 2.1.3 | <i>Wirtschaftliche und technische Vorteile</i> | 8 |
| 2.1.4 | <i>Systemlimitationen</i> | 9 |
| 2.1.5 | <i>Anwendungsdomänen und Einsatzgebiete</i> | 9 |
| 2.1.6 | <i>Sicherheitsbetrachtung</i> | 9 |
| 2.1.7 | <i>Marktreife</i> | 10 |
| 2.1.8 | <i>Distanz</i> | 11 |
| 2.1.9 | <i>Kosten</i> | 12 |
| 2.2 | LITERATURANALYSE..... | 12 |
| 2.2.1 | <i>Die vier Grundphasen der Schlüsselgenerierung</i> | 13 |
| 2.2.2 | <i>Phase 1: Kanalerkundung</i> | 13 |
| 2.2.3 | <i>Phase 2: Schlüsselbit-Extraktion</i> | 14 |
| 2.2.4 | <i>Phase 3 & 4: Fehlerkorrektur und Privatsphärenverstärkung</i> | 14 |
| 2.2.5 | <i>Bewertung der Schlüsselqualität</i> | 14 |
| 2.2.6 | <i>Schutz vor Angriffen</i> | 15 |
| 2.2.7 | <i>Fortgeschrittene Schlüsselvereinbarungsverfahren</i> | 15 |
| 2.2.8 | <i>Moderne Kommunikationstechnologien</i> | 16 |
| 2.2.9 | <i>Vollduplex-Transceiver</i> | 16 |
| 2.2.10 | <i>Praktische Anwendungen</i> | 16 |
| 2.3 | LITERATURVERZEICHNIS | 17 |
| 3 | PROJEKTIINHALT | 22 |
| 3.1 | SDR / SATELLITENKOMMUNIKATION | 22 |
| 3.2 | ENTWICKLUNGSPROJEKT FÜR ALGORITHMIK | 22 |
| 3.2.1 | <i>Messung Fehlerkorrektur</i> | 25 |
| 3.2.2 | <i>Normalisierung</i> | 25 |
| 3.2.3 | <i>Grid Quantisierung + Loess</i> | 25 |
| 3.2.4 | <i>Discrete Cosine Transformation</i> | 27 |
| 3.2.5 | <i>Cascade Error Correction</i> | 27 |
| 3.2.6 | <i>Secure Sketch</i> | 28 |
| 3.2.7 | <i>Privacy Amplification</i> | 28 |
| 3.3 | LORA MODUL ENTWICKLUNG | 29 |
| 3.4 | MESSDATENERHEBUNG | 31 |

| | | |
|----------|---|-----------|
| 3.5 | EVALUIERUNG DER MESSDATEN UND VERFAHREN | 32 |
| 3.6 | BITS PRO MESSPUNKT, AUFLÖSUNG..... | 32 |
| 3.6.1 | <i>Cascade Error Korrektion</i> | 33 |
| 3.6.2 | <i>Schlüsselgenerierungsmethode</i> | 34 |
| 3.6.3 | <i>Analyse Angreifer (Eve)</i> | 35 |
| 3.6.4 | <i>Konsumentenprojekte</i> | 36 |
| 4 | ERGEBNISSE | 37 |
| 4.1 | DOCKERBASIEREND | 37 |
| 4.2 | DATENFLUSS UND VERARBEITUNGSPipeline | 37 |
| 5 | SCHLUSSFOLGERUNGEN UND AUSBLICK | 38 |
| | ABBILDUNGSVERZEICHNIS | 39 |
| 6 | LITERATURVERZEICHNIS | 40 |
| | ABKÜRZUNGEN | 43 |

1 Kurzfassung

Motivation

RKD (Radio-signal key generation) wird in der Literatur unter verschiedenen Bezeichnungen geführt, wie z.B. Physical Layer Key Generation (PLKG), und stellt ein etabliertes Forschungsgebiet dar. Trotz umfangreicher wissenschaftlicher Literatur konnte jedoch kein kommerzielles Produkt identifiziert werden, das RKD-Technologien zur Erzeugung und Verteilung kryptografischer Schlüssel für Endverbraucher einsetzt. Dieser Umstand sollte mit der Entwicklung eines vollständigen RKD-Gerätes geändert werden.

Ausgangssituation/Status Quo

Die systematische Analyse des Forschungsstandes offenbart eine erhebliche Implementierungslücke zwischen theoretischen Erkenntnissen und praktischer Umsetzung. Dem RKD-Forschungsfeld mangelt es an praxistauglichen, marktfähigen Lösungen.

Projekt-Inhalte und Zielsetzungen

Das primäre Projektziel bestand in der Entwicklung eines vollständig implementierten RKD-Geräts. Dieses soll in doppelter Ausführung mit genügend Dynamik durch Bewegung des Geräts sichere symmetrische Schlüssel erzeugen und zwischen den beiden Kommunikationspartnern austauschen. Diese kryptografischen Schlüssel können dann zur Datenverschlüsselung, aber auch für andere kryptografische Funktionen wie MAC-Berechnung, genutzt werden.

Methodische Vorgehensweise

Nach einer umfassenden Literaturstudie zur Evaluation aktueller Methodiken und Identifikation bestehender Limitationen wurden zwei teilweise unabhängige Entwicklungsprojekte unter der jeweiligen Leitung von Herrn Dipl.-Ing. Dr. Henri Ruotsalainen und Herrn Jakob Heigl-Auer, BSc., gestartet. Diese parallele Entwicklungsstrategie ermöglichte die Evaluation unterschiedlicher Ansätze sowie einer leichteren Entscheidungsfindung zur Identifikation optimaler Systemkomponenten hinsichtlich Effizienz, Sicherheit, Kosten und Benutzerfreundlichkeit.

Ergebnisse und Schlussfolgerungen

Die Entwicklungsarbeit resultierte in funktionsfähigen Geräten, die als Gerätepaar die Erzeugung und Verteilung identischer kryptographischer Schlüssel in einem Radius von maximal einigen Kilometern ermöglichen. Nach der räumlichen Bewegung und der Aufzeichnung der jeweiligen Signalstärke werden die Geräte an Computern angeschlossen. Eine eigene Software führt dann die Schlüsselgenerierung und Fehlerkorrektur über eine herkömmliche Internetverbindung durch. Beide Parteien erhalten identische, kryptographisch hochsichere Schlüssel.

Ausblick

Die entwickelten Lösungen demonstrieren das Potenzial für die praktische Anwendung von RKD-Geräten in realen Kommunikationsszenarien und bilden die Grundlage für eine kommerzielle Nutzung.

2 Ausgangslage

Die Entwicklung sicherer Kommunikationsverfahren stellt in der heutigen digitalisierten Welt eine zentrale Herausforderung dar. QKD (Quantum Key Distribution) gilt zwar als eine hochsichere Lösung für die Erzeugung und Verteilung kryptografischer Schlüssel, jedoch stehen ihrer praktischen Implementierung erhebliche wirtschaftliche Hürden entgegen. Die benötigte hochspezialisierte Hardware macht QKD äußerst kostspielig. Eine weitere Lösung für die hochsichere Erzeugung und Verteilung kryptografischer Schlüssel stellt MKD (Memory Key Distribution) dar. Ein technologie-neutraler Vergleich von RKD, QKD und MKD findet sich in der KIRAS-Studie „Kryptovergleich“ und im Buch „Data Encryption at the Intersection of Mathematics and Physics – Comparing Physical Methods of Cryptography“, das Ende 2025 im Verlag Springer-Nature“ erscheinen wird.

Zu Beginn der Forschungsarbeit war die Grundüberlegung, eine kostengünstige und dennoch sichere Alternative zu QKD zu entwickeln, das sowohl über kurze Entfernungen (terrestrischer Bereich), als auch über große Entfernungen mit Einbindung von Satelliten einsetzbar ist.

Da eine genauere Analyse ergab, dass der vorgesehene Zeitrahmen nicht für eine zufriedenstellende Umsetzung ausgereicht hätte, wurde der satellitenbasierte Projektteil nach Rücksprache mit der FFG gestoppt und der terrestrische Bereich ausgebaut. Diese Neuausrichtung erwies sich als gute Entscheidung für die weitere Entwicklung des Projekts. Dadurch konnte im terrestrischen Bereich eine umfangreichere Evaluation der Lösungsmöglichkeiten in den verschiedenen Systemphasen (siehe unten) und zwei verschiedene Lösungen vollständig implementiert und umfangreich getestet werden.

2.1 Terrestrischer Bereich

Funktionsweise der Erzeugung und Verteilung kryptografischer Schlüssel

Bei RKD senden zwei Kommunikationsgeräte (Alice und Bob) halbwegs gleichzeitig Funksignale mit Frequenzen über 30 MHz in beide Richtungen und messen dabei kontinuierlich die empfangenen Signaleigenschaften. Typischerweise werden die Signalstärke (RSSI - Received Signal Strength Indicator), der Phasenwinkel oder die Laufzeit der Signale erfasst. Nachdem beim Direktfunk (Freistrahkanäle) meist die Signalstärke gemessen wird, bezieht sich der nachfolgende Text auf die Signalstärke. Ausgenommen davon ist die Anwendung mit Satellitenverbindungen, wo die Signalstärke nur bei einem Schlüsselaustausch zwischen Erde und Satellit einsetzbar ist, weil die Satelliten mit ihrem transparenten Transponder die Signale verstärken.

Das zentrale Prinzip liegt in der Reziprozität des Funkkanals: Da beide Geräte denselben physikalischen Übertragungsweg nutzen, messen sie nahezu identische Kanaleigenschaften. Diese gemeinsamen Messwerte bilden die Grundlage für die Generierung identischer kryptografischer Schlüssel auf beiden Seiten, ohne dass diese Informationen über einen separaten Kanal ausgetauscht werden müssen. Mit RKD entstehen auf beiden Seiten (A und B) gleiche nichtdeterministische Zufallszahlen, die ihre Entropie direkt aus den physikalischen Eigenschaften der Funkübertragung beziehen.

RKD führt damit eine Erzeugung und Verteilung von Schlüsseln zwischen zwei Seiten durch, die auf physikalischen Verfahren basiert. Diese Funkkanalparameter (Messwerte) sind jeweils nur den an der Übertragung beteiligten Geräten A und B bekannt und können von einem Dritten (Angreifer) nicht gemessen werden. Änderungen der Messungen entstehen vor allem durch die Dynamik des Übertragungsweges (Entfernungsänderungen, Reflexionen etc.), die bei ruhenden Objekten zum Teil künstlich erzeugt werden muss. Im Falle von Satellitenverbindungen ergibt sich die Dynamik durch die Bewegung der Satelliten im LEO-Bereich (ca. 1.000 km Höhe), die aber als späterer Schlüssel Qualitätsprobleme bei der Zufälligkeit haben können. Bei Satellitenverbindungen ergibt sich auch das Problem des Man-in-the-middle, den der Satellit darstellt, was bei direkten Verbindungen (Freistrahkanälen) nicht der Fall ist.

Der Vorteil von RKD ergibt sich vor allem bei den Kosten und der Robustheit, insbesondere bei bewegten Objekten. Die erforderlichen Sende-/Empfangsstationen sind am Markt als SDR (Software Defined Radio) kostengünstig erhältlich. Mit diesen Geräten können nicht nur die Funkübertragung, sondern auch die Messungen ausreichend genau durchgeführt werden.

Der Nachteil von RKD ist die extrem langsame Schlüsselerzeugung, die sich aus den Dynamikanforderungen ergibt - maximal einige Bits pro Sekunde sind möglich. In Verbindung mit einem AES-256 zur Datenverschlüsselung und/oder einer MAC-Berechnung zur Integritätssicherung reicht es, bei einem One-Time-Pad sind aber nur sehr kleine Datenmengen möglich.

2.1.1 Physikalische Grundlagen der Zufälligkeit

Die für die Schlüsselgenerierung erforderliche Zufälligkeit entsteht z.B. beim Einsatz der Signalstärke durch kontinuierliche Schwankungen der Signalstärke, die durch eine Vielzahl physikalischer Faktoren verursacht werden:

- Bewegung der Kommunikationsgeräte: Bereits minimale Positionsänderungen (wenige Zentimeter) führen zu messbaren Veränderungen der Signalstärke durch veränderte Interferenzmuster
- Dynamische Umgebungseinflüsse: Bewegliche Objekte im Funkfeld, wie Personen, Fahrzeuge oder schwankende Vegetation verändern kontinuierlich die Ausbreitungsbedingungen
- Reflexionsverhalten: Sich verändernde Reflexionen an Wänden, Gebäuden und anderen Oberflächen erzeugen komplexe Interferenzmuster und beeinflussen damit die Signalqualität
- Atmosphärische Bedingungen: Luftfeuchtigkeit, Temperatur und andere meteorologische Parameter beeinflussen die Funkausbreitung
- Elektromagnetische Interferenzen: Andere Funksignale und elektromagnetische Störungen schaffen zusätzliche Variabilität

Aus diesen rein physikalischen Veränderungen kann nun ein kryptografischer Schlüssel berechnet werden. Der entscheidende Vorteil liegt darin, dass beide Kommunikationspartner dieselben physikalischen Bedingungen messen und somit zu identischem Schlüsselmaterial gelangen können, während für außenstehende Dritte diese Informationen nicht zugänglich sind.

Die Sicherheit von RKD beruht auf dem fundamentalen physikalischen Prinzip, dass Funkkanaleigenschaften stark ortsabhängig sind. Ein potentieller Angreifer (Eve), der sich wenige Meter entfernt befindet, misst aufgrund der räumlichen Dekorrelation des Funkkanals signifikant andere Werte und kann daher keine verwertbaren Informationen über den generierten Schlüssel erlangen.

