WHZ Westsächsische Hochschule Zwickau
Hochschule für Mobilität

Diplomarbeit

Analyse zum Thema KFZ-Diebstahl & Prävention: Sicherheitsrisiko durch Keyless-Systeme

eingereicht an der Fakultät Kraftfahrzeugtechnik
der Westsächsischen Hochschule Zwickau
zur Erlangung des akademischen Grades eines

Diplomingenieurs (FH)

vorgelegt von: cand. Ing. **Mosch, Laurenz**
geboren am: 05.02.2002

Studiengang: Kraftfahrzeugtechnik
Studienschwerpunkt: Instandhaltung und Unfallanalyse

Erstbetreuer: Prof. Dr. Klaus Dieter Brösdorf
Zweitbetreuer: Prof. Dr.-Ing. Lutz Nagel

WHZ Fakultät Elektrotechnik

Selbstständigkeitserklärung zur Abschlussarbeit

Thema: Analyse zum Thema KFZ-Diebstahl & Prävention: Sicherheitsrisiko durch Keyless-Systeme

Name: Mosch Vorname: Laurenz

Matrikel-Nr.: 41834 Seminargruppen-Nr.: 202235/KIU

Hiermit versichere ich, dass ich die vorliegende Arbeit in allen Teilen selbstständig angefertigt und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel benutzt habe sowie dass ich die Arbeit in gleicher oder ähnlicher Form in noch keiner anderen Prüfung vorgelegt habe. Mir ist bewusst, dass ich Autor/in der vorliegenden Arbeit bin und die volle Verantwortung für den Text trage.	☒
Ich erkläre, dass ich wörtlich oder sinngemäß aus anderen Werken – dazu gehören auch Internetquellen – übernommene Inhalte als solche kenntlich gemacht und die entsprechenden Quellen angegeben habe.	☒
Mir ist bewusst, dass meine Arbeit auf Plagiate überprüft werden kann. Mir ist bekannt, dass es sich bei der Abgabe eines Plagiats um ein schweres akademisches Fehlverhalten handelt und dass Täuschungen nach der für mich gültigen Prüfungsordnung geahndet werden können.	☒
Zusätzlich versichere ich, dass ich auf künstlicher Intelligenz (KI) basierende Werkzeuge nur in Absprache mit den Prüfern verwendet habe. Dabei stand meine eigene geistige Leistung im Vordergrund und ich habe jederzeit den Prozess steuernd bearbeitet.	☒
Diese Werkzeuge habe ich im Quellenverzeichnis in der Rubrik „Übersicht verwendeter Hilfsmittel" mit ihrem Produktnamen und einer Übersicht des im Rahmen dieser Prüfungs-/Studienarbeit genutzten Funktionsumfangs unter Angabe der Textstelle in der Arbeit vollständig aufgeführt.	☒
Ich versichere, dass ich keine KI-basierten Tools verwendet habe, deren Nutzung die Prüfer explizit schriftlich ausgeschlossen haben. Ich bin mir bewusst, dass die Verwendung von Texten oder anderen Inhalten und Produkten, die durch KI-basierte Tools generiert wurden, keine Garantie für deren Qualität darstellt.	☒
Ich verantworte die Übernahme jeglicher von mir verwendeter maschinell generierter Passagen vollumfänglich selbst und trage die Verantwortung für eventuell durch die KI generierte fehlerhafte oder verzerrte Inhalte, fehlerhafte Referenzen, Verstöße gegen das Datenschutz- und Urheberrecht oder Plagiate.	☒

Nossen, 02.10.2025
Ort, Datum

Unterschrift

Inhaltsverzeichnis

I. Abbildungsverzeichnis III
II. Tabellenverzeichnis IV
III. Abkürzungsverzeichnis V
IV. Formelverzeichnis VI
1 Einleitung 1
2 Übergang von mechanischen zu elektronischen Sicherheitssystemen 2
3 Statistiken und Fakten zu KFZ-Diebstählen 8
3.1 Nationale Zahlen der letzten Jahre 8
3.2 Häufig betroffene Fahrzeugtypen und Regionen 10
4 Moderne Sicherheitssysteme in Fahrzeugen 12
4.1 Elektronische Wegfahrsperren 12
4.2 Fahrzeugschlüssel 16
4.3 Keyless-Go-System 17
5 Angriffe auf schlüssellose Zugangssysteme 25
6 Versuche zu Relay-Angriffen auf Keyless-Systeme 27
6.1 Versuchskonzeption 27
6.2 Relay-System Aufbau 30
6.3 Versuchsvorbereitung 34
6.4 Versuchsdurchführung 35
6.5 Versuchsergebnisse und Auswertung 50
7 Fehlerbetrachtung 55
8 Präventionsmaßnahmen und Zukunftsperspektiven 57
8.1 Technologische Gegenmaßnahmen gegen moderne Diebstahl-methoden 57
8.2 Aktuelle Trends der Fahrzeugüberwachung und Diebstahlprävention 61
9 Fazit 64
V. Literaturverzeichnis 66
VI. Anlagen 69

I. Abbildungsverzeichnis

Abbildung 1: Slim Jim 2
Abbildung 2: Einsatz von Montagekissen 3
Abbildung 3: Bestandteile Fahrzeugschlüssel 4
Abbildung 4: Beispiel Boardnetzwerk 5
Abbildung 5: Key Programmer 6
Abbildung 6: Statistik GDV wirtschaftlicher Schaden 9
Abbildung 7: Statistik GDV Anzahl der Diebstähle von PKW in Deutschland 10
Abbildung 8: Funktionsweise RFID 14
Abbildung 9: Schematische Funktionsweise Rolling Code 15
Abbildung 10: Aufbau Keyless Türgriff 18
Abbildung 11: Funktionsweise Timo of Fligh 20
Abbildung 12: Entfernung in Abhängigkeit von ToF 22
Abbildung 13: Beispiel RSA [18] 26
Abbildung 14: Relay-System Vorderseite 30
Abbildung 15: Relay-System Rückseite 30
Abbildung 16: Transmitter 33
Abbildung 17: Receiver 33
Abbildung 18: V01 - Audi A5 37
Abbildung 19: V02 - BMW X1 38
Abbildung 20: V03 - Renault Captur 39
Abbildung 21: V04 - Ford Kuga 41
Abbildung 22: V05 - Mercedes Benz CLS 400d 42
Abbildung 23: V06 - Mercedes Benz E 300d 43
Abbildung 24: V07 - Mercedes Benz R 320 CDI 45
Abbildung 25: V08 - Skoda Kodiaq 46
Abbildung 26: V09 - Seat Cupra Leon SP 47
Abbildung 27: V10 - Toyota Corolla 49
Abbildung 28: Darstellung Ergebnisse aus Versuch 50
Abbildung 29: Einteilung in Schutzlevel 51
Abbildung 30: Vergleich UWB in Bezug auf Relay-Angriff 54
Abbildung 31: Beispiel digitaler Fahrzeugschlüssel 60
Abbildung 32: Funktionsweise Blockchain-Technologie 62

II. Tabellenverzeichnis

Tabelle 1: Statistik GDV Häufigkeit KFZ-Diebstahl bestimmter Fahrzeugherstellern 11
Tabelle 2: Statistik GDV Häufigkeit KFZ-Diebstahl bestimmter deutschen Regionen11
Tabelle 3: Entfernung in Abhängigkeit von ToF.....22
Tabelle 4: Darstellung von Fahrzeugherstellern und Ihren Keyless – Systemen 24
Tabelle 5: technische Daten Transmitter.....31
Tabelle 6: techn. Daten Receiver 32

III. Abkürzungsverzeichnis

AU	Abgasuntersuchung
BLE	Bluetooth Low Energy
bzw.	beziehungsweise
c	Lichtgeschwindigkeit
CAN	Controller Area Network
CAR2X/C2X	Car to Everything
C2C	Car to Car
C2I	Car to Infrastructure
CAS	Car Access System
ESP	Elektronisches Stabilitätsprogramm
FIN	Fahrzeugidentnummer
GHz	Gigahertz
HU	Hauptuntersuchung
HSM	Hardware-Sicherheitsmodul
LF	Low Frequency
m	Meter
Mio.	Millionen
NFC	Nahfeldkommunikation
ns	Nanosekunden
OBD	On-Board-Diagnose
Pkw	Personenkraftwagen
RFID	Radio Frequency Identification
RSA	Relay-Station-Attack
s	Sekunde
ToF	Time-of-Flight
UHF	Ultra High Frequency
UWB	Ultrawideband
z.B.	zum Beispiel

IV. Formelverzeichnis

Formel 1: $ToF = \frac{T_{loop} - T_{reply}}{2}$

Formel 2: $Distanz = ToF \cdot c$

1 Einleitung

Mit dem Fortschritt der Fahrzeugvernetzung und der zunehmenden Integration elektronischer Komfortsysteme haben sich auch die Anforderungen an die Fahrzeugsicherheit wesentlich verändert. Besonders schlüssellose Zugangssysteme wie zum Beispiel Keyless-Go gehören mittlerweile zur serienmäßigen Ausstattung vieler Fahrzeuge und ermöglichen den Zugang sowie die Inbetriebnahme des Fahrzeuges ohne aktive Bedienung des Schlüssels. Die Authentifizierung erfolgt hierbei durch einen drahtlosen Kommunikationsvorgang zwischen Fahrzeug und einem Transponder im Fahrzeugschlüssel.

Parallel zu dieser Entwicklung haben sich auch die Methoden des Fahrzeugdiebstahls gewandelt. Klassische mechanische Angriffe wurden zunehmend durch elektronische Manipulationen ersetzt. Eine zentrale Rolle spielen hierbei Relay-Angriffe, bei denen die Funkverbindung zwischen Fahrzeug und Schlüssel durch elektronische Mittel verlängert wird. Auf diese Weise lässt sich ein unautorisierter Zugang ermöglichen, obwohl sich der Originalschlüssel außerhalb der Reichweite des Fahrzeuges befindet. Solche Angriffe erfordern keine physische Beschädigung des Fahrzeuges und hinterlassen häufig keine sichtbaren Spuren.

Die vorliegende Arbeit verfolgt das Ziel, die Funktionsweise schlüsselloser Zugangssysteme systematisch zu analysieren, sicherheitstechnische Schwachstellen zu identifizieren und die praktische Anfälligkeit gegenüber Relay-Angriffen unter realitätsnahen Bedingungen zu untersuchen. Ergänzend dazu wird ein Überblick über die historische Entwicklung des Fahrzeugdiebstahls sowie über bestehende und zukünftige präventive Maßnahmen gegeben, um die sicherheitstechnische Relevanz der Thematik im gesamtgesellschaftlichen und technischen Kontext zu verdeutlichen.

Im Rahmen einer experimentellen Versuchsreihe wurden zehn Serienfahrzeuge unterschiedlicher Hersteller und Baujahre mit einem auf handelsüblichen Komponenten basierenden Relay-Gerät getestet. Der Fokus der Untersuchung liegt dabei auf der praktischen Durchführbarkeit des Angriffs, der Identifikation von Einflussfaktoren sowie der Einordnung der Ergebnisse in den aktuellen Stand von Forschung und Entwicklung.

2 Übergang von mechanischen zu elektronischen Sicherheitssystemen

In den letzten Jahrzehnten hat sich die Methode des KFZ-Diebstahls in Abhängigkeit von technologischen Entwicklungen und Sicherheitsmaßnahmen erheblich verändert. In den 1970er und 1980er Jahren dominierten mechanische Diebstahlmethoden. Täter manipulierten Türschlösser, brachen Fenster auf oder nutzten Slim Jims, dünne Metallwerkzeuge wie in Abbildung 1 dargestellt, um Türverriegelungen zu entriegeln.

Abbildung 1: Slim Jim [2]

Die Fahrzeuge jener Zeit verfügten oft über einfache Schließsysteme ohne zusätzliche Sicherungen, was den Diebstahl unkompliziert machte. Neben den genannten Metallwerkzeugen reichten zu dieser Zeit auch Kleiderhaken oder Sägeblätter, um das Fahrzeug in Sekunden zu entriegeln, ohne Beschädigungen zu hinterlassen. Später wurden auch Montagekissen zur Hilfe genommen. Hierbei wurde, wie in Abbildung 2 zu sehen, mit Hilfe des Montagekissens der Spalt zwischen Tür und Rahmen vergrößert, um leichter mit Metallwerkzeugen oder Kleiderhaken die Tür zu entriegeln.

Abbildung 2: Einsatz von Montagekissen [3]

Mit der Einführung von Lenkradschlössern und Alarmanlagen in den 1990er Jahren wurde der Diebstahl mechanisch gesicherter Fahrzeuge erschwert. Diese Systeme erhöhten die notwendige Zeit und das Risiko für Täter erheblich, ohne jedoch eine vollständige Sicherheit zu gewährleisten. Kriminelle entwickelten Methoden, um Lenkradschlösser zu brechen oder Alarmanlagen zu deaktivieren. [4]

Die Digitalisierung der Fahrzeugtechnik brachte neue Herausforderungen mit sich. In den 1990er und frühen 2000er Jahren begannen Fahrzeughersteller elektronische Wegfahrsperren zu integrieren. Diese Systeme kombinierten Transponder im

Schlüssel (siehe Abbildung 3) mit Steuergeräten im Fahrzeug, die eine Synchronisation erforderten, um den Motor zu starten.

Abbildung 3: Bestandteile Fahrzeugschlüssel [5]

Während dies zunächst als Durchbruch in der Diebstahlsicherung galt, fanden Kriminelle Wege, diese Technologien durch Manipulation der OBD-Schnittstelle oder das Klonen von Schlüsseln zu umgehen.

Frühere mechanische Sicherheitssysteme in Kraftfahrzeugen umfassten vor allem Lenkradschlösser und Türschlösser. Diese boten zunächst einen gewissen Schutz vor unerlaubtem Eindringen, da somit eine physische Barriere geschaffen wurde, waren

jedoch leicht zu überwinden. Türschlösser konnten mit einfachen Werkzeugen wie Dietrichen, Slim Jims oder Schraubenzieher manipuliert bzw. überdreht werden, während Lenkradschlösser durch rohe Gewalt umgangen werden konnten.