Die räumliche Vielfalt der Übertragung und den zufälligen Bewegungsmustern erzeugt eine natürliche Zufallsquelle, die Man-in-the-Middle-Angriffe praktisch ausschließt.

2.1.2 Dynamikanforderungen

Für eine erfolgreiche Schlüsselgenerierung ist eine gewisse Dynamik des Übertragungsweges erforderlich. Diese entsteht natürlicherweise durch Entfernungänderungen zwischen den Kommunikationspartnern, Bewegungen in der Umgebung oder sich verändernde Reflexionsbedingungen. Bei statischen Szenarien muss diese Dynamik teilweise künstlich erzeugt werden, z.B. durch kontrollierte Bewegung eines der Geräte oder durch Nutzung rekonfigurierbarer Antennen.

2.1.3 Wirtschaftliche und technische Vorteile

Die Vorteile von RKD zeigen sich in den geringen Gerätekosten und der hohen Systemrobustheit, insbesondere bei mobilen Anwendungen. Die erforderliche Hardware basiert auf kommerziell verfügbaren LoRa-Modulen oder Software Defined Radios (SDRs), die inklusive Energieversorgung, Gehäuse und Software bereits ab circa 200 Euro erhältlich sind. Diese kostengünstigen Komponenten ermöglichen sowohl die Funkübertragung als auch die präzise Erfassung der für die Schlüsselgenerierung erforderlichen Kanalmessungen bis hin zum kryptografischen Schlüssel.

Dort, wo RKD gut anwendbar ist, bietet sie eine kostengünstige und massentaugliche Lösung und das gilt vor allem für bewegliche Objekte, wie Verkehrsinfrastrukturen (Straße, Schiene, Wasser, Luft), beweglichen IoT-Geräten, Drohnen, militärische Einheiten, Laptops etc. Es ist kein zusätzlicher nichtdeterministischer Zufallszahlengenerator erforderlich, weil sich die Zufälligkeit aus den zufälligen Messwerten ergibt. In diesem Umfeld ergeben sich auch Anwendungen mit sehr geringen Datenmengen, die One-Time-Pad fähig sind.

Für Anwendungen mit erweiterten Reichweitenanforderungen über Satellitenverbindungen steigen die Systemkosten auf mehrere tausend Euro pro Endgerät, da zusätzliche Signalverstärker und hochwertige Antennen erforderlich werden. Allerdings ist die satellitengestützte Infrastruktur bereits vorhanden, da lediglich transparente Transponder in LEO- und GEO-Satelliten benötigt werden, die schon vorhanden sind, wodurch keine neue Infrastruktur im Weltraum erforderlich ist.

Mit RKD ist also kostengünstig und massentauglich die zufällige Erzeugung und hochsichere Verteilung von symmetrischen Schlüsseln auf Basis physikalischer Verfahren möglich und folgend eine end-to-end Datenverschlüsselung.

2.1.4 Systemlimitationen

Die wesentliche Limitation von RKD liegt in der geringen Schlüsselgenerierungsrate, die systembedingt auf maximal 2-8 Bits pro Sekunde beschränkt ist. Diese Einschränkung resultiert aus den erforderlichen Dynamikanforderungen des Systems und der notwendigen Korrelationszeit zwischen den Kanalmessungen. Für konventionelle symmetrische Verschlüsselungsverfahren wie AES-256 oder Message Authentication Code (MAC) Berechnungen ist diese Rate ausreichend. Bei der Implementierung von One-Time-Pad-Verfahren ergeben sich jedoch erhebliche Einschränkungen hinsichtlich der verschlüsselbaren Datenmengen.

2.1.5 Anwendungsdomänen und Einsatzgebiete

RKD zeigt besondere Eignung für Anwendungen mit bereits gegebener Mobilität, da das System für die Schlüsselgenerierung Kanaldynamik benötigt. Primäre Einsatzgebiete umfassen:

- Verkehrsinfrastrukturen: Straßen-, Schienen-, Wasser- und Luftverkehr
- Mobile IoT-Systeme: Bewegliche Sensornetze und autonome Geräte
- Unbemannte Systeme: Drohnen und autonome Fahrzeuge
- Militärische und Sicherheitsanwendungen: Mobile Kommunikationseinheiten

2.1.6 Sicherheitsbetrachtung

Die Sicherheitsanalyse von RKD-Systemen erfordert eine differenzierte Betrachtung verschiedener Angriffsszenarien. Aufgrund der inhärenten Messungenauigkeiten und der probabilistischen Natur der Funkkanalcharakteristik sind passive Man-in-the-Middle-Angriffe theoretisch möglich, wenn sich ein Angreifer (Eve) in einer räumlich optimalen Position zu einem der legitimen Kommunikationspartner positionieren kann.

Für einen erfolgreichen Angriff aus einiger Entfernung (bei mehreren Metern müsste ein Angreifer mindestens drei bis vier kalibrierte Empfangsgeräte in verschiedenen räumlichen Positionen um Alice oder Bob platzieren. Diese Messung an mehreren Punkten wäre erforderlich, um die dreidimensionalen Anteile der Funkfeldverteilung zu erfassen und mittels räumlicher Interpolation die Signalcharakteristik am Zielort (Opfer, Bob oder Eve) zu rekonstruieren. Dieses Szenario funktioniert ohne Berücksichtigung der Reflexionen, d.h. z.B. im freien Feld ohne Bebauung, Bäume etc.

Der technische Aufwand für diese Attacke ist erheblich: Alle Empfangsgeräte müssten präzise zeitlich synchronisiert werden, identische Kalibrierung aufweisen und kontinuierlich ihre exakten räumlichen Positionen relativ zum Zielobjekt bestimmen. Bei bewegten Szenarien – und die ist bei RKD üblich – potenziert sich diese Komplexität exponentiell, da das gesamte Messsystem in Echtzeit der Bewegung folgen und dabei die räumlichen Korrelationen aufrechterhalten müsste. Diese praktischen Limitationen machen koordinierte räumliche Angriffe in realen Umgebungen, insbesondere wenn auch Reflexionen auftreten, undurchführbar, insbesondere bei den typischen Mobilitätsszenarien, für die RKD primär konzipiert ist.

Experimentelle Validierungen unter kontrollierten Bedingungen haben gezeigt, dass bereits bei Abständen von 50 cm bis 1 m zwischen Eve und den legitimen Kommunikationspartnern eine signifikante räumliche Dekorrelation der Kanalmessungen auftritt. In diesen Worst-Case-Szenarien

weist Eve eine zwei- bis dreifach höhere Bitfehlerrate gegenüber Alice und Bob auf, was die Lokalität der Kanalcharakteristik bestätigt.

Privacy Amplification Verfahren, basierend auf dem Leftover Hash Lemma, bieten informationstheoretische Sicherheit selbst bei partieller Kompromittierung des rohen Schlüsselmaterials. Ein zunächst kontraintuitiver Aspekt des Systems ist die Toleranz gegenüber der großen Anzahl an öffentlich preisgegebenen Bits. Es stellt tatsächlich kein sicherheitstechnisches Problem dar, wenn bis zu 80% des ursprünglichen Schlüsselmaterials während der Cascade-Korrektur öffentlich kommuniziert werden. Diese Robustheit resultiert aus den Informationstheoretischen Grundlagen der Privacy Amplification. Folgende Beispielrechnung soll dies erläutern:

Roher Schlüssel: $n = 2000 \text{ Bits}$

Öffentlich übertragene Bits: $n \times 80\% = 1600 \text{ Bits}$

Niemals übertragene Bits: $v = n \times 20\% = 400 \text{ Bits}$

Sicherheitsmarge: $s = 50 \text{ Bits}$

$$\text{Sicherer Schlüssel} = n - v - s = 2000 - 1600 - 50 = 350 \text{ Bits}$$

Selbst ein Angreifer mit Kenntnis von über 1600 Bits (80%) des ursprünglichen Schlüsselmaterials kann keinerlei Rückschlüsse auf den finalen 256-Bit Schlüssel ziehen. Diese Eigenschaft basiert auf den informationstheoretischen Garantien des Leftover Hash Lemmas und stellt sicher, dass die verbleibende Entropie vollständig in den sicheren Schlüssel extrahiert wird.

Bei satellitengestützten RKD-Implementierungen fungiert der Satellit systembedingt als transparenter Repeater, der empfangene Signale verstärkt und retransmittiert. Dies stellt per Definition einen Man-in-the-Middle dar, wodurch die Vertrauenswürdigkeit der Satelliteninfrastruktur zur Systemvoraussetzung wird.

Alternative Sicherheitsarchitekturen können dieses Problem durch die Beschränkung der sicheren Kommunikation auf direkte Satellit-Bodenstation-Verbindungen adressieren, wobei die End-to-End-Sicherheit zwischen terrestrischen Endpunkten durch nachgelagerte kryptographische Protokolle gewährleistet wird.

2.1.7 Marktreife

Die systematische Analyse des Forschungsstandes offenbarte eine erhebliche Implementierungslücke zwischen theoretischen Erkenntnissen und praktischen Marktanwendungen. Obwohl RKD seit zwei Jahrzehnten ein etabliertes Forschungsgebiet darstellt und umfangreiche wissenschaftlicher Literatur vorliegt, konnte kein kommerzielles Produkt identifiziert werden, das RKD zur Erzeugung und Verteilung kryptografischer Schlüssel für Endverbraucher ermöglicht. Das heißt, RKD mangelt es an praxistauglichen, marktfähigen Lösungen.

Dieser Umstand führte zur Entwicklung eines praxistauglichen Produkts und umfangreichen Praxistests, um im Rahmen des vorliegenden Projektes zu Praxisdaten in realen Umgebungen zu kommen. Dieses Produkt wurde im Rahmen von zwei von der FFG finanzierten KIRAS Projekten von der Firma insitu software gmbh entwickelt und ist inzwischen – noch ohne Zertifizierung - am Markt

verfügbar. Es stellt ein LoRa-basiertes RKD-System dar und umfasst eine vollständige Implementierung, wobei die LoRa-Module autonom Messdaten sammeln und nach dem Anschluss über die USB-Schnittstelle z.B. an einem Laptop eine Software, die ebenfalls Teil der Lösung ist, die Schlüsselgenerierung durchführt. Für die Hardware und Software muss insgesamt mit rund € 200,- gerechnet werden. Die Hardware ist in einem kleinen Gehäuse verbaut (siehe Bild), mobil, sehr robust und enthält neben einer USB-Schnittstelle zur Schlüsselanlieferung einen Akku. In Verbindung z.B. mit einem Laptop erzeugt das RKD-Gerät dann ständig Schlüsselbits, wenn es in Bewegung ist (z.B. wenn der Träger des Laptops im Unternehmen unterwegs ist) und wenn der Laptop in Verwendung ist, was meist im Stillstand passiert, liefert das RKD-Gerät wieder neues Schlüsselmaterial. Das Innenleben des RKD-Gerätes kann auch in andere Geräte integriert werden – es besteht ausschließlich aus weltweit verfügbaren Standardprodukten des Massenmarktes – oder in der vorliegenden Form an mobile Geräte angeschlossen werden.

Die Software ist in zwei Versionen verfügbar, die unterschiedliche Lösungsansätze verfolgen. Nachdem der aktuelle Forschungsstand viele verschiedene Lösungsansätze behandelt (siehe unten Literaturanalyse), die, je nach Anwendungsumgebung, alle ihre Vor- und Nachteile aufweisen, die aber in den Publikationen oftmals nur eingeschränkt erkennbar sind, wurden nach einer Evaluierung zwei Lösungsansätze ausgewählt und implementiert. Dadurch war eine leichtere Entscheidungsfindung zur Identifikation optimaler Systemkomponenten hinsichtlich Effizienz, Sicherheit, Kosten und Benutzerfreundlichkeit möglich.

Auf das vorliegende Projekt bezogen konnten dadurch die umfangreichen Praxistests breiter angelegt werden, um zu noch besseren Praxisdaten in realen Umgebungen zu kommen. Auf Basis der Literaturanalyse war dies nur eingeschränkt und mit großen Unsicherheiten möglich. Im Text oben erfolgte nur eine allgemeine Beschreibung von RKD. Für Leser, die detaillierter erfahren möchten, wie RKD wirklich funktioniert und nicht die umfangreiche wissenschaftliche Literatur durcharbeiten möchten, ist im Anhang 1 eine detailliertere Beschreibung angegeben.

2.1.8 Distanz

Die Distanz ist bei Direktfunk-basierten RKD-Systemen auf rund 15 Kilometer begrenzt, wobei bei hervorragenden Bedingungen wesentlich größere Entfernungen möglich sind. Das entwickelte und als Produkt verfügbare LoRa-basierte System erreicht bei guten Sichtverbindungen bis zu einigen Kilometer, wobei hier die Distanz durch die erlaubte Sendeleistung und Technologiestandards begrenzt ist. Die Reichweitenbeschränkungen ergeben sich aus mehreren regulatorischen und technischen Faktoren: LoRa-Module operieren im lizenzfreien ISM-Band (z.B. 863-870 MHz in Europa) mit einer maximalen effektiven Sendeleistung von 25 mW ERP nach EU-Regulierung. Diese Leistungsbegrenzung, kombiniert mit der für RKD erforderlichen Präzision der RSSI-Messungen, limitiert die praktische Reichweite erheblich. Theoretisch sind mit hochwertigen Antennen und optimalen Ausbreitungsbedingungen Reichweiten bis zu 5 Kilometern möglich, jedoch sinkt dabei die Messgenauigkeit der Signalstärke, die für die Schlüsselgenerierung essentiell ist. Die räumliche Korrelation der Kanaleigenschaften zwischen Alice und Bob nimmt mit der Distanz ab, wodurch

sich die Fehlerrate in der Schlüsselgenerierung exponentiell erhöht. Der dokumentierte LoRa-Distanzrekord liegt bei 1336 Kilometern (erzielt auf offenem Meer unter perfekten Ausbreitungsbedingungen). Es ist nicht verifizierbar, ob bei solchen extremen Entfernungen genügend RSSI-Schwankungen vorhanden wären, um sichere Schlüssel ableiten zu können.