Der Übergang zu elektronischen Sicherheitssystemen begann in den 1980er und 1990er Jahren. Die Weiterentwicklung der Fahrzeugtechnik führte in diesen Jahren zu einer Verschiebung von mechanischen hin zu elektronischen Angriffen. Moderne Fahrzeuge sind heute mit komplexen Bordnetzwerken ausgestattet, die zahlreiche Steuergeräte und Sensoren umfassen (siehe Abbildung 4). Diese Systeme, darunter der CAN-Bus (Controller Area Network), welcher ein Kommunikationssystem darstellt, das sowohl den Datenaustausch zwischen verschiedenen Steuergeräten im Fahrzeug ermöglicht als auch eine präzise Steuerung von Funktionen wie dem Zugangssystem, der Motorsteuerung und der Wegfahrsperre.

Abbildung 4: Beispiel Boardnetzwerk [6]

Die zunehmende Vernetzung der Fahrzeuge hat jedoch auch neue Angriffspunkte geschaffen. Kriminelle nutzen spezielle Hardware, um Steuergeräte zu manipulieren oder Kommunikationsprotokolle abzufangen. Beispiele hierfür sind das Auslesen von Schlüsseldaten über Funk oder der Einsatz von Key-Emulator, um neue Schlüssel zu programmieren bzw. zu emulieren. Für das Emulieren eines Fahrzeugschlüssels

benötigt man zum einen das Gerät, den Key Emulator wie in Abbildung 5 dargestellt, einen Hersteller-spezifischen PIN-Code zum Programmieren des Schlüssels und einige Funksignale aus der Kommunikation zwischen Fahrzeugschlüssel und Fahrzeug. Diese benötigten Funksignale können in kurzer Zeit und sehr unauffällig abgefangen werden, da hierbei die Entfernung zwischen Fahrzeugschlüssel und Emulator bis zu 20 m betragen kann. Die erforderlichen Signale sind:

- RF-Key-ID-Signal (wird gesendet sobald sich Fahrzeugschlüssel in Nähe des Fahrzeuges befindet)
- Comfort-Signal (wird vom Fahrzeug gesendet)
- Keyless-Go-Signal (durch Betätigen des Knopfes oder Türgriffsensor)

Hat man diese Funksignale mit dem Key-Emulator eingefangen und einen dazugehörigen PIN-Code für die Programmierung des Schlüssels kann man im Anschluss daran beliebig oft das Fahrzeug ver- und entriegeln oder starten. Hierbei ist der originale Fahrzeugschlüssel nicht mehr notwendig. [7]

Abbildung 5: Key Programmer [8]

Besonders die OBD-Schnittstelle, welche sich meist im linken unteren Bereich des Armaturenbrettes befindet und ursprünglich für Diagnosezwecke entwickelt wurde, hat sich als Schwachstelle erwiesen, da sie einen direkten Zugriff auf zentrale Steuergeräte ermöglicht.

Der Übergang von mechanischen zu elektronischen Sicherheitssystemen markiert einen Meilenstein in der Fahrzeugentwicklung. Während mechanische Systeme auf physikalischen Barrieren basierten, setzen elektronische Systeme auf digitale Authentifizierungsprozesse. Ein Beispiel hierfür ist die Einführung von Keyless-Go-Systemen, bei denen der Schlüssel nur noch als Sender fungiert und durch das Fahrzeug automatisch erkannt wird. Diese Systeme bieten Komfort, sind jedoch anfällig für spezifische Angriffe wie Relay-Angriffe, bei denen das Funksignal des Schlüssels verlängert wird, um das Fahrzeug zu öffnen und zu starten. Die Automobilindustrie hat auf diese Bedrohungen mit verbesserten Verschlüsselungstechniken und der Integration von Bewegungs- oder Zeitbeschränkungen reagiert. Dennoch bleibt die kontinuierliche Weiterentwicklung von Sicherheitssystemen erforderlich, um der Dynamik krimineller Innovationen entgegenzuwirken. Ein weiterer Schwachpunkt liegt in der Integration mechanischer Schlösser mit elektronischen Systemen. Bei vielen Fahrzeugen erlaubt ein mechanischer Schlüssel den Zugang zur Fahrerkabine, während die elektronische Wegfahrsperre den Motorstart verhindert. Diese hybride Konstruktion eröffnet potenzielle Angriffspunkte, da ein erfolgreicher physischer Zugang oft den Zugriff auf elektronische Systeme ermöglicht.

3 Statistiken und Fakten zu KFZ-Diebstählen

3.1 Nationale Zahlen der letzten Jahre

Die Anzahl der KFZ-Diebstähle hat in den letzten zwei Jahrzehnten weltweit eine besondere Entwicklung durchlaufen. Während in einigen Ländern ein Rückgang verzeichnet wurde, stiegen die Zahlen in anderen Regionen aufgrund technologischer Schwachstellen und organisierter Kriminalität an.

Während der politischen Sonderlage in den Jahren 2020 bis 2022 und dessen bedingten Einschränkungen war ein Rückgang der Autodiebstähle in Deutschland zu verzeichnen und somit ein Rückgang des daraus entstandenen wirtschaftlichen Schadens (siehe Abbildung 6). Mit dem Ende dieser Situation ist jedoch eine signifikante Zunahme der Diebstähle festzustellen, wie sie auch in den Berichten der Kfz-Versicherungen reflektiert werden. Im Jahr 2023 wurden insgesamt 14.585 kaskoversicherte Pkw entwendet, was im Vergleich zum Vorjahr einen Anstieg von nahezu 20 % bedeutet. Durch Autodiebstähle entstand im Jahr 2023 ein wirtschaftlicher Schaden von mehr als 310 Millionen Euro (siehe Abbildung 6). Ein markanter Trend, der die Bevorzugung höherpreisiger SUV und Oberklassemodelle durch Diebe widerspiegelt, zeigt sich auch in der durchschnittlichen Schadenhöhe. Versicherungen mussten für einen Diebstahl im Durchschnitt 21.400 Euro leisten, was im Vergleich zum Vorjahr einen Anstieg von etwa sechs Prozent darstellt. [9]