LEO-Satellitenverbindungen ermöglichen globale Reichweiten von mehreren tausend Kilometern zwischen beliebigen Erdpunkten. Für die Schlüsselgenerierung muss aber von beiden Kommunikationspartnern in beide Richtungen halbwegs gleichzeitig eine Verbindung via einem Satellit möglich sein, was die Zeitdauer der Satellitenverbindung und damit der Schlüsselgenerierung sowie die maximale Entfernung zwischen den beiden Kommunikationspartnern einschränkt. Des Weiteren entstehen Sicherheitsrisiken, da der Satellit als unvermeidbarer Man-in-the-Middle fungiert und die Vertrauenswürdigkeit der Satelliteninfrastruktur voraussetzt. In der Praxis bedeutet das bei LEO-Satelliten (ca. 1000km Flughöhe) eine Verbindungszeit pro Satellitenüberflug von rund 5 bis 15 Minuten.

2.1.9 Kosten

Die Kosten von RKD im terrestrischen Bereich sind aufgrund der kostengünstigen, kommerziell verfügbaren Komponenten gering:

- LoRa Module: € 15 - € 40
- Antenne: € 5 - € 15
- Energieversorgung: € 8 - € 15
- Gehäuse: € 3 - € 8
- Kleinteile: € 2 - € 5 (Kabel, Schrauben, Dichtungen, USB-Anschluss)
- PCB und Elektronik: € 5 - € 10 (Spannungsregler, LED-Indikatoren, Schalter)
- Software: wegen der aktuell geringen Stückzahl sind hier noch höhere Beträge erforderlich

Satellitenkompatible RKD-Systeme erfordern eine vollständige Bodenstation mit speziellen Komponenten:

- Hochwertiges SDR
- Nachführbares Antennensystem
- Verstärker und Filter
- Stromversorgung
- Zulassungen (Funktechnik, Schalttechnik)

Die Kosten steigen damit auf einige tausend Euro pro Endgerät.

2.2 Literaturanalyse

RKD (Radio-signal key distribution) wird in der wissenschaftlichen Literatur verschieden bezeichnet (siehe Literaturverzeichnis), z.B. mit "Wireless Physical Layer Key Agreement". Im Gegensatz zu QKD, das mit Lichtquanten arbeitet, nutzt RKD Funksignale über 30 MHz.

Wenn zwei Kommunikationspartner in der drahtlosen Übertragung Zugang zu einer gemeinsamen Zufallsquelle haben, z.B. durch Messungen eines sich verändernden Kanalzustands, können sie eine geheime Schlüsselvereinbarung treffen. Dabei wandeln sie ihre gemessenen Werte in identische Schlüsselbits um. Diese Methode, auch als Schlüsselvereinbarung auf der physikalischen Schicht bekannt, hat insbesondere in der Forschung zur drahtlosen Kommunikationssicherheit an Popularität gewonnen [Yener15, Zeng15].

Die gemeinsame Zufallsquelle nutzt zwei fundamentale Eigenschaften von Funkkanälen: Kanalreziprozität und inhärente Unvorhersagbarkeit. Diese Eigenschaften können von drahtlosen Kommunikationsendgeräten erfasst werden. Wenn ein Angreifer keinen Zugriff auf die gemeinsamen Messungen hat, kann er keine Informationen über die geheimen Schlüssel extrahieren. Die Sicherheit liegt daher nicht in Vermutungen, sondern in physikalischen Gesetzen.

Die aktuelle Forschung zur Schlüsselvereinbarung auf der physikalischen Schicht lässt sich in fünf Hauptkategorien unterteilen:

- Messtechniken (wird nachfolgend nicht behandelt)
- Algorithmen zur Schlüsselgenerierung
- Widerstandsfähigkeit gegen Angriffe
- Fortgeschrittene Schlüsselvereinbarungsmethoden
- Experimentelle Validierungsbemühungen

Der nachfolgende Überblick behandelt wissenschaftliche Arbeiten aus dem Zeitraum 2007-2024.

2.2.1 Die vier Grundphasen der Schlüsselgenerierung

Die Umwandlung gemessener Funkkanaleigenschaften in geheime Schlüsselbits erfolgt in vier grundlegenden Phasen:

- Kanalerkundung
- Schlüsselbit-Extraktion
- Fehlerkorrektur
- Privatsphärenverstärkung

2.2.2 Phase 1: Kanalerkundung

In der ersten Phase tauschen die Kommunikationspartner kurze Nachrichten über den drahtlosen Kanal aus und schätzen anschließend die Funkkanaleigenschaften aus den empfangenen Signalen. Für die Kanalerkennung wurden verschiedene Signalmerkmale untersucht:

- Empfangssignalstärke (RSS) [Mathur08, Premnath14, Aono05]
- Amplitude [Wilson07]
- Phasenwinkel [Mathur11, Wang11]
- Hüllkurve [Azimi-Sadjadi07]
- Ankunftszeitwinkel [Badawy15]
- Ankunftszeit [Marino14]

- Kanalimpulsantwort [Liu2012]
- Kanalfrequenzantwort [Hongbo13]

Zusätzlich wurden adaptive Messstrategien entwickelt, die sich ändernde Kanalbedingungen automatisch verfolgen [Yasukawa08].

2.2.3 Phase 2: Schlüsselbit-Extraktion

In der zweiten Phase werden die verarbeiteten Messwerte mittels Quantisierungsverfahren in binäre Schlüsselsequenzen umgewandelt. Die verwendeten Algorithmen umfassen:

- Einfache 1-Bit-Quantisierer mit einem [Aono05, Tope01] oder zwei Schwellenwerten [Mathur08]
- Mehrbit-Quantisierer [Patwari10, Ambekar12]
- Adaptive Quantisierer [Hamida09]
- Vektorquantisierung [Hong17]
- Auf Singulärwertzerlegung basierende Quantisierer [Furqan16]

Ergänzend können digitale Signalverarbeitungsalgorithmen [Pawtari10, Yasukawa08] eingesetzt werden, um Abweichungen zwischen den Messwerten zu reduzieren, die durch Rauschen oder Hardware-Ungenauigkeiten entstehen.

2.2.4 Phase 3 & 4: Fehlerkorrektur und Privatsphärenverstärkung

Anschließend werden Korrekturalgorithmen und Privatsphärenverstärkung angewendet, um weitere Fehlerkorrektur und Widerstandsfähigkeit gegen Abhörversuche zu gewährleisten. Die Fehlerkorrektur umfasst:

- Fehlerkorrekturcodes [Ambekar12, Etesami12]
- Reed-Solomon-Codes [Zhang10]
- Informationsabgleichsprotokolle [Brassard94]

Diese Verfahren dienen der Integritätsprüfung der generierten Schlüssel. Nach der Fehlerkorrektur werden universelle Hash-Funktionen zur Privatsphärenverstärkung verwendet [Premnath13]. Dieser Prozess eliminiert Informationen, die potenzielle Lauscher während der Übertragung erhalten haben könnten.

2.2.5 Bewertung der Schlüsselqualität

Vor der Verwendung des extrahierten Schlüssels in kryptographischen Algorithmen muss dessen Qualität, insbesondere die Zufälligkeit der Bits, bewertet werden.

Die vom US National Institute of Standards and Technology (NIST) empfohlenen statistischen Tests [Rukhin10] umfassen:

- Mono-Bit-Frequenztest: Überprüft das Verhältnis von Nullen und Einsen im Schlüssel
- Runs-Test: Bewertet die Unabhängigkeit aufeinanderfolgender Bitsequenzen

- Spektraltest: Analysiert die diskrete Fourier-Transformation des Schlüsselstroms

Speziell für die drahtlose Schlüsselgenerierung wurden weitere Tests entwickelt:

- Maurers statistischer Test: Besonders geeignet für kurze Schlüsselsequenzen [Maurer92]
- Online-Entropieschätzung: Konzipiert für leichtgewichtige Hardware-Implementierungen und überwacht direkt die Zufälligkeit der Kanalparameter [Zenger15-2]

2.2.6 Schutz vor Angriffen

Komplexere Schlüsselgenerierungsschemata wurden entwickelt, um die Widerstandsfähigkeit gegen verschiedene Angriffe zu verbessern. Arbeiten wie [Jana09, Eberz12] untersuchen die Auswirkungen passiver und aktiver Man-in-the-Middle-Angriffe. In diesen Szenarien übernimmt ein geschickter Angreifer die Kontrolle über den Schlüsselgenerierungsprozess, indem er Kanalbedingungen manipuliert oder gefälschte Sondierungspakete einschleust.

Ähnliche Angriffe, einschließlich Signalmaskierung während der Kanalerkundung und entsprechende Gegenmaßnahmen, werden in [Zafer12] behandelt. Weitere Studien haben gezeigt, dass die sogenannte Pilot-Randomisierungstechnik aktive Signalinjektionsangriffe erfolgreich in weniger schädliche reaktive Störangriffe umwandeln kann [Mitev19].

Diese Technik wurde kürzlich auch für fortgeschrittene Kommunikationssysteme untersucht:

- Drahtlose Relaiskommunikation [Letafati23]
- Schutz vor Angriffen auf intelligente reflektierende Oberflächen [Hu23]

2.2.7 Fortgeschrittene Schlüsselvereinbarungsverfahren

Eine zweite Gruppe fortgeschrittener Verfahren zielt darauf ab, den Kommunikationsaufwand während der Kanalerkundung zu verringern. Dies wird durch verschiedene fortschrittliche Messtechniken erreicht:

- Synchronisierte Messungen in Zusammenarbeit mit drahtlosen Sensornetzwerken [Premnath14]
- Multiple-Input-Multiple-Output-Antennen (MIMO) für parallele Kanalerkennung [Wallace10] und Strahlformung [Huang13]

Beide Ansätze haben auch in statischen Kommunikationsszenarien Verbesserungen der Schlüsselgenerierungsraten gezeigt.

Das MIMO-Konzept wurde in [Jiao18] auf mmWave-Massive-MIMO-Konfigurationen erweitert, wie sie in 5G-Netzwerken eingesetzt werden. Hier führen Störungen des Ankunfts winkels zu einer deutlichen Erhöhung der geheimen Schlüsselrate.

2.2.8 Moderne Kommunikationstechnologien

Jüngste Fortschritte in drahtlosen Kommunikationssystemen wurden untersucht, um die Schlüsselgenerierung zu verbessern:

Rekonfigurierbare parasitäre Antennenarrays [Mehmood12] und intelligente reflektierende Oberflächen (IRS) [Ji21] können die Zufälligkeit der Kanalmessungen erhöhen. Ein Beispiel ist die elektronisch steuerbare parasitäre Array-Strahlerantenne, die zufällige Strahlsteuerung für schnellere Schlüsselgenerierung nutzt [Aono05].

Intelligente reflektierende Oberflächen bestehen aus großen passiven Anordnungen reflektierender Antennenelemente und wurden ursprünglich zur Erhöhung der Kanalkapazität eingesetzt. Wie in [Ji21] gezeigt, kann durch geeignete Steuerung der Array-Elemente die geheime Schlüsselkapazität für Nutzer mit Einzelantennen maximiert werden, selbst bei Anwesenheit nicht-kooperierender Lauscher.

Dieses Konzept wurde in [Li23] auf mmWave-MIMO-Systeme erweitert, wo IRS in Kombination mit kompressivem Sampling herkömmliche kanalzustandsbasierte Verfahren bei niedrigen Signal-Rausch-Verhältnissen übertraf.

2.2.9 Vollduplex-Transceiver

Die drahtlose Schlüsselgenerierung wurde auch für Vollduplex-Transceiver untersucht - Geräte, die gleichzeitiges Senden und Empfangen auf demselben Kanal ermöglichen [Vogt19]. Der Vollduplexmodus verringert unter bestimmten Bedingungen die Fähigkeit von Lauschern, Schlüsselmaterial der legitimen Parteien zu extrahieren, wodurch die Angriffsresistenz gestärkt wird.

Wie jedoch in [Luo23] gezeigt wurde, hängen die erreichbare Schlüsselkapazität und die Leistungsgewinne gegenüber Halbduplex-Verfahren stark von der analogen Selbstinterferenzunterdrückung ab.

2.2.10 Praktische Anwendungen

Verschiedene Ansätze wurden entwickelt, um Schlüsselvereinbarungstechniken näher an reale Anwendungen heranzuführen:

- IoT-Geräte mit geringem Stromverbrauch: Maßgeschneiderte Lösungen wurden in [Zenger14, Zenger15-1] vorgeschlagen
- Fahrzeugsysteme: [Zan13] entwickelte Schlüsselgenerierung zur Sicherung der Fahrzeugkommunikation
- LoRaWAN-Systeme: Für stromsparende Weitbereichsnetzwerke stellte [Ruotsalainen20] eine rekonfigurierbare antennengestützte Schlüsselübertragungskette vor und lieferte umfangreiche experimentelle Ergebnisse für Innen- und Außenbereichsszenarien

2.3 Literaturverzeichnis

[Zeng15] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," in IEEE Communications Magazine, vol. 53, no. 6, pp. 33-39, June 2015.

[Yener15] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1814-1825, Oct. 2015.

[Mathur08] S. Mathur & al. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel." In Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom '08). ACM, New York, NY, USA, pp. 128-139.

[Premnath14] S.N. Premnath & al. "Efficient High-Rate Secret Key Extraction in Wireless Sensor Networks Using Collaboration." in ACM Transactions on Sensor Networks, Vol. 11, No. 1, Jul. 2014

[Aono05] T. Aono & al., "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Transactions on Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[Wilson07] R. Wilson, D. Tse, and R. A. Scholtz, Channel identification: Secret sharing using reciprocity in ultrawideband channels, IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 364–375, Sep. 2007

[Mathur11] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, ProxiMate: Proximity-based secure pairing using ambient wireless signals, in Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys), Washington, DC, USA, Jul. 2011, pp. 211–224.

[Wang11] Q. Wang, H. Su, K. Ren and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," 2011 Proceedings IEEE INFOCOM, Shanghai, China, 2011

[Azimi-Sadjadi07] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. 2007. Robust key generation from signal envelopes in wireless networks. In Proceedings of the CCS '07. ACM, New York, NY, USA, 401-410.

[Badawy15] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trincherro and C. -F. Chiasserini, "Secret Key Generation Based on AoA Estimation for Low SNR Conditions," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 2015

[Marino14] F. Marino, E. Paolini and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," 2014 IEEE International Conference on Ultra-WideBand (ICUWB), Paris, France, 2014

[Liu12-1] Y. Liu, S. C. Draper and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[Hongbo13] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. 2013. Fast and practical secret key extraction by exploiting channel response. In Proceedings of IEEE INFOCOM). IEEE, Turin, Italy, 3048–3056.

[Yasukawa08] S. Yasukawa, H. Iwai and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM," in Proceedings of the International Symposium on Information Theory and Its Applications, Auckland, 2008, pp. 1-6.

[Ambekar12] A. Ambekar, M. Hassan and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in Proceedings of the International Symposium on Signals, Systems, and Electronics (ISSSE), Potsdam, 2012, pp. 1-4.

[Hamida09] S. Hamida, J. Pierrot and C. Castelluccia, "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements" in Proceedings of the 3rd International Conference on New Technologies, Mobility and Security, Cairo, 2009, pp. 1-5

[Hong17] P. Hong, & al., "Vector Quantization and Clustered Key Mapping for Channel-Based Secret Key Generation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1170-1181, May 2017

[Furgan16] H. M. Furqan, J. M. Hamamreh and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," 2016 International Symposium on Wireless Communication Systems (ISWCS), Poznan, Poland, 2016, pp. 597-602

[Etesami12] J. Etesami and W. Henkel, "LDPC code construction for wireless physical-layer key reconciliation," in Proceedings of the First IEEE International Conference on Communications in China, Beijing, China, Aug. 15-18, 2012.

[Zhang10] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in Proc. 32nd IEEE International Conference of Computer Communications (INFOCOM), San Diego, CA, USA, Mar. 2010, pp. 1-5.

[Brassard94] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in Proceedings of the Workshop Theory Applied Cryptography (EUROCRYPT), pp. 410-423, 1994

[Premnath13] S. N. Premnath et al., "Secret key extraction from wireless signal strength in real environments," in IEEE Transactions on Mobile Computing, vol. 12, no. 5, pp. 917-930, May 2013.

[Rukhin10] A. L. Rukhin & al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in Tech. Rep. of National Institution of Standards and Technology, Gaithersburg, MD, USA, 800-22, Apr. 2010

[Maurer92] Maurer, U.M. A universal statistical test for random bit generators. J. Cryptology 5, 89–105 (1992).

[Zenger15-1] CT Zenger, J Zimmer, M Pietersz, JF Posielek, C Paar, Exploiting the physical environment for securing the internet of things, Proceedings of the 2015 New Security Paradigms Workshop, 44-58

[Jana09] S. Jana & al. 2009. "On the effectiveness of secret key extraction from wireless signal strength in real environments." In Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom '09). ACM, New York, NY, USA, 321-332.

[Eberz12] S. Eberz & al. "A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols" In Proceedings of the 17th European Symposium on Research in Computer Security (ESORICS '12), Springer, 2012.

[Zafer12] M. Zafer & al. "Limitations of generating a secret key using wireless fading under active adversary." in IEEE/ACM Transactions of Networking, Vol. 20 No. 5, Oct. 2012, pp. 1440-1451

[Premnath14] S.N. Premnath & al. "Efficient High-Rate Secret Key Extraction in Wireless Sensor Networks Using Collaboration." in ACM Transactions on Sensor Networks, Vol. 11, No. 1, Jul. 2014

[Mitev19] M. Mitev, A. Chorti, E. V. Belmega and M. Reed, "Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6

[Letafati23] M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Learning-Based Secret Key Generation in Relay Channels Under Adversarial Attacks," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 749-764, 2023, doi: 10.1109/OJVT.2023.3315216

[Hu23] L. Hu, G. Li, A. Hu and D. W. K. Ng, "Exploiting Malicious RIS for Secret Key Acquisition in Physical-Layer Key Generation," in IEEE Wireless Communications Letters, doi: 10.1109/LWC.2023.3330809

[Wallace10] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 381-392, Sept. 2010.

[Huang13] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in Proceedings of IEEE INFOCOM, Turin, 2013, pp. 2292-2300.

[Mehmood12] R. Mehmood and J. W. Wallace, "Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas," 2012 6th European Conference on Antennas and Propagation (EUCAP), Prague, 2012, pp. 1151-1155.

[Jiao18] L. Jiao, N. Wang and K. Zeng, "Secret Beam: Robust Secret Key Agreement for mmWave Massive MIMO 5G Communication," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6

[Aono05] T. Aono, K. Higuchi, T. Ohira, B. Komiyama and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," in IEEE Transactions on Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005

[Ji21] Z. Ji et al., "Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 1030-1034, Jan. 2021

[Li23] H. Li, L. Chen, T. Lu and A. Hu, "Angular-domain Secret Key Generation for RIS-aided mmWave MIMO systems," 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), Hong Kong, Hong Kong, 2023, pp. 1-6, doi: 10.1109/VTC2023-Fall60731.2023.10333834.

[Vogt19] H. Vogt, Z. H. Awan and A. Sezgin, "Secret-Key Generation: Full-Duplex Versus Half-Duplex Probing," in IEEE Transactions on Communications, vol. 67, no. 1, pp. 639-652, Jan. 2019

[Luo23] H. Luo, N. Garg and T. Ratnarajah, "A Channel Frequency Response-Based Secret Key Generation Scheme in In-Band Full-Duplex MIMO-OFDM Systems," in IEEE Journal on Selected Areas in Communications, vol. 41, no. 9, pp. 2951-2965, Sept. 2023

[Ruotsalainen20] H. Ruotsalainen, J. Zhang and S. Grebeniuk, "Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1745-1755, March 2020

Nachfolgend befindet sich ein Auszug weiterer wichtiger Literatur mit einer Kurzbeschreibung des Inhalts:

Fast, efficient error reconciliation for quantum cryptography. W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue and C. G. Peterson.

Beschreibung von Verfahren zur Fehlerkorrektur.

Demystifying the Information Reconciliation Protocol Cascade, Jesus Martinez-Mateo, Christoph Pacher, Momtchil Peev, Alex Ciurana, and Vicente Martin. Juli 2014.

Beschreibung des Cascade Protokolls zur Fehlerkorrektur in QKD. Erklärt die mögliche Leistung, Stärken, Schwächen sowie den Vergleich verschiedener modifizierter Versionen. Dieses Verfahren ist auch für RKD sehr interessant.

Efficient physical layer key generation technique in wireless communications. Rushan Lin, Li Xu, He Fang, Chuan Huang. 9. Jänner 2020.

Beschreibung eines Schlüsselgenerierungssystems auf Basis von Signalstärkemessung.

Error Detection and Authentication in Quantum Key Distribution. Akihiro Yamamura, Hirokazu Ishizuka. 2001

Beschreibung eines gesamten Ablaufs der Schlüsselgenerierung sowie eine Analyse verschiedener Fehlerkorrekturverfahren. Dieses Verfahren ist auch für RKD sehr interessant.

A Physical-Layer Key Generation Approach Based on Received Signal Strength in Smart Homes. H. Zhao, Y. Zhang, X. Huang, Y. Xiang and C. Su. 1. April 2022.

Schlüsselgenerierung für Smart Home Geräte. Adaptives Verfahren auf Basis von Signalstärkemessung. Komplexes Quantisierungsverfahren.

Physical Layer Key Generation in 5G Wireless Networks. . Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang and K. Zeng. Oktober 2019.

Analyse der Technologie im 5G Bereich. Beschreibung der Vorteile von 5G, weil Lauschangriffe

durch Beamforming erschwert werden. Weiters eignen sich der sonst ungenutzte Kanal sehr gut, um Fehler im Schlüssel zu minimieren.

Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems. Jiang Wan, Anthony Lopez, Mohammad Abdullah Al Faruque. 30 Oktober 2018.

Beschreibung der Herausforderungen im Automotive Bereich. Erklärung wie Code-Overhead reduziert werden konnte. Simulation mit ferngesteuerten Fahrzeugen.

Physical Layer Secret Key Generation in Static Environments. Nasser Aldaghri, Hesham Mahdavi. 17 Februar 2020.

Erklärung wie auch in statischen Umgebungen RKD genutzt werden kann. Kombination aus lokalen Zufälligkeiten sowie der Funkkanaleigenschaften.

Error Reconciliation in Quantum Key Distribution Protocols. Miralem Mehic, Marcin Niemiec, Harun Siljak, Miroslav Voznak. 2020.

Genauer Vergleich mehrerer Fehlerkorrekturverfahren und den erwartbaren Verlust and Schlüsselbits der von dritten Parteien abgefangen werden kann.

3 Projektinhalt

3.1 SDR / Satellitenkommunikation

Im Projektteil Satellitenkommunikation sah das ursprüngliche Konzept vor, die Laufzeiten von Signalen zwischen zwei Bodenstationen über einen Satelliten als Informationsquelle zu nutzen. Durch präzise Messung der Signallaufzeiten und deren kontinuierlicher Schwankungen sollten kryptographische Schlüssel berechnet werden. Diese Variationen entstehen durch die orbitale Bewegung des Satelliten, atmosphärische Einflüsse und andere physikalische Faktoren.

Da eine genauere Analyse ergab, dass der vorgesehene Zeitrahmen nicht für eine zufriedenstellende Umsetzung ausgereicht hätte, wurde der Satelliten-basierte Projektteil nach Rücksprache mit der FFG gestoppt und der terrestrische Bereich ausgebaut, indem zwei Lösungsvarianten implementiert wurden.

Auf der Basis des KIRAS-Forschungsprojektes KIF und den Arbeiten in den ersten zwei Projektmonaten entstand auch im Projektteil Satellitenkommunikation schon einiges Know-how, das in den weiteren Projektverlauf übernommen wurde. Dabei geht es vor allem um:

- Aufbau der Entwicklungsumgebung
- Ablaufdiagramme der Prozessschritte
- Literaturanalyse, weil der Forschungsbereich viele Überlappungen aufweist
- Erfahrungen und Algorithmen der Signalstärkeanalyse

3.2 Entwicklungsprojekt für Algorithmmik

Die Literaturanalyse (siehe Kap. 2.2) zeigt, dass der Forschungsstand viele verschiedene Lösungsansätze ermöglicht. Je nach Anwendungsumgebung haben alle diese Lösungsansätze Vor- und Nachteile, die aber in den Publikationen oftmals nur eingeschränkt erkennbar sind. Daher erfolgte vor Projektstart und während des Projektes eine Evaluierung des Forschungsstandes. Aus dieser haben sich zwei Lösungsansätze ergeben, die dann implementiert wurden. Dieses Kapitel enthält eine umfangreiche Beschreibung der zwei Produktvarianten.

Nach der Entscheidung für ein terrestrisches System auf Basis von Signalstärkemessungen wurde ein umfassendes Entwicklungsprojekt gestartet. Als Entwicklungsplattform wurde Python 3 gewählt, um eine agile Prototyping-Umgebung zu schaffen, die schnelle Iterationen, flexible Umstrukturierungen und kreative Ideenfindung ermöglichte. Das Projekt durchlief kontinuierliche „Umstrukturierungen“, um eine möglichst breite Palette von Ansätzen gut evaluieren zu können. Trotz der dynamischen Entwicklung folgte die Softwareentwicklung einem konsistenten Grundablauf, der als stabiles Fundament für alle Experimente diente. Der Entwicklungsprozess war geprägt von einem durchgehenden Wechsel zwischen verschiedenen Algorithmen und Komponenten.

Diese methodische Herangehensweise ermöglichte es, die leistungsfähigsten Ansätze zu identifizieren und gezielt weiterzuentwickeln, während weniger erfolgreiche Konzepte frühzeitig ausgeschlossen und entfernt werden konnten.

Nachfolgend werden nur die Komponenten betrachtet, welche auch tatsächlich übernommen wurden.