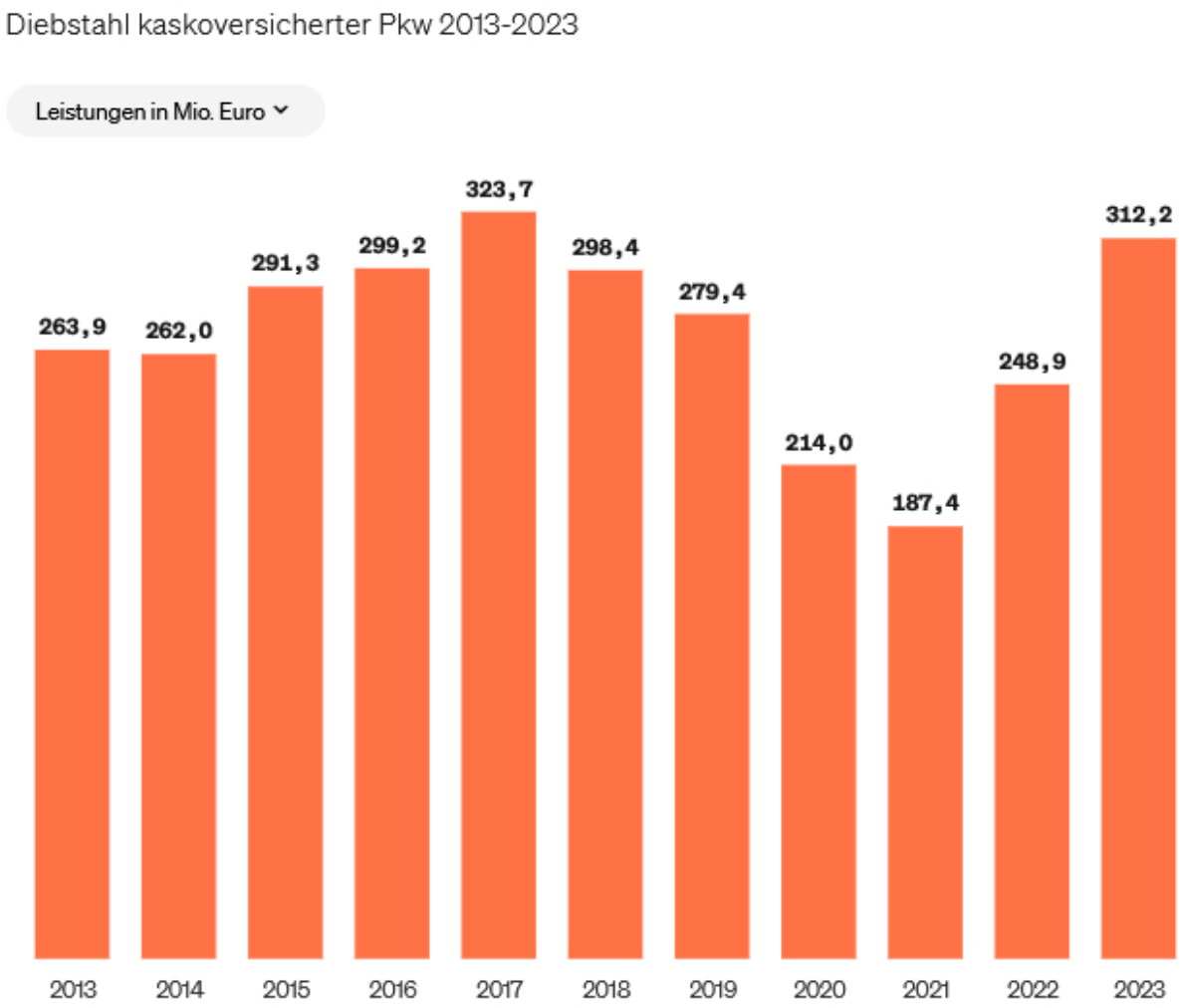


Abbildung 6: Statistik GDV wirtschaftlicher Schaden [9]

Gesellschaftlich betrachtet, tragen KFZ-Diebstähle zur Unsicherheit in der Bevölkerung bei und beeinflussen das Vertrauen in moderne Sicherheitstechnologien. Die steigende Zahl digitaler Diebstähle hat zudem Diskussionen über die Sicherheit vernetzter Fahrzeuge und die Verantwortung der Automobilhersteller angestoßen. Betrachtet man zusätzlich die Jahre vor 2000, erkennt man das Ausmaß der Einführung einer elektronischen Wegfahrsperre bei neu zugelassenen PKW, was die Sicherheit erhöhte und somit zu einem Rückgang der KFZ-Diebstähle führte. Während im Jahr 2000 noch rund 40.000 Fahrzeuge als gestohlen gemeldet wurden, lag die Zahl im Jahr 2020 bei etwa 10.000 Fällen (siehe Abbildung 7). Dieses Thema wird in Kapitel 4.1 der Arbeit näher erläutert.

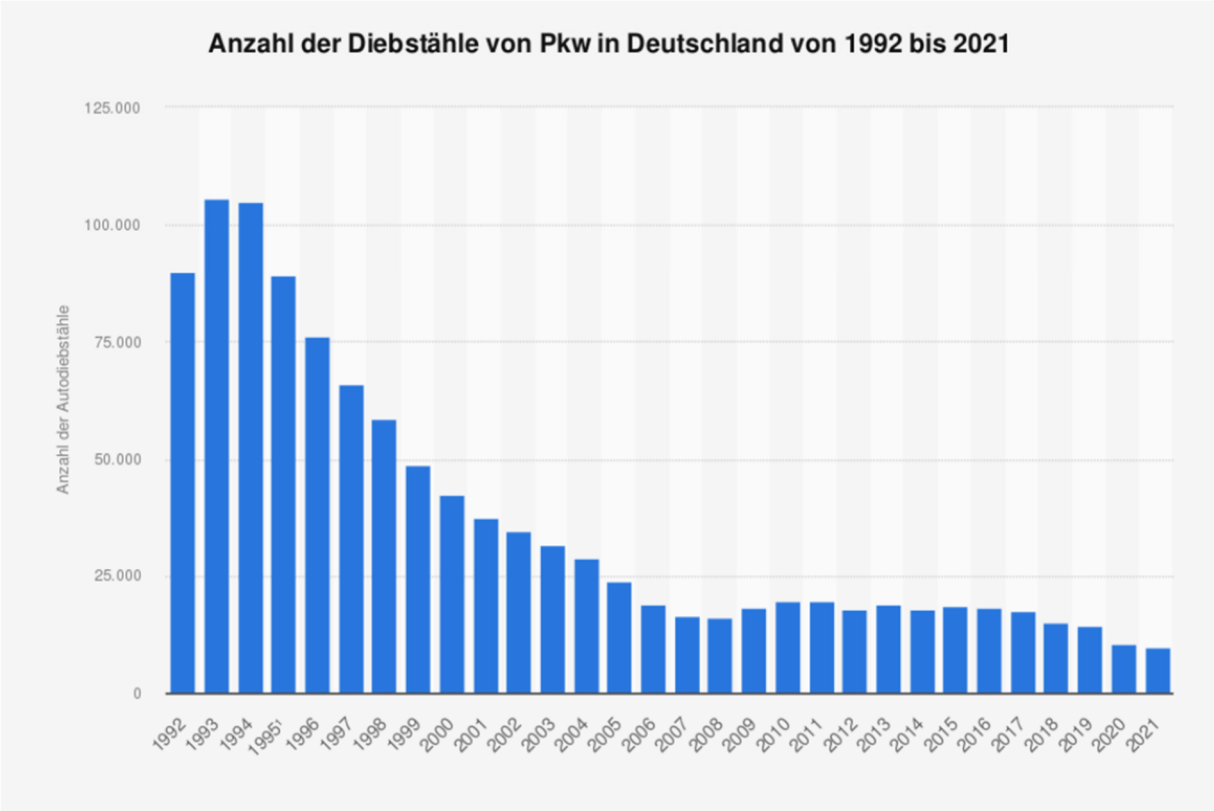


Abbildung 7: Statistik GDV Anzahl der Diebstähle von PKW in Deutschland [10]