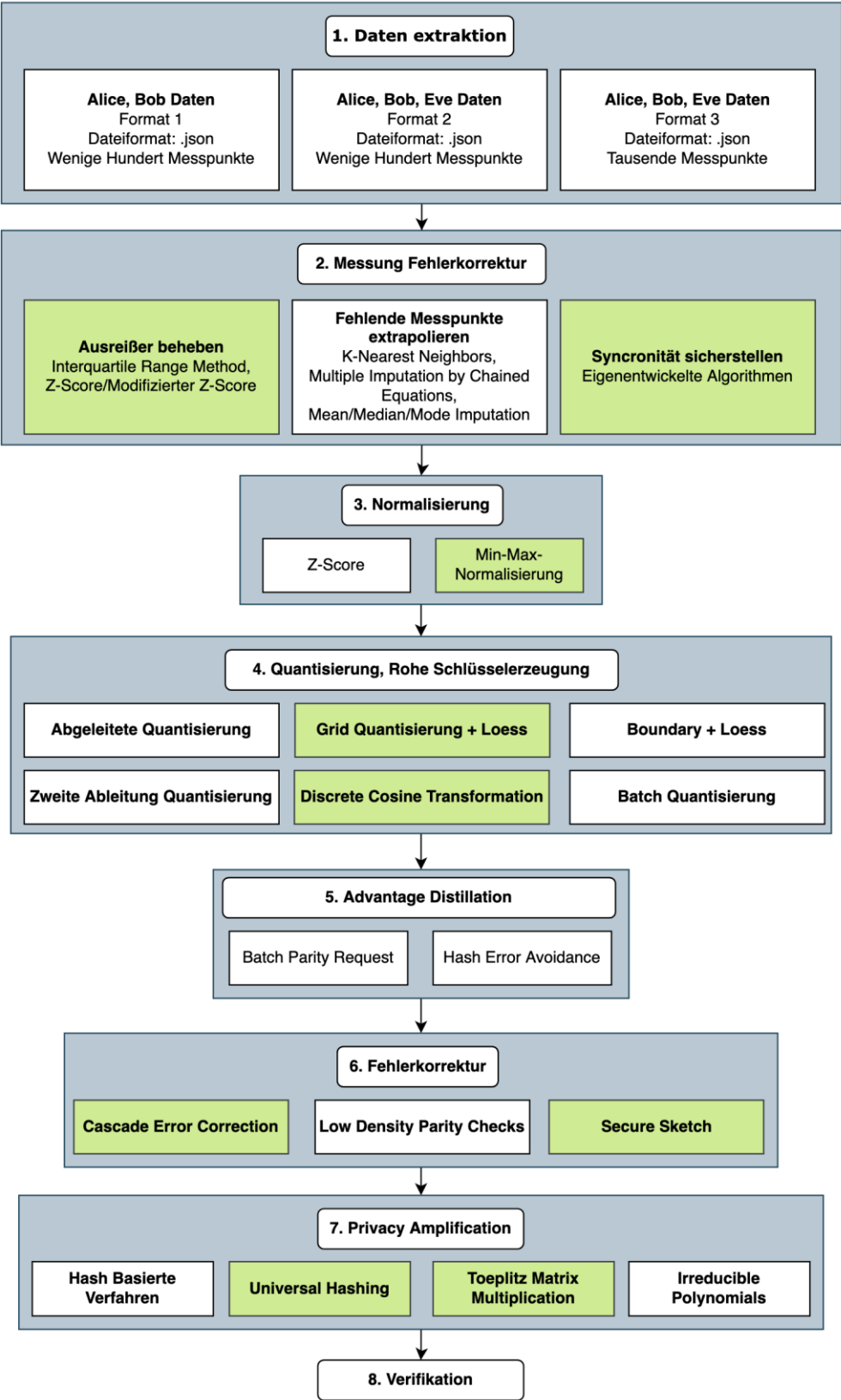


Abbildung 1: Darstellung Ablauf und getestete Methoden

Nachdem alle Module getestet wurden, konnten die besten identifiziert werden. Diese wurden in der Abbildung grün markiert.

3.2.1 Messung Fehlerkorrektur

Durch elektronische Fehler kommt es immer wieder zu unvermeidbaren Fehlern in den Messdaten. Das äußert sich durch das Fehlen einzelner Messblöcke oder gravierenden Ausreißern. Diese werden gleich zu Beginn behoben, um im späteren Verlauf der Datenverarbeitung keine Fehler zu erzeugen.

3.2.2 Normalisierung

Nach der Auswertung verschiedenster Messszenarien zeigte sich, dass es keinen signifikanten Unterschied zwischen den bevorzugten Normalisierungsarten gibt. Aufgrund der einfacheren und schnelleren Berechnung wurde die Min-Max-Normalisierung ausgewählt.

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

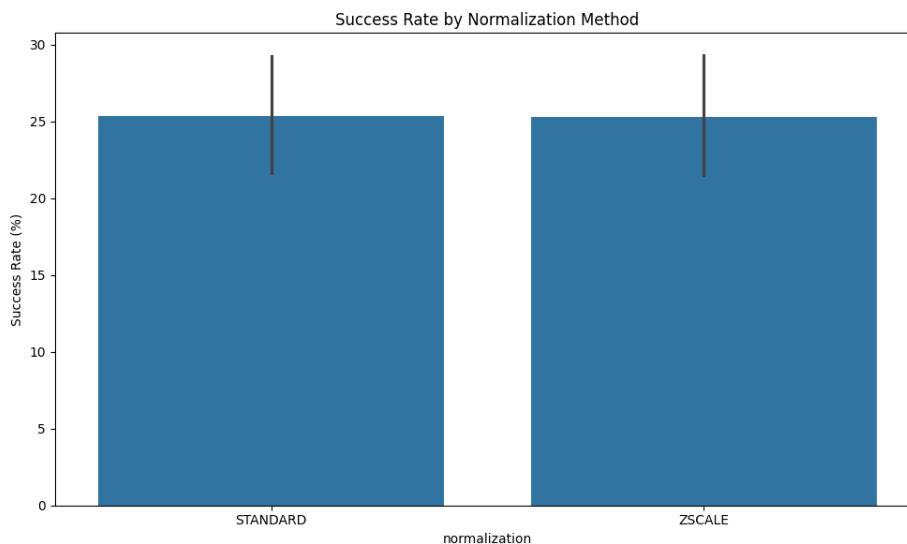


Abbildung 2: Vergleich der Normalisierungsmethoden

3.2.3 Grid Quantisierung + Loess

Nach der Normalisierung jedes Messabschnitts wird eine LOESS-Transformation (Locally Estimated Scatterplot Smoothing) angewendet. Diese statistische Methode ist für RSSI-Messungen gut geeignet, da diese naturgemäß starken Schwankungen unterliegen und nicht exakt auf einer Linie verlaufen. LOESS erzeugt durch lokale Regression eine geglättete Kurve, die den grundlegenden Trend der verrauschten RSSI-Datenpunkte widerspiegelt und gleichzeitig die charakteristischen Variationen des Funkkanals bewahrt.

Die resultierende LOESS-Kurve bildet die Grundlage für alle weiteren Berechnungen.

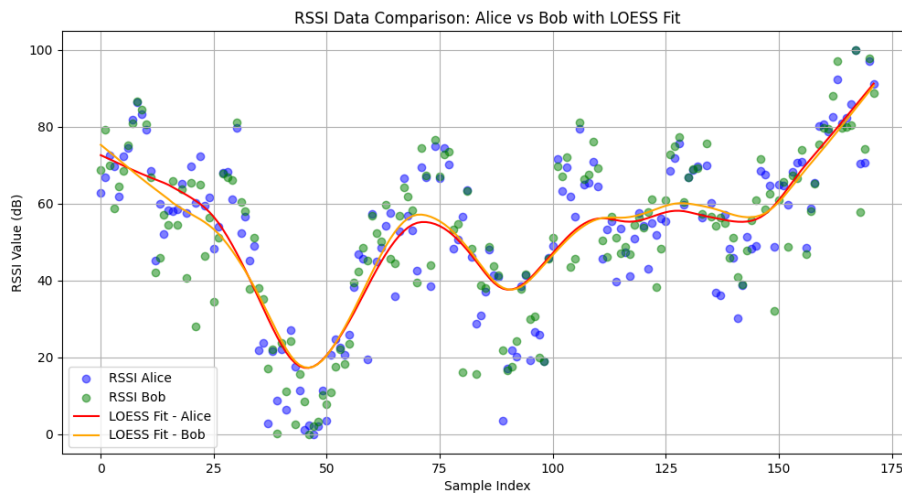


Abbildung 3: Darstellung Loess Kurve

Es wird nun, je nach gewünschter Genauigkeit, ein weit- bis engmaschiges Gitter (Grid) über die Loesskurve gelegt. Nachfolgend wird ausgehend von der Kurve die Distanz zu den Punkten berechnet, die der Kurve am nächsten sind. Die Position des nächsten Punkts auf der Y-Achse spiegelt den binären Wert dieses Teils des Schlüssels wider. Der Vorgang wird, basierend auf der gewünschten Gesamtschlüssellänge, bis zu mehrere tausend Mal wiederholt.

Je nach gewünschter Auflösung wird ein Gitter (Grid) mit unterschiedlich dicht platzierten Punkten über die LOESS-Kurve gelegt. Die Gitterdichte fungiert als primärer Steuerparameter:

- **Weitmaschiges Gitter:** Höhere Robustheit gegenüber Messrauschen, niedrigere Auflösung
- **Engmaschiges Gitter:** Feinere Auflösung, höhere Sensitivität gegenüber Kanalschwankungen

Für jeden Zeitpunkt der Schlüsselgenerierung wird ausgehend von der LOESS-Kurve die euklidische Distanz zu sämtlichen Gitterpunkten berechnet. Der Algorithmus identifiziert systematisch den Gitterpunkt mit der geringsten Distanz zur ausgewählten Kurvenposition. Die Y-Koordinate des nächstgelegenen Gitterpunkts wird zur Bestimmung des binären Werts herangezogen. Diese Position wird entsprechend der zuvor definierten Quantisierungslogik in einen Binärcode umgewandelt, wobei die Anzahl der Bits pro Messpunkt die Auflösung der Y-Achsen-Segmentierung bestimmt.

Der beschriebene Vorgang wird, basierend auf der gewünschten Gesamtschlüssellänge, iterativ durchgeführt. Für typische kryptographische Schlüssel kann diese Wiederholung bis zu mehrere tausend Mal erfolgen, wobei jede Iteration weitere Bits des finalen Schlüssels generiert.

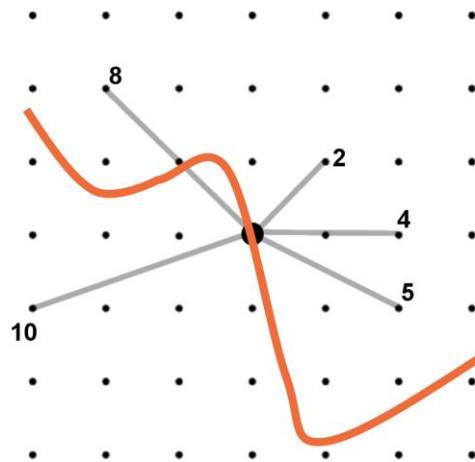


Abbildung 4: Visualisierung Gitter

3.2.4 Discrete Cosine Transformation

Ein alternativer Ansatz zur Quantisierung des rohen Schlüsselmaterials ist die Discrete Cosine Transformation (DCT) zur Frequenzanalyse der Messdaten. Bei dieser Methode werden die RSSI-Daten mittels DCT in ihre einzelnen Frequenzkomponenten zerlegt und der Schlüssel aus den einzelnen Frequenzanteilen generiert. Die Auswertung zeigt, dass sowohl die untersten als auch die höchsten Frequenzanteile des Spektrums nur schwach zwischen Alice und Bob korrelieren, was vermutlich auf systembedingtes Rauschen und hochfrequente Störeinflüsse zurückzuführen ist. Der mittlere Frequenzbereich hingegen weist eine signifikant höhere Korrelation zwischen den Kommunikationspartnern auf, während Eve in diesem Frequenzbereich deutlich geringere Korrelationsdaten zeigt. Diese Methode ermöglicht es die Frequenzkomponenten für die Schlüsselgenerierung zu nutzen, die sowohl eine hohe Korrelation zwischen Alice und Bob gewährleisten als auch eine maximale Dekorrelation gegenüber potenziellen Angreifern aufweisen.

3.2.5 Cascade Error Correction

Nach einer umfangreichen Analyse der Cascade Error Correction sowie des Low Density Parity Checks (LDPC) wurde für Cascade entschieden. Cascade erwies sich als deutlich einfacher zu implementieren. Während LDPC-Codes eine komplexe Matrixstruktur und aufwendige Belief-Propagation-Algorithmen erfordern, bietet Cascade einen intuitiven, schrittweisen Ansatz zur Fehlerkorrektur. Ein entscheidender Vorteil von Cascade ist seine adaptive Natur. Das Protokoll kann sich an die tatsächlichen Fehlercharakteristiken des Kanals anpassen, während LDPC-Codes für spezifische Fehlerraten optimiert werden müssen.

Für die moderate Fehlerrate des vorliegenden Systems (typisch 10% bis 12.5%) zeigte Cascade einen geringeren Rechenaufwand als LDPC. Besonders bei kleineren Blockgrößen, wie sie im vorliegenden Anwendungsfall auftreten, ist Cascade effizienter. Weil Cascade bei QKD (Quantum Key

Distribution) weit verbreitet ist, bietet es eine solide, erprobte Basis mit umfangreicher Literatur und bekannten Optimierungsmöglichkeiten.

Eine umfassende statistische Auswertung der im Projekt durchgeführten Cascade-Implementation bestätigte, dass die entwickelte Lösung sowohl die erwartete Effizienz als auch die geforderten Sicherheitsstandards erfüllt. Als Referenzmaßstab diente dabei das bereits beschriebene Paper „Error Reconciliation in Quantum Key Distribution Protocols“, dessen Ergebnisse und Leistungskennzahlen als Benchmark für die Bewertung herangezogen wurden.

3.2.6 Secure Sketch

Secure Sketch ist eine mögliche Alternative zum interaktiven Cascade-Protokoll, die das Fehlerkorrekturproblem mit einem völlig anderen Ansatz löst. Anstatt durch mehrere Übertragungen und Korrekturen schrittweise Fehler zu identifizieren, nutzt dieses Verfahren eine einmalige größere Übertragung zur Korrektur. Das Verfahren basiert auf der Idee, dass Alice eine Art "Korrektursignatur" ihres Schlüssels erstellt und öffentlich übertragen kann, ohne dabei den Schlüssel selbst preiszugeben. Diese Korrektursignatur, auch Sketch genannt, enthält gerade genug Informationen, um Bob bei der Korrektur seiner fehlerhaften Version zu helfen, ohne einem Außenstehenden nützliche Erkenntnisse zu liefern.