3.2 Häufig betroffene Fahrzeugtypen und Regionen

Die Präferenz der Diebe richtet sich oft nach Fahrzeugtyp und Region. In Europa sind deutsche Marken wie Audi, BMW, Mercedes-Benz und Volkswagen besonders begehrt (siehe Tabelle 1). In Tabelle 1 ist deutlich zu erkennen, dass die Fahrzeugmarken Audi, BMW, Mercedes-Benz und Volkswagen deutlich höhere Diebstahlzahlen aufweisen als alle anderen Marken. Während die Anzahl der Diebstähle von der Fahrzeugmarke Ford bei 840 lagen, weisen Fahrzeugmarken wie BMW, Audi, Mercedes-Benz und Toyota Diebstahlfälle über 1000 auf. Hier ist zusätzlich ein großer Sprung zwischen Toyota mit 1475 und VW mit 1810 gemeldeten Diebstählen. Dies liegt nicht nur an ihrem hohen Wiederverkaufswert, sondern auch an der internationalen Nachfrage nach Ersatzteilen. SUV und Elektrofahrzeuge sind zunehmend Ziel von Diebstählen, da sie durch den hohen Marktwert und der technischen Ausstattung besonders attraktiv für Diebstähle sind.

Tabelle 1: Statistik GDV Häufigkeit KFZ-Diebstahl bestimmter Fahrzeugherstellern [9]

		Häufigkeit Pkw-Diebstähle	
Platz	Marke[1]	Anzahl	Veränderung gg. Vorjahr
1	Volkswagen-VW	1.810	-7,4%
2	Toyota (inkl. Lexus)	1.475	115,0%
3	Audi AG	1.377	-2,1%
4	Mercedes-Benz	1.287	13,3%
5	BMW (inkl. Mini)	1.171	8,3%
6	Hyundai	887	41,9%
7	Ford/Europa	840	34,8%
8	Kia Motor	724	155,8%

Regionale Unterschiede zeigen, dass urbane Zentren und Grenzregionen besonders betroffen sind (siehe Tabelle 2). In Deutschland liegen in Berlin, Hamburg und Brandenburg die Schwerpunkte von KFZ-Diebstählen. Ähnliche Muster lassen sich in anderen Ländern beobachten, wobei Metropolregionen aufgrund der höheren Fahrzeugdichte und der Anonymität des städtischen Umfelds bevorzugt werden.

Tabelle 2: Statistik GDV Häufigkeit KFZ-Diebstahl bestimmter deutschen Regionen [9]

	Diebstahlquote	Pkw-Diebstähle		Schaden pro Diebstahl	
Bundesland	pro 10.000[2]	Anzahl	Veränderung gg. Vorjahr[1]	in EUR	Veränderung gg. Vorjahr[1]
Berlin	42	4.266	45,9%	22.484 €	-
Hamburg	13	853	-3,1%	23.706 €	+
Brandenburg	11	1.325	20,7%	23.160 €	+
Sachsen	4	652	24,2%	19.017 €	-
Sachsen-Anhalt	4	375	-3,8%	21.465 €	+
Bremen	4	110	1,9%	20.439 €	+
Nordrhein-Westfalen	3	2.915	12,2%	19.815 €	+

4 Moderne Sicherheitssysteme in Fahrzeugen

4.1 Elektronische Wegfahrsperren

Die Einführung der elektronischen Wegfahrsperre in Kraftfahrzeugen ist eng mit der sicherheitstechnischen Weiterentwicklung auf Anregung der Versicherungswirtschaft verbunden. Insbesondere das Allianz Zentrum für Technik (AZT), das ingenieurtechnische Prüflabor der Allianz Versicherungsgruppe, trieb in den späten 1980er und frühen 1990er Jahren die Entwicklung praxisnaher Maßnahmen zur Reduktion von Fahrzeugdiebstählen maßgeblich voran. Anlass hierfür war der deutliche Anstieg der polizeilich erfassten Kfz-Diebstähle in Deutschland, insbesondere in urbanen Räumen sowie im Kontext der deutschen Wiedervereinigung, was einen verstärkten Bedarf an diebstahlhemmenden Systemen zur Folge hatte. [25, 26]

Im Zuge dieser Entwicklung wurde die elektronische Wegfahrsperre als technologiegestützte Diebstahlverhinderungsmaßnahme konzipiert. Sie löste die bis dahin vorherrschenden mechanischen Sicherungselemente wie Lenkradsperren und Zündschlossverriegelung schrittweise ab, da diese mit entsprechendem Werkzeug leicht zu überwinden waren. Die ersten serienmäßigen Systeme wurden in Deutschland ab etwa 1991 verbaut, zunächst vornehmlich in Oberklassefahrzeugen. Bereits Mitte der 1990er Jahre fand eine sukzessive Integration in volumenstärkere Segmente der Fahrzeugklassen statt. Am 1.Januar 1998 trat schließlich eine gesetzliche Verpflichtung zum Einbau elektronischer Wegfahrsperren für alle neu zugelassenen Personenkraftwagen in Kraft, wodurch eine einheitliche Sicherheitsbasis im Markt geschaffen wurde. [11]

Straßenverkehrs-Zulassungs-Ordnung (StVZO)

§ 38a Sicherungseinrichtungen gegen unbefugte Benutzung von Kraftfahrzeugen [12]

(1) Personenkraftwagen sowie Lastkraftwagen, Zugmaschinen und Sattelzugmaschinen mit einem zulässigen Gesamtgewicht von nicht mehr als 3,5 t – ausgenommen land- oder forstwirtschaftliche Zugmaschinen und Dreirad-Kraftfahrzeuge – müssen mit einer Sicherungseinrichtung gegen unbefugte Benutzung, Personenkraftwagen zusätzlich mit einer Wegfahrsperre ausgerüstet sein. Die

Sicherungseinrichtung gegen unbefugte Benutzung und die Wegfahrsperre müssen den im Anhang zu dieser Vorschrift genannten Bestimmungen entsprechen.

(2) Krafträder und Dreirad-Kraftfahrzeuge mit einem Hubraum von mehr als 50 ccm oder einer durch die Bauart bestimmten Höchstgeschwindigkeit von mehr als 45 km/h, ausgenommen Kleinkrafträder und Fahrräder mit Hilfsmotor (§ 3 Absatz 2 Satz 1 Nummer 1 Buchstabe d der Fahrzeug-Zulassungsverordnung), müssen mit einer Sicherungseinrichtung gegen unbefugte Benutzung ausgerüstet sein, die den im Anhang zu dieser Vorschrift genannten Bestimmungen entspricht.

(3) Sicherungseinrichtungen gegen unbefugte Benutzung und Wegfahrsperren an Kraftfahrzeugen, für die sie nicht vorgeschrieben sind, müssen den vorstehenden Vorschriften entsprechen.

Das Grundprinzip basiert auf der Verknüpfung von Schlüssel und Steuergerät. Ein im Schlüssel integrierter Transponder, meist ein RFID-Chip, sendet bei der Zündung ein codiertes Signal an das Steuergerät. Nur wenn der Code übereinstimmt, wird der Motorstart freigegeben. Die Wegfahrsperre wird nach Abschaltung der Zündung automatisch aktiviert. RFID entspricht einer Identifizierung über elektronische Wellen. Dies fand bereits im Zweiten Weltkrieg Anwendung, um zwischen Feind und Freund zu unterscheiden oder heutzutage in Kleidungs- oder Alkoholgeschäften zur Sicherung der Ware. RFID basiert auf der Nutzung von elektromagnetischen Feldern, die zwischen einem Lesegerät und einem RFID-Tag oder Transponder ausgetauscht werden (siehe Abbildung 8).

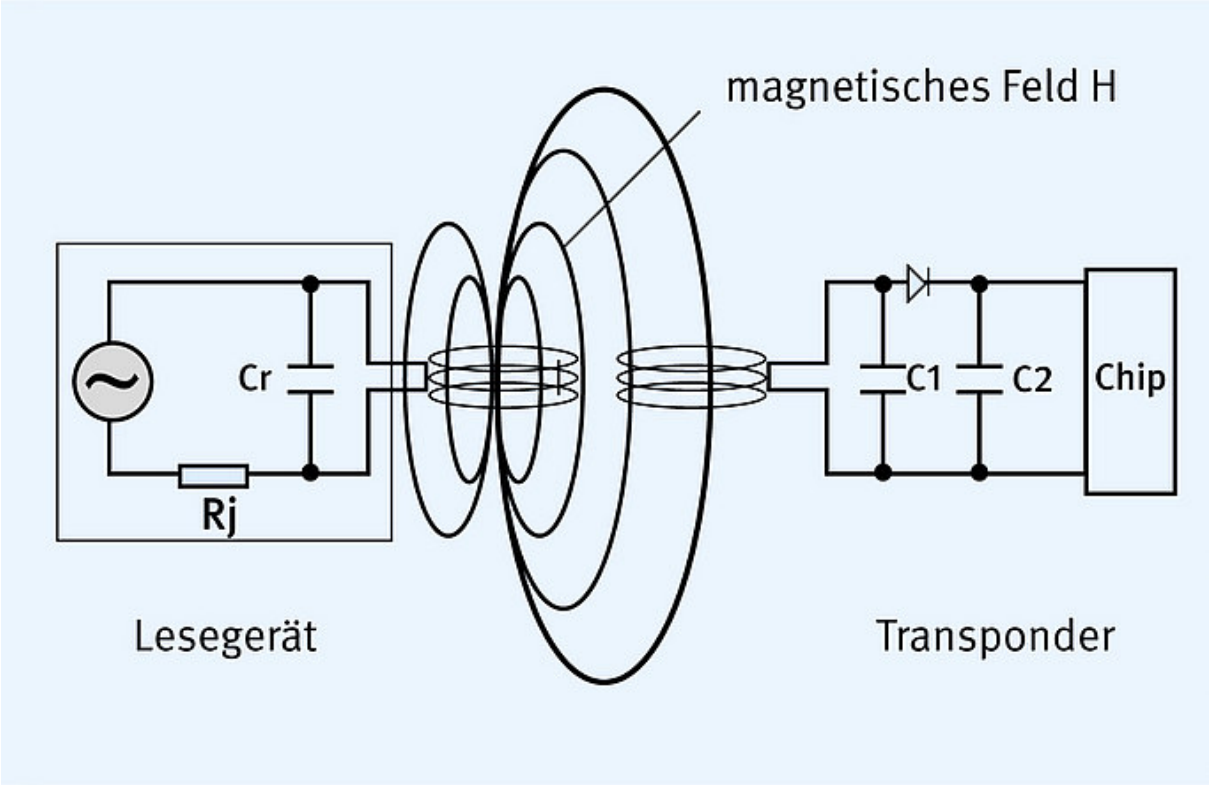


Abbildung 8: Funktionsweise RFID [13]

In einem RFID-Tag befinden sich ein Mikrochip, welcher gespeicherte Informationen, beispielsweise eine eindeutige Identifikationsnummer, enthält und eine Antenne, die Daten vom Chip an das Lesegerät überträgt. Wenn ein RFID-Tag in die Nähe eines Lesegerätes gelangt, wird es durch das elektromagnetische Feld mit Energie versorgt, sodass der Chip die gespeicherten Daten an das Lesegerät senden kann. Ein Vorteil hierbei ist die berührungslose und schnelle Datenübertragung, welche jedoch unter Umständen abgefangen und manipuliert werden kann.

Die erste Generation von Wegfahrsperren arbeitete in den meisten Fällen nach dem Prinzip der Dreikreis-Unterbrechung (Zündung, Treibstoffzufuhr und Anlasser), was jedoch nur einen mäßigen Schutz bietet und für Diebe leicht durch Überbrücken zu überwinden war. Bei der zweiten Generation hingegen, welche ab ca. 1994 eingesetzt wurden, arbeiten diese Wegfahrsperren nicht mehr mit der Dreikreisunterbrechung, sondern erteilen dem Motorsteuergerät über eine elektronische Kommunikation eine Freigabe, ohne die der Motor nicht startet. Diese Kommunikation erfolgt meist über das Fahrzeug-Bussystem und ist verschlüsselt. Die benutzten RFID-Chips in den Schlüsseln sind in den meisten Fällen einfache Read-Only-Transponder, wie sie auch zur Kennzeichnung von Tieren verwendet werden und nur eine feste bzw. zugeordnete

Seriennummer zyklisch im Klartext senden. Die Wegfahrsperre selbst kann hierbei ein eigenständiges Steuergerät oder auch in ein anderes integriert sein, etwa im Kombiinstrument oder dem Boardcomputer. Bei aktuellen Wegfahrsperren der dritten Generation findet eine Kommunikation zwischen RFID-Transponder und Wegfahrsperre zur Authentifizierung des berechtigten Fahrers anhand seines Schlüssels kryptographisch statt. In einigen Systemen werden zusätzlich weitere Steuergeräte wie Motorsteuergerät (ECM) einbezogen, um die Authentifizierung abzusichern z.B. das Nissan Anti-Theft System (NATS). Moderne Systeme verwenden also verschlüsselte Kommunikationsprotokolle, um die Sicherheit zu erhöhen. Zusätzlich ist der Code beim Rolling-Code-Verfahren häufig dynamisch und ändert sich bei jeder Nutzung. Hierbei gehen, wie in Abbildung 9 simuliert dargestellt, Sender und Empfänger systematisch eine definierte Tabelle von Codes durch. Der Code zur Authentifizierung wechselt nach jedem Befehl bzw. nach jeder Datenübertragung und führt zu einer Ungültigkeit des letzten Codes. Trotz dieser Maßnahmen bleibt die elektronische Wegfahrsperre anfällig für Angriffe wie das Code Grabbing, bei dem der Code während der Übertragung abgefangen wird. [1, 14]