Alice nimmt ihren korrekten Schlüssel und verknüpft ihn mit einer zufällig generierten Sequenz, die nach bestimmten mathematischen Regeln strukturiert ist. Diese Version wird als Sketch über den öffentlichen Kanal gesendet. Bob kann mit seinem fehlerhaften Schlüssel und dem empfangenen Sketch seine Fehler automatisch korrigieren, vorausgesetzt die Anzahl der Fehler bleibt unter einer bestimmten Grenze. Der Korrekturprozess erfolgt dabei vollautomatisch ohne weitere Interaktion zwischen den Parteien.

Das Verfahren ist sicher, weil der Sketch für einen Angreifer wie eine völlig zufällige Bitsequenz aussieht. Ohne Kenntnis einer Version des ursprünglichen Schlüssels kann aus dem Sketch keine verwertbare Information extrahiert werden. Selbst wenn ein Angreifer den gesamten Sketch abfängt, erhält er dadurch kaum Rückschlüsse auf das ursprüngliche Schlüsselmaterial.

Der größte Nachteil liegt in der fehlenden Flexibilität. Das System muss im Voraus auf eine bestimmte maximale Fehlerrate kalibriert werden. Treten mehr Fehler auf als erwartet, versagt die Korrektur vollständig. Sind weniger Fehler vorhanden, wird Kapazität verschwendet. Zusätzlich erfordert das Verfahren, dass die Fehler gleichmäßig über den Schlüssel verteilt sind. Treten Fehler in größeren Gruppen auf, kann dies zu Problemen führen. Im Gegensatz zu Cascade benötigt Secure Sketch jedoch nur eine einzige Übertragungsrunde und ist damit wesentlich effizienter in der Kommunikation.

3.2.7 Privacy Amplification

Nach der erfolgreichen Fehlerkorrektur durch das Cascade-Protokoll verfügen Alice und Bob über identische Bitsequenzen, die jedoch nicht vollständig sicher sind. Ein potentieller Angreifer könnte

während der öffentlichen Kommunikation Informationen über Teile des Schlüssels erhalten haben. Um aus diesem partiell kompromittierten Material einen informationstheoretisch sicheren Schlüssel zu extrahieren, wird Privacy Amplification angewendet.

Das implementierte Verfahren basiert auf dem Leftover Hash Lemma. Dieses besagt, dass Universal Hash Functions in der Lage sind, aus schwach-zufälligen Quellen nahezu perfekte Zufälligkeit zu extrahieren. Als Universal Hash Function wird eine Toeplitz-Matrix verwendet, die durch ihre besonderen strukturellen Eigenschaften sowohl theoretische Sicherheitsgarantien als auch effiziente Implementierung ermöglicht.

Die Privacy Amplification erfolgt durch Multiplikation der ursprünglichen Bitsequenz mit einer zufällig generierten Toeplitz-Matrix.

Die Ausgabelänge des sicheren Schlüssels berechnet sich nach der Formel:

$$secureKeyLength = n - v - s$$

Hier ist n die ursprüngliche Schlüssellänge (z.B. 2048), v die Anzahl der möglicherweise kompromittierten Bits (z.B. 612) und s eine zusätzliche Sicherheitsmarge (2% bis 5% des Schlüssels) darstellt.

Um die rechnerische Effizienz zu steigern, wird die Toeplitz-Matrix-Multiplikation nicht direkt durchgeführt, sondern über eine Fast Fourier Transform (FFT) realisiert. Diese Optimierung reduziert die Komplexität von $O(n^2)$ auf $O(n \log n)$ und ermöglicht auch bei größeren Schlüssellängen eine schnelle Berechnung.

Das Verfahren bietet informationstheoretische Sicherheit: Selbst ein Angreifer mit sehr hohen Rechenkapazitäten kann aus dem resultierenden Schlüssel keine Informationen über den ursprünglichen Schlüssel extrahieren, sofern die Anzahl der kompromittierten Bits korrekt geschätzt wurde. Die Sicherheitsmarge s stellt zusätzlich sicher, dass auch bei Unterschätzung des Bitverlusts an Dritte ein ausreichendes Sicherheitsniveau gewährleistet bleibt.

Die Privacy Amplification stellt die finale Stufe der Schlüsselgenerierung dar und transformiert das korrigierte, aber potentiell teilweise bekannte Schlüsselmaterial in einen verwendbaren kryptographischen Schlüssel mit garantierter Zufälligkeit.

3.3 Lora Modul Entwicklung

Zur Durchführung der RSSI-Messungen wurde ein LoRa Modul benötigt. Hierfür wurde das „Lilygo lora32 t3_v1.6.1“ Modul ausgewählt.

Die Architektur der Firmware und des Messsystems ist in drei Schichten gegliedert:

- **Hardware-Ebene:** LILYGO LoRa-Modul mit ESP32-Mikrocontroller
- **Steuerungsebene:** Python-Scripts für die Computer (Alice/Bob)
- **Synchronisationsebene:** Redis-Datenbank als zentrale Koordinationsstelle

Die LILYGO-Module werden über serielle Schnittstelle (/dev/ttyAlice, /dev/ttyBob) von den Python-Skripts gesteuert. Diese starten die notwendigen Messungen, indem sie die Firmware ansprechen.

Alice und Bob führen koordinierte LoRa-Übertragungen durch. Dabei misst jede Seite die Signalstärke (RSSI), die momentane Signalstärke (IRSSI) und das Signal-Rausch-Verhältnis (SNR) der empfangenen Pakete. Das System sammelt systematisch 128 Messungen pro Batch. Jede Messung erhält einen eindeutigen Index, und die Indexfolge wird gehasht, um Messdatensätze eindeutig zu identifizieren.

Es gibt zwei Betriebsmodi:

- **Interaktiver Modus:** Direkte serielle Kommunikation mit sofortiger Datenübertragung
- **Headless-Modus:** Messungen werden im ESP32-Flash gespeichert und periodisch über esptool.py ausgelesen. Das ist ideal für unbeaufsichtigten Langzeitbetrieb.

Ebenfalls wurde ein Eve Modus implementiert, um einen Lauscher für Testzwecke einbinden zu können.

3.4 Messdatenerhebung

Zur Optimierung der einzelnen Verfahrensschritte wurde eine solide experimentelle Evaluierung durchgeführt. Diese systematische Analyse erforderte eine große Anzahl von Messungen unter diversen Umgebungsbedingungen und mit verschiedenen Bewegungsmustern, um die optimalen Parameter für die jeweiligen Algorithmen und Komponenten zu finden.

Sämtliche Messungen wurden unter perfekten Angriffsbedingungen für Dritte durchgeführt. Ein Lauscher (Eve) war während aller Experimente aktiv und immer zwischen 50 cm und 1 m von Alice entfernt. Alice war wie Eve stationär. Diese Konfiguration ermöglichte eine präzise Analyse der tatsächlichen Diskrepanz zwischen den Signalmessungen der legitimierten Kommunikationspartner und dem potenziellen Angreifer. Die gewählte geringe Distanz von maximal 1 m stellt einen Optimalfall für einen Angreifer dar, da eine derart nahe Positionierung in realen Szenarien äußerst schwierig unentdeckt aufrechtzuerhalten wäre.

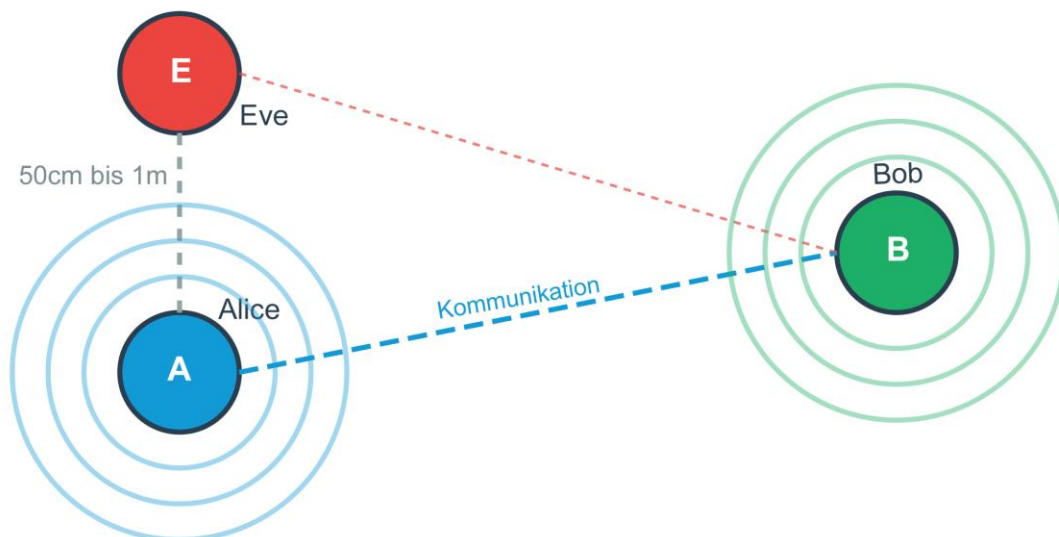


Abbildung 5: Messaufbau

Durch die Simulation dieser unrealistisch günstigen Angriffsbedingungen wurde eine konservative Sicherheitsbewertung erreicht. Wenn das System unter diesen idealen Bedingungen für einen Angreifer dennoch sicher funktioniert, ist die Sicherheit unter realistischen Bedingungen - wo ein Lauscher deutlich weiter entfernt und weniger optimal positioniert wäre - umso stärker gewährleistet.

Folgende Messszenarien wurden durchgeführt:

Statisch:

- Statische Systeme ohne Bewegung

Bewegung in Gebäude:

- Bewegung im selben Raum
- Bewegung im selben Stockwerk durch mehrere Räume
- Minimale Bewegung im Nebenraum
- Schnelles/langsames Spazieren im Gebäude in mehreren Stockwerken

Bewegung um Gebäude:

- Bewegung um das Gebäude herum und in naher Distanz zum Gebäude

Größere Entfernungen:

- Spazieren bis auf 1.2km Entfernung
- Laufen bis auf 800m Entfernung

Fahrzeuge bis max. 500m:

- Vom Gebäude wegfahren
- Hin und zurück fahren
- Vorbeifahren

3.5 Evaluierung der Messdaten und Verfahren

Alle zuvor durchgeführten Messungen wurden mit verschiedensten Algorithmusparametern getestet und die Ergebnisse ausgewertet. Dies ergab den Projektbeteiligten Auskunft über die optimalen Betriebsparameter, die im Endprodukt genutzt werden sollen.

3.6 Bits pro Messpunkt, Auflösung

Ein kritischer Parameter ist die Anzahl der Bits, die pro Messpunkt generiert werden sollen. Dieser Wert spiegelt die Auflösung wider, mit welcher die Loess Kurve betrachtet wird. Ein zu hoher Wert führt dazu, dass bereits minimalste Abweichungen zwischen Alice und Bob zu großen Unterschieden im rohen Schlüssel führt. Damit sinkt die Wahrscheinlichkeit diese anschließend alle korrigieren zu können. Ein zu niedriger Wert erhöht die Auflösung erheblich und ermöglicht es Angreifern den Schlüssel zu erraten.

- **2 Bit pro Messpunkt:** Wird als untere Grenze betrachtet, da hier die Fehlerrate noch tolerierbar bleibt und der Schlüssel ausreichend sicher ist
- **3-4 Bit pro Messpunkt:** Stellt den optimalen Betriebsbereich dar, in dem ein ausgewogenes Verhältnis zwischen Schlüsselgenerierungsrate und Fehlerrate erreicht wird
- **>4 Bit pro Messpunkt:** Führt zu exponentiell ansteigenden Fehlerrate und ist daher für praktische Anwendungen meist ungeeignet

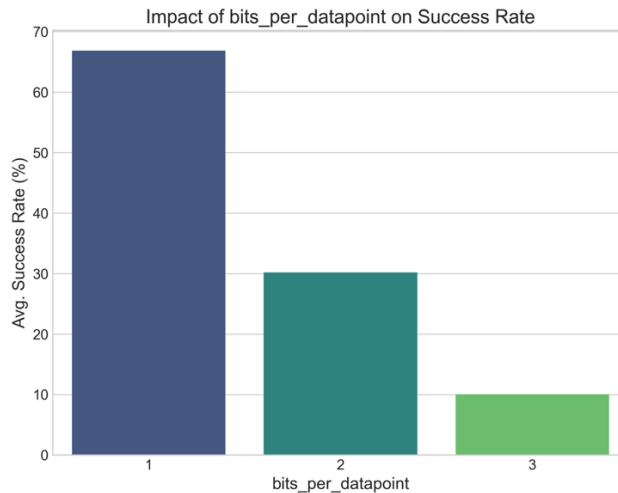


Abbildung 6: Bit Auflösung

3.6.1 Cascade Error Korrektion

Der Cascade Error Correciton Algorithmus ist adaptiv und passt sich automatisch an die erwarteten Fehlerraten des rohen Schlüssels an. Bei höheren erwarteten Fehlerrate führt Cascade mehr Iterationen mit feineren Blockgrößen durch. Dies erhöht die Wahrscheinlichkeit, sämtliche Diskrepanzen zwischen Alice und Bob zu identifizieren und zu korrigieren.