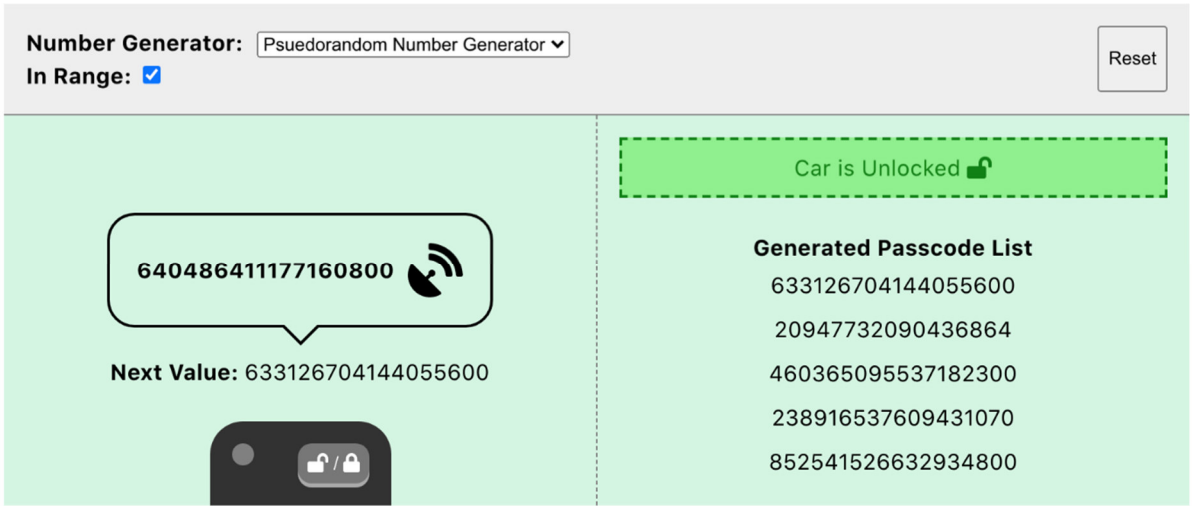


Abbildung 9: Schematische Funktionsweise Rolling Code [14]

4.2 Fahrzeugschlüssel

Kontaktlose Fahrzeugschlüssel stellen eine zentrale Komponente moderner Fahrzeugsicherheitssysteme dar und sind integraler Bestandteil der serienmäßigen Ausstattung zahlreicher aktueller Fahrzeugmodelle. Sie ermöglichen einen komfortablen, schlüssellosen Zugang zum Fahrzeug sowie die Inbetriebnahme dessen und tragen dabei maßgeblich zur Zugangssicherung gegenüber unbefugten Dritten bei. Die technologische Grundlage dieser Systeme bildet der Einsatz drahtloser Kommunikationstechnologien, insbesondere Radio Frequency Identification (RFID) und Bluetooth Low Energy (BLE). RFID-basierte Systeme operieren in der Regel über die Nahfeldkommunikation (NFC) und erlauben eine Kommunikation zwischen Schlüssel und Fahrzeug nur innerhalb eines sehr begrenzten Entfernungsbereichs von wenigen Zentimetern. BLE-basierte Lösungen hingegen ermöglichen eine deutlich größere Reichweite von mehreren Metern, wodurch Funktionen wie Passive Entry und Passive Start realisiert werden können. In beiden Fällen ist der Fahrzeugschlüssel mit einem Mikrochip ausgestattet, auf dem ein eindeutiger Authentifizierungscode gespeichert ist. Dieser Code wird bei Annäherung an das Fahrzeug über ein drahtloses Signal vom Steuergerät empfangen und mit dem im Fahrzeug hinterlegten Referenzwert abgeglichen. Erst bei Übereinstimmung erfolgt die Freigabe des Zugangssystems bzw. der Startfunktion.

Mit dem Aufkommen digitaler Mobilitätslösungen werden vermehrt auch Smartphones in die Rolle eines digitalen Schlüssels eingebunden. Diese Funktionalität wird durch spezifische Anwendungen (Apps) realisiert, in denen digitale Schlüssel in Form kryptographisch gesicherter Zertifikate gespeichert sind. Dabei werden hochsensible Informationen wie die Fahrzeugidentifikationsnummer (FIN), Zugangscodes, benutzerspezifische Sicherheitsprotokolle, teilweise auch Kilometerstände sowie Zeitstempel gespeichert. Diese Informationen werden sowohl im Fahrzeug als auch im physischen Schlüssel oder dem mobilen Endgerät vorgehalten. Um unbefugten Zugriff zu verhindern, erfolgt die Speicherung grundsätzlich unter Anwendung kryptografischer Verfahren, insbesondere durch symmetrische oder asymmetrische Verschlüsselungstechnologien.

Die im Fahrzeug gespeicherten Zugangsdaten befinden sich in der Regel in verschiedenen elektronischen Steuergeräten (ECU), welche über das CAN-Bus miteinander vernetzt sind. Diese netzwerkbasierte Architektur erlaubt eine flexible Steuerung fahrzeuginterner Funktionen, stellt jedoch auch eine potenzielle Angriffstelle für sicherheitsrelevante Manipulationen dar. Angreifer könnten versuchen durch physische Zugriffe, z.B. über die OBD-Schnittstelle oder drahtlose Kommunikationskanäle, beispielsweise durch Funkverlängerung, Zugriff auf sicherheitskritische Daten zu erlangen oder diese zu manipulieren.

Als Reaktion auf diese Angriffspotenziale werden in modernen Fahrzeugsystemen zunehmend spezielle Sicherheitskomponenten implementiert. Hierzu zählen unter anderem isolierte Sicherheitschips (Secure Elements) sowie Hardware Security Module (HSM). Letztere zeichnen sich durch eine hardwarebasierte Implementierung kryptografischer Funktionen aus und dienen der sicheren Speicherung und Verarbeitung vertraulicher Informationen. Durch diese Maßnahmen wird der Widerstand des Systems gegenüber unautorisierten Zugriffen signifikant erhöht. In der Gesamtheit verdeutlicht sich somit, dass kontaktlose Fahrzeugschlüssel nicht nur ein Komfortmerkmal darstellen, sondern zugleich ein hochkomplexes sicherheitstechnisches Element im Spannungsfeld zwischen Benutzerfreundlichkeit und Angriffssicherheit bilden. [1]

4.3 Keyless-Go-System

Keyless-Go beschreibt ein System, bei dem ein Fahrzeug ohne aktive Benutzung des Autoschlüssels (also "keyless", zu Deutsch "schlüssellos") zu entriegeln und durch das bloße Betätigen des Startknopfes zu starten ist. Ermöglicht wird dies durch einen Keyless-Go-Schlüssel mit Chip, welchen der Fahrzeugführer mit sich führt. Sobald sich eine Hand dem Türgriff eines mit Keyless-Go ausgestatteten Fahrzeugs bis auf wenige Zentimeter nähert, wird das System mit Hilfe eines kapazitiven oder optischen Näherungssensor im Türgriff (siehe Abbildung 10) aus dem Sleep-Mode geweckt und über mehrere im Fahrzeug verteilte Antennen ein codiertes Anfragesignal mit einer LF-Frequenz von 125 bzw. 130 kHz ausgesendet.