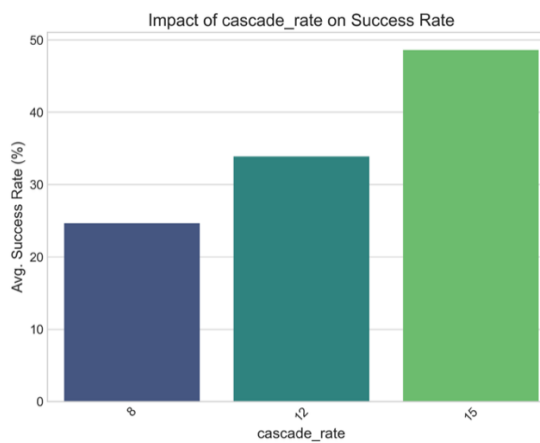


Abbildung 7: Cascade angenommene Fehlerrate

Diese erhöhte Korrekturgenauigkeit ist jedoch nicht immer optimal. Jede zusätzliche Iteration und jede feinere Blockaufteilung erfordern mehr Paritätsinformationen, die über den öffentlichen Kanal zwischen Alice und Bob ausgetauscht werden müssen. Ein passiver Angreifer (Eve), der diese Kommunikation abhört, kann aus diesen Paritätsbits Teile des rohen Schlüssels rekonstruieren.

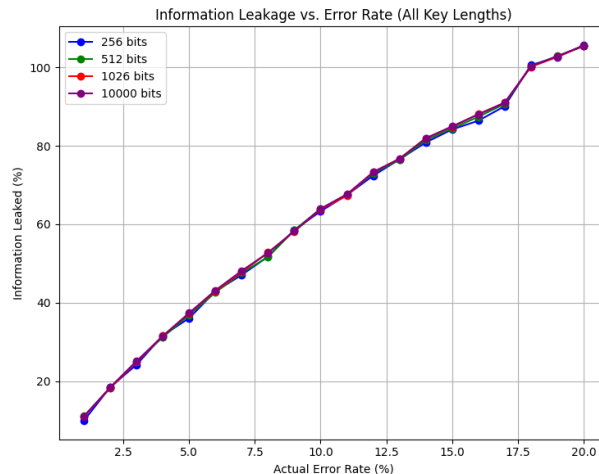


Abbildung 8: Informationsverlust an Dritte

Die Auswertung ergab, dass eine erwartete Fehlerrate zwischen 10% bis 15% als optimal für das System anzusehen ist. Diese Werte bieten den besten Kompromiss zwischen Korrektoreffizienz und Informationsverlust an Dritte

Ein zunächst kontraintuitiver Aspekt des Systems ist die Toleranz gegenüber der großen Anzahl an öffentlich preisgegebenen Bits. Es stellt tatsächlich kein sicherheitstechnisches Problem dar, wenn bis zu 80% des ursprünglichen Schlüsselmaterials während der Cascade-Korrektur öffentlich kommuniziert werden. Diese Robustheit resultiert aus den Informationstheoretischen Grundlagen der Privacy Amplification. Folgende Beispielrechnung soll dies erläutern:

- Roher Schlüssel: $n = 2000 \text{ Bits}$
- Öffentlich übertragene Bits: $n \times 80\% = 1600 \text{ Bits}$
- Niemals übertragene Bits: $v = n \times 20\% = 400 \text{ Bits}$
- Sicherheitsmarge: $s = 50 \text{ Bits}$

$$\text{Sicherer Schlüssel} = n - v - s = 2000 - 1600 - 50 = 350 \text{ Bits}$$

Selbst ein Angreifer mit Kenntnis von über 1600 Bits des ursprünglichen Schlüsselmaterials kann keinerlei Rückschlüsse auf den finalen 256-Bit Schlüssel ziehen kann. Diese Eigenschaft basiert auf den informationstheoretischen Garantien des Westover Hash Lemmas und stellt sicher, dass die verbleibende Entropie vollständig in den sicheren Schlüssel extrahiert wird.

3.6.2 Schlüsselgenerierungsmethode

Viele der initial implementierten Methoden zur Schlüsselgenerierung scheiterten bereits in den ersten Evaluierungsphasen aufgrund unzureichender Performance oder praktischer Limitierungen. Die aussichtsreichsten Methoden, die die initiale Evaluierung erfolgreich bestanden, wurden einer detaillierten Leistungsanalyse unterzogen. Diese Untersuchung ergab, dass die Performance der verbleibenden Kandidaten nahezu identisch war. Die Grad-Methode zeigte eine um 5% höhere

Wahrscheinlichkeit für eine erfolgreiche Schlüsselgenerierung. Daher wurde sie abschließend ausgewählt.

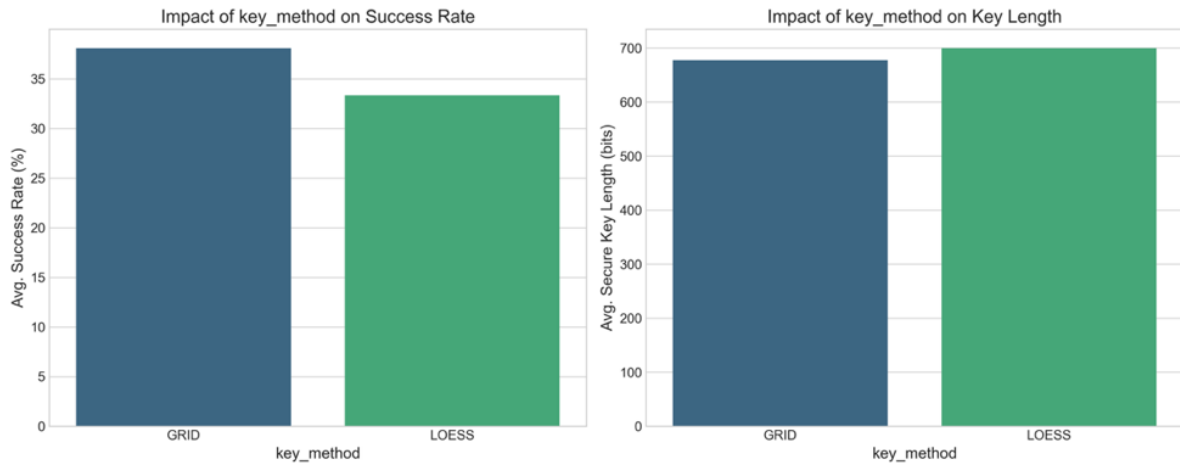


Abbildung 9: Vergleich Schlüsselgenerierung

3.6.3 Analyse Angreifer (Eve)

Für jede durchgeführte Messung generierte auch Eve einen rohen Schlüssel basierend auf ihren RSSI-Messungen. Dieser wurde anschließend jeweils mit den Schlüsseln von Alice und Bob verglichen, um die Sicherheit des Systems quantitativ zu bewerten. Die Analyse zeigt sowohl für die 2-Bit- als auch die 3-Bit-Auflösung einen statistisch signifikanten Unterschied zwischen den Bitfehlerrate der legitimierten Kommunikationspartner und dem Angreifer.

Eve weist im Durchschnitt eine zwei- bis dreifach höhere Bitfehlerrate gegenüber Alice und Bob auf. Diese Diskrepanz bestätigt die theoretischen Erwartungen über die Lokalität der Kanalcharakteristik. Eges erhöhte Fehlerrate demonstriert, dass trotz der optimalen Angriffsbedingungen (50cm bis 1m Abstand, stationäre Position) die räumliche Dekorrelation des Funkkanals ausreichend ist, um eine effektive Sicherheitsbarriere zu schaffen. Je weiter Eve von Alice und Bob entfernt ist, desto weniger korreliert sind ihre Messungen mit dem legitimen Schlüsselmaterial.

Zur korrekten Interpretation der nachfolgenden Grafiken wird darauf hingewiesen das eine 50%ige Bitfehlerrate bedeutet, dass Eges Schlüssel statistisch nicht von einem zufällig gewürfelten Schlüssel unterscheidbar ist. Eine 100%ige Fehlerrate würde bedeuten, dass Eve's Schlüssel perfekt anti-korreliert ist. Eve könnte dann alle Bits invertieren und erhielte den korrekten Schlüssel. Dies wäre

genauso gefährlich wie eine 0%ige Fehlerrate.

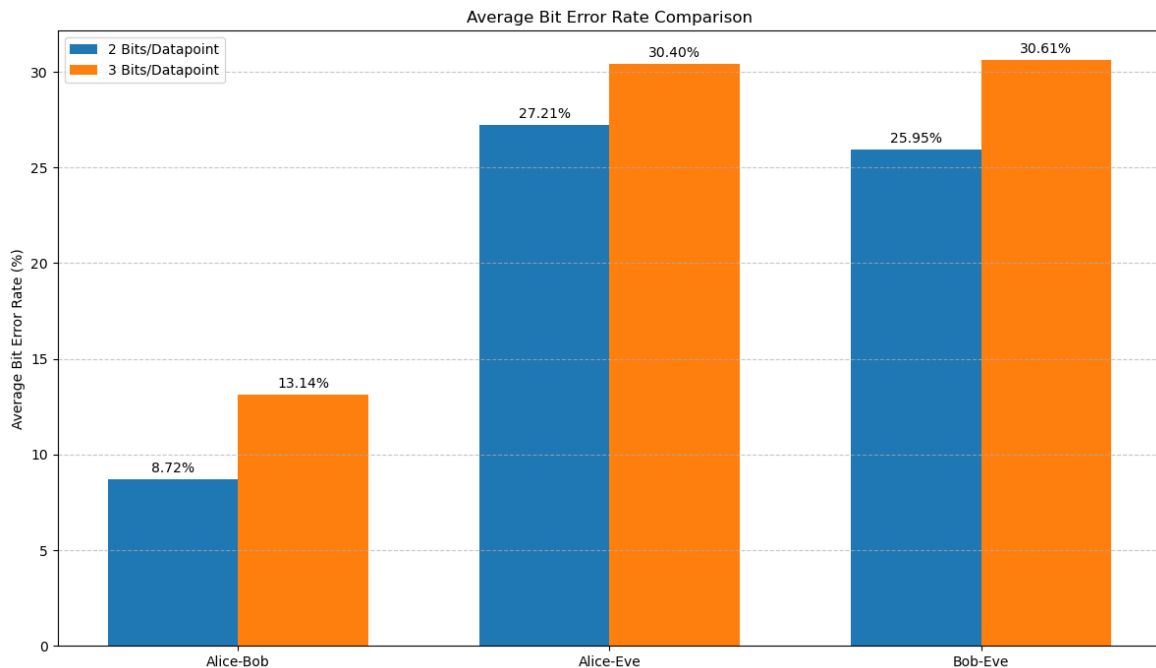


Abbildung 10: Vergleich Fehlerrate von drei Parteien

3.6.4 Konsumentenprojekte

Basierend auf den Vorentwicklungen wurden nach der Auswahl der richtigen Komponenten die Entwicklung von zwei Softwareentwicklungsprojekten gestartet. Die dabei entstehende RKD-Software soll benutzerfreundlich und ohne hohes technisches Vorwissen bedienbar sein. Als Ziel wurde definiert, dass zwei Lora Module durchgehend akkubetrieben, wenn es die Distanz erlaubt, Messdaten erheben. Nach einer beliebigen Zeit stecken die Konsumenten die Geräte an einen Computer mit der RKD-Software an. Diese führt dann mit den erhobenen Messdaten die Erzeugung und Verteilung der kryptografischen Schlüssel durch und stellt sie in einem nicht näher spezifizierten Format dem Konsumenten zur Verfügung. Als minimal ausgegebene Schlüssellänge wurden 256 Bits definiert, da dies in Kombination mit dem weit etablierten AES Algorithmus als Quantencomputersicher gilt.

4 Ergebnisse

4.1 Dockerbasierend

Das finale System ist als Multi-Container-Docker-Anwendung konzipiert, die eine saubere Trennung zwischen Datenerfassung und Schlüsselgenerierung ermöglicht. Diese Architektur gewährleistet Skalierbarkeit, einfache Wartung und ein einfaches Deployment.

- **Redis--Container:** Eine Datenbank mit Queue-Funktionalität. Hier werden die gesammelten Messdaten als JSON-Objekte gespeichert und über verschiedene Queues zwischen den Services koordiniert.
- **Measurement-Service-Container:** Führt die RSSI-Messungen durch. Diese Container benötigen privilegierte Rechte (`privileged: true`) für direkten Hardware-Zugriff auf die seriellen Schnittstellen der LILYGO-Module. Sie implementieren sowohl interaktive als auch headless Modi für verschiedene Einsatzszenarien.
- **Keygen-Service-Container:** Implementiert die komplexe Schlüsselgenerierung. Diese Container führen die kryptographischen Operationen durch und koordinieren sich über SSL/TLS-verschlüsselte Verbindungen zwischen Alice und Bob.

4.2 Datenfluss und Verarbeitungspipeline

Phase 1: Koordinierte Messungen: Alice initiiert LoRa-Übertragungen und beide Seiten messen synchron RSSI-Werte. Die Messwerte werden in 128er-Batches organisiert und über kryptographische Hashes der Indexsequenzen eindeutig identifiziert.

Phase 2: Signalverarbeitung: Die gesammelten RSSI-Daten durchlaufen eine Verarbeitungskette. Die Discrete Cosine Transformation wird zur Rauschreduzierung und Frequenzbereichsfilterung verwendet. Danach werden die Daten in den rohen binären Schlüssel umgewandelt.

Phase 3: Fehlerkorrektur: Da physikalische Messungen nie perfekt identisch sind, implementiert das System Secure Sketches. Dieses Verfahren ermöglicht es Bob seine Fehler zu korrigieren, ohne sensible Daten preiszugeben.

Phase 4: Privacy Amplification: Die korrigierten Schlüssel werden durch SHA256-Hashing verkürzt und von potentiellen Korrelationen befreit, um sichere Endschlüssel zu erzeugen.

Phase 5: Digest-Verifikation: Alice und Bob berechnen CRC32-Checksummen ihrer generierten Schlüssel und vergleichen diese. Nur bei Übereinstimmung werden die Schlüssel als gültig akzeptiert und in den finalen Schlüsselspeicher transferiert.

Eve-Simulation: Optional kann ein dritter Container als Lauscher betrieben werden, der versucht, aus abgehörten Übertragungen identische Schlüssel zu generieren - ein kritischer Test für die Sicherheit des Verfahrens.

Dieses System stellt eine vollständige, produktionsreife Implementierung der physikalischen Schlüsselgenerierung dar, die sowohl für Forschungszwecke als auch für praktische Anwendungen in sicherheitskritischen Umgebungen eingesetzt werden kann.

5 Schlussfolgerungen und Ausblick

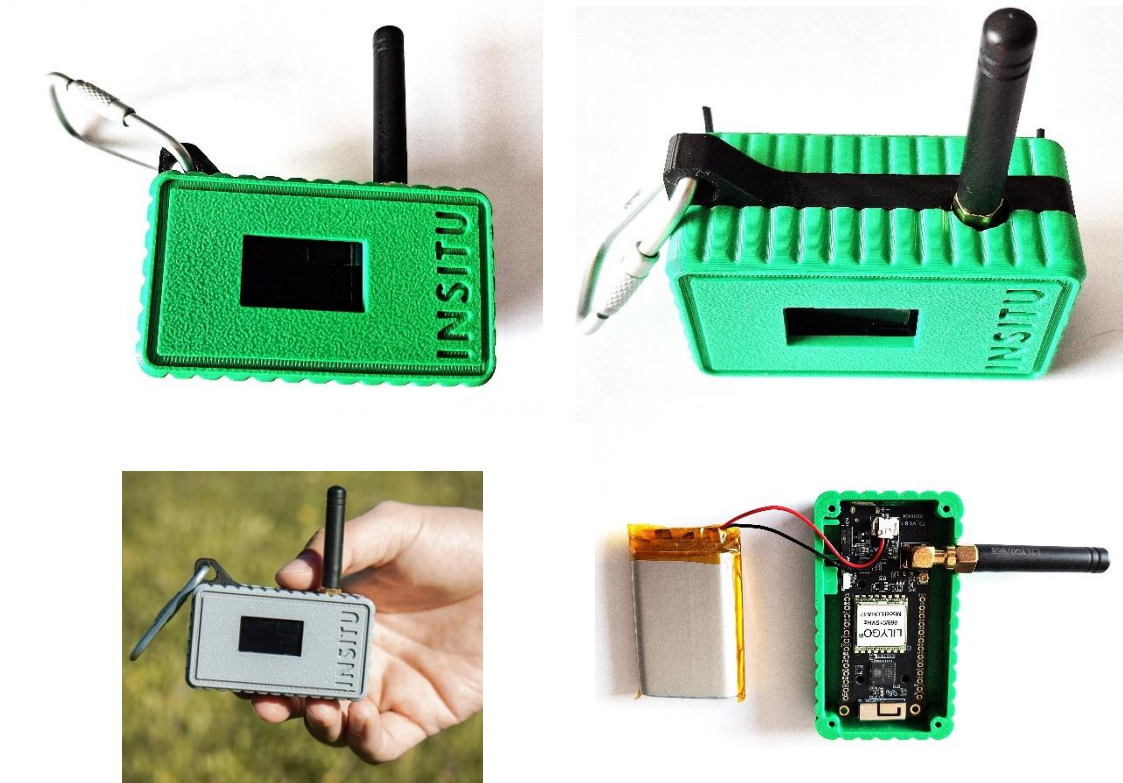
Das Projekt resultierte, wie geplant, in einem voll funktionsfähigen Gerät (siehe Bilder unten) und Software für die beiden Computer (Alice und Bob), welches durch RKD sichere kryptografische Schlüssel auf beiden Kommunikationsseiten generieren kann. Diese generierten Schlüssel können anschließend für unterschiedlichste kryptografische Anwendungsfälle weiterverwendet werden und bilden damit eine solide Grundlage für sichere Kommunikationssysteme.

Die während des Projekts gewonnenen Erkenntnisse eröffnen zudem interessante Perspektiven für weiterführende Forschungsarbeiten. Insbesondere die ursprünglich angedachte Lösung zur Schlüsselgenerierung durch Laufzeitmessungen bei Satellitenübertragungen bleibt ein vielversprechendes Forschungsfeld. Das durch dieses Projekt geschaffene breite Fundament an grundlegendem Wissen zur sicheren Schlüsselgenerierung stellt eine gute Basis dar.

Das nun vorliegende Produkt wurde schon intensiv bei der Studie „Kryptovergleich“ eingesetzt, bei der die physikalischen Verfahren zur Erzeugung und Verteilung kryptografischer Schlüssel QKD (Quantum Key Distribution), RKD (Radio-signal key distribution) und MKD (Memory key distribution) technologieneutral verglichen werden.

Mit dem vorliegenden Gerät und der Software steht erstmals ein Produkt für den Weltmarkt zur Verfügung. Es fehlen noch Zertifizierungen, die im Umfeld von Kryptografie, insbesondere hochsicherer Kryptografie, am Markt gefordert werden.

Die insitu software gmbh strebt die erforderlichen Zertifizierungen an und wird ab 2026 das Produkt am Weltmarkt anbieten.



Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1: Darstellung Ablauf und getestete Methoden | 24 |
| Abbildung 2: Vergleich der Normalisierungsmethoden..... | 25 |
| Abbildung 3: Darstellung Loess Kurve | 26 |
| Abbildung 4: Visualisierung Gitter..... | 27 |
| Abbildung 5: Messaufbau..... | 31 |
| Abbildung 6: Bit Auflösung..... | 33 |
| Abbildung 7: Cascade angenommene Fehlerrate | 33 |
| Abbildung 8: Informationsverlust an Dritte | 34 |
| Abbildung 9: Vergleich Schlüsselgenerierung | 35 |
| Abbildung 10: Vergleich Fehlerrate von drei Parteien..... | 36 |

6 Literaturverzeichnis

[Zeng15] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," in IEEE Communications Magazine, vol. 53, no. 6, pp. 33-39, June 2015.

[Yener15] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1814-1825, Oct. 2015.

[Mathur08] S. Mathur & al. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel." In Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom '08). ACM, New York, NY, USA, pp. 128-139.

[Premnath14] S.N. Premnath & al. "Efficient High-Rate Secret Key Extraction in Wireless Sensor Networks Using Collaboration." in ACM Transactions on Sensor Networks, Vol. 11, No. 1, Jul. 2014

[Aono05] T. Aono & al., "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Transactions on Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[Wilson07] R. Wilson, D. Tse, and R. A. Scholtz, Channel identification: Secret sharing using reciprocity in ultrawideband channels, IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 364–375, Sep. 2007

[Mathur11] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, ProxiMate: Proximity-based secure pairing using ambient wireless signals, in Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys), Washington, DC, USA, Jul. 2011, pp. 211–224.

[Wang11] Q. Wang, H. Su, K. Ren and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," 2011 Proceedings IEEE INFOCOM, Shanghai, China, 2011

[Azimi-Sadjadi07] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. 2007. Robust key generation from signal envelopes in wireless networks. In Proceedings of the CCS '07. ACM, New York, NY, USA, 401-410.

[Badawy15] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trincherro and C. -F. Chiasserini, "Secret Key Generation Based on AoA Estimation for Low SNR Conditions," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 2015

[Marino14] F. Marino, E. Paolini and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," 2014 IEEE International Conference on Ultra-WideBand (ICUWB), Paris, France, 2014

[Liu12-1] Y. Liu, S. C. Draper and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[Hongbo13] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. 2013. Fast and practical secret key extraction by exploiting channel response. In Proceedings of IEEE INFOCOM). IEEE, Turin, Italy, 3048–3056.

[Yasukawa08] S. Yasukawa, H. Iwai and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM," in Proceedings of the International Symposium on Information Theory and Its Applications, Auckland, 2008, pp. 1-6.

[Ambekar12] A. Ambekar, M. Hassan and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in Proceedings of the International Symposium on Signals, Systems, and Electronics (ISSSE), Potsdam, 2012, pp. 1-4.

[Hamida09] S. Hamida, J. Pierrot and C. Castelluccia, "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements" in Proceedings of the 3rd International Conference on New Technologies, Mobility and Security, Cairo, 2009, pp. 1-5

[Hong17] P. Hong, & al., "Vector Quantization and Clustered Key Mapping for Channel-Based Secret Key Generation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1170-1181, May 2017

[Furgan16] H. M. Furqan, J. M. Hamamreh and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," 2016 International Symposium on Wireless Communication Systems (ISWCS), Poznan, Poland, 2016, pp. 597-602

[Etesami12] J. Etesami and W. Henkel, "LDPC code construction for wireless physical-layer key reconciliation," in Proceedings of the First IEEE International Conference on Communications in China, Beijing, China, Aug. 15-18, 2012.

[Zhang10] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in Proc. 32nd IEEE International Conference of Computer Communications (INFOCOM), San Diego, CA, USA, Mar. 2010, pp. 1-5.

[Brassard94] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in Proceedings of the Workshop Theory Applied Cryptography (EUROCRYPT), pp. 410-423, 1994

[Premnath13] S. N. Premnath et al., "Secret key extraction from wireless signal strength in real environments," in IEEE Transactions on Mobile Computing, vol. 12, no. 5, pp. 917-930, May 2013.

[Rukhin10] A. L. Rukhin & al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in Tech. Rep. of National Institution of Standards and Technology, Gaithersburg, MD, USA, 800-22, Apr. 2010

[Maurer92] Maurer, U.M. A universal statistical test for random bit generators. J. Cryptology 5, 89–105 (1992).

[Zenger15-1] CT Zenger, J Zimmer, M Pietersz, JF Posielek, C Paar, Exploiting the physical environment for securing the internet of things, Proceedings of the 2015 New Security Paradigms Workshop, 44-58

- [Jana09]** S. Jana & al. 2009. "On the effectiveness of secret key extraction from wireless signal strength in real environments." In Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom '09). ACM, New York, NY, USA, 321-332.
- [Eberz12]** S. Eberz & al. "A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols" In Proceedings of the 17th European Symposium on Research in Computer Security (ESORICS '12), Springer, 2012.
- [Zafer12]** M. Zafer & al. "Limitations of generating a secret key using wireless fading under active adversary." in IEEE/ACM Transactions of Networking, Vol. 20 No. 5, Oct. 2012, pp. 1440-1451
- [Premnath14]** S.N. Premnath & al. "Efficient High-Rate Secret Key Extraction in Wireless Sensor Networks Using Collaboration." in ACM Transactions on Sensor Networks, Vol. 11, No. 1, Jul. 2014
- [Mitev19]** M. Mitev, A. Chorti, E. V. Belmega and M. Reed, "Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6
- [Letafati23]** M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Learning-Based Secret Key Generation in Relay Channels Under Adversarial Attacks," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 749-764, 2023, doi: 10.1109/OJVT.2023.3315216
- [Hu23]** L. Hu, G. Li, A. Hu and D. W. K. Ng, "Exploiting Malicious RIS for Secret Key Acquisition in Physical-Layer Key Generation," in IEEE Wireless Communications Letters, doi: 10.1109/LWC.2023.3330809
- [Wallace10]** J. W. Wallace and R. K. Sharma, "Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 381-392, Sept. 2010.
- [Huang13]** P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in Proceedings of IEEE INFOCOM, Turin, 2013, pp. 2292-2300.
- [Mehmood12]** R. Mehmood and J. W. Wallace, "Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas," 2012 6th European Conference on Antennas and Propagation (EUCAP), Prague, 2012, pp. 1151-1155.
- [Jiao18]** L. Jiao, N. Wang and K. Zeng, "Secret Beam: Robust Secret Key Agreement for mmWave Massive MIMO 5G Communication," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6
- [Aono05]** T. Aono, K. Higuchi, T. Ohira, B. Komiyama and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," in IEEE Transactions on Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005
- [Ji21]** Z. Ji et al., "Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 1030-1034, Jan. 2021

[Li23] H. Li, L. Chen, T. Lu and A. Hu, "Angular-domain Secret Key Generation for RIS-aided mmWave MIMO systems," 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), Hong Kong, Hong Kong, 2023, pp. 1-6, doi: 10.1109/VTC2023-Fall60731.2023.10333834.

[Vogt19] H. Vogt, Z. H. Awan and A. Sezgin, "Secret-Key Generation: Full-Duplex Versus Half-Duplex Probing," in IEEE Transactions on Communications, vol. 67, no. 1, pp. 639-652, Jan. 2019

[Luo23] H. Luo, N. Garg and T. Ratnarajah, "A Channel Frequency Response-Based Secret Key Generation Scheme in In-Band Full-Duplex MIMO-OFDM Systems," in IEEE Journal on Selected Areas in Communications, vol. 41, no. 9, pp. 2951-2965, Sept. 2023

[Ruotsalainen20] H. Ruotsalainen, J. Zhang and S. Grebeniuk, "Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1745-1755, March 2020

Abkürzungen

| | |
|---------|--|
| RKD | Radio-signal Key Distribution |
| SDR | Software Defined Radio |
| PLKG | Physical Layer Key Generation |
| QKD | Quantum Key Distribution |
| RSSI | Received Signal Strength Indicator |
| RSS | Received Signal Strength |
| IoT | Internet of Things |
| LoRa | Long Range |
| LoRaWAN | Long Range Wide Area Network |
| MIMO | Multiple-Input-Multiple-Output |
| IRS | Intelligent Reflecting Surface |
| LDPC | Low Density Parity Check |
| BCH | Bose-Chaudhuri-Hocquenghem |
| DCT | Discrete Cosine Transformation |
| LOESS | Locally Estimated Scatterplot Smoothing |
| FFT | Fast Fourier Transform |
| AES | Advanced Encryption Standard |
| SNR | Signal-to-Noise Ratio |
| RF | Radio Frequency |
| OFDM | Orthogonal Frequency Division Multiplexing |

insitu software gmbH

Heinrich Schneidmadl Strasse 15

3100 St. Pölten

+43 676 433 7123

piller@insitu.software