Abbildung 10: Aufbau Keyless Türgriff [15]

Das System geht daraufhin in einen Empfangsmodus im UHF-Bereich und wartet auf Bestätigung. Ist der Schlüssel mit dem RFID-Transponder in Reichweite, empfängt dieser auf 125 kHz das Signal, decodiert es und sendet dieses mit einer neuen Codierung im UHF-Frequenzband wieder aus. Hierbei wird das Signal wiederum von einem Steuergerät im Fahrzeug decodiert. Da das Keyless-Go-Steuergerät beide Codiertabellen kennt, kann es die eigene ursprüngliche Aussendung mit dem gerade empfangenen Signal vergleichen. Gibt es innerhalb einer definierten Zeit keine korrekte Antwort, passiert nichts und das System schaltet wieder auf Standby. Ein Ziehen am Türgriff hat hierbei keine Wirkung, da der Zustand des Türschlosses vom Keyless-Go-System nicht verändert wurde. Stimmen jedoch beide Codes überein, bewirkt dies eine Authentisierung. Das System gibt somit das Türschloss frei und ein Ziehen am Türgriff öffnet die Tür. Alternativ kann das Fahrzeug auch mit dem Fahrzeugschlüssel per Fernsignal geöffnet werden. Zudem gibt es einen mechanischen Notschlüssel, mit dem sich die Fahrertür öffnen lässt. Ein Fahrzeugschlüssel eines Keyless-Fahrzeuges besteht daher aus mechanischem Schlüssel, Fernbedienung und einem RFID-Transponder. Bei aktuellen Fahrzeugen ist der elektronische Schlüssel sowohl Fernbedienung als auch Transponder.

Der Motorstartvorgang entspricht im Wesentlichen dem des Türentriegelungs-vorgangs, nur dass hierbei der Motorstart-/Startknopf betätigt wird. Entscheidend für die Funktion ist, dass der Transponder durch das Keyless-Go-Steuergerät als im Fahrzeug befindlich erkannt wird. In der Entwicklungsphase ist die Innen-Außen-Abgrenzung eine der größten Herausforderungen. So sollte der Fahrzeugführer den Schlüssel überall innerhalb des Fahrzeuges ablegen können, wobei der Schlüssel stets innen erkannt werden muss. Gleiches gilt für die Außenabgrenzung, wobei dafür

sichergestellt werden muss, dass der Schlüssel außerhalb des Fahrzeuges überall als außen erkannt wird. Sofern es der Fahrzeugbesitzer wünscht, verriegelt sich das Fahrzeug automatisch, sobald sich der Transponder im Fahrzeugschlüssel außerhalb einer bestimmten Reichweite befindet. Entsprechend den im Fahrzeug vorgegebenen Bedingungen für Größe, Position, Stromverbrauch von Antennen und Elektronik sowie zulässige Sendeenergie sind die erzielten Reichweiten gering. Dieser Effekt ist aus Sicherheitsgründen ausdrücklich gewünscht. Dieses Bedienszenario des automatischen Verriegelns ist die bei Keyless-Go-Systemen umstrittenste Funktion, weshalb diese technische Besonderheit abschaltbar ist bzw. von vielen Herstellern nicht angeboten wird. Aus diesem Grund ist bei vielen Herstellern, z.B. Mercedes-Benz, zum Verriegeln des Fahrzeuges ein kleiner Knopf oder Sensor zu betätigen, welcher sich außen am Türgriff befindet. Hierbei bestätigt ein Blinkerleuchten wie bei der üblichen Verriegelung den Verriegelungsvorgang.

Keyless-Go soll in der Lage sein, Sonderfälle zu erkennen und entsprechend darauf reagieren, beispielsweise wenn sich der Transponder im Kofferraum befindet, während der Fahrt verloren geht oder mehrere Transponder im Fahrzeug vorhanden sind. Es ist wichtig, dass das Fahrzeug nicht gestartet werden kann, wenn sich der Keyless-Go-Schlüssel außerhalb des Fahrzeuges befindet. Hierbei wurde eine maximale Überlappung zwischen detektiertem Innen- und Außenbereich von 10 cm (gemessen an der Seitenscheibe/Frontscheibe) definiert. Bei mehr als 10 cm befindet sich der Schlüssel definitiv entweder innen oder außen, wobei weniger als 10 cm eine Grauzone darstellt und die Positionserkennung des Transponders aus wirtschaftlichen Gründen falsch sein darf. So ist sichergestellt, dass in Alltagssituationen der Fahrer, vorausgesetzt er trägt den Transponder bei sich, beispielsweise sein Fahrzeug betanken und das im Innenraum sitzende Kind nicht den Motor des Fahrzeuges starten kann. Die Reichweite, der beim Keyless-Go verwendeten LF-Antennen ist begrenzt, somit kann es vorkommen, dass ein im Innenraum des Fahrzeuges befindlicher Transponder als "nicht im Fahrzeug vorhanden" detektiert wird. Ebenso kann er z.B. bei einem Cabriolet als im Fahrzeug befindlich detektiert werden, obwohl er sich auf dem Fahrzeugdach befindet. Dieses Phänomen des toten Winkels erklärt sich indirekt aus den vorhergehenden Erklärungen. [1, 15]

Moderne Systeme setzen auf Ultra-Wideband-Technologie zur präzisen Abstandsmessung. Die UWB-Technologie basiert auf dem IEEE-Standard 802.15.4z [17] und bestimmt mittels Impulsfunk die relative Position von Peer-Geräten mit sehr hoher Genauigkeit. Sobald ein Gerät, welches mit einem UWB-Radio ausgestattet ist, zum Beispiel ein Smart Key, in die Reichweite eines anderen UWB-Gerätes gelangt, beginnen die Geräte mit der Entfernungsmessung. Die Bestimmung der Entfernung erfolgt mithilfe von Time-of-Flight-Messungen zwischen Geräten. Die Time-of-Flight wird berechnet, indem die Zeitdauer ermittelt wird, die ein Signal für Hin- und Rückweg zwischen zwei Geräten benötigt. Dabei sendet ein initiierendes Gerät ein Signal an ein antwortendes Gerät, welches nach einer definierten Verarbeitungszeit eine Antwort übermittelt. Die gemessene Gesamtdauer dieses Signalumlaufs wird als Roundtrip-Zeit bezeichnet. Um die Time-of-Flight nun zu erhalten (siehe Formel in Abbildung 11) subtrahiert man die Verarbeitungszeit von der Roundtrip-Zeit und teilt sie durch zwei. Multipliziert man die Time-of-Flight nun mit der Lichtgeschwindigkeit in der Luft erhält man die Entfernung zwischen den beiden Geräten. Je nach Art der Anwendung (Asset-Tracking oder Gerätelokalisierung) berechnet entweder das mobile oder das feste UWB-Gerät den genauen Standort des Gerätes. Ultra-Wide-Band verwendet eine Kanalbandbreite von 500 MHz mit kurzen Impulsen von jeweils ca. 2 ns im 0,3 - 3 GHz Band. Die Bewegungen der mobilen Vorrichtung werden in Echtzeit sehr genau verfolgt und eine Positions- und Bewegungserkennung ist somit im Zentimeterbereich möglich. [16] Durch die Verwendung bzw. Einbindung von UWB in neuen KFZ-Schlüsselsystemen ist keine Reichweitenverlängerung mehr möglich.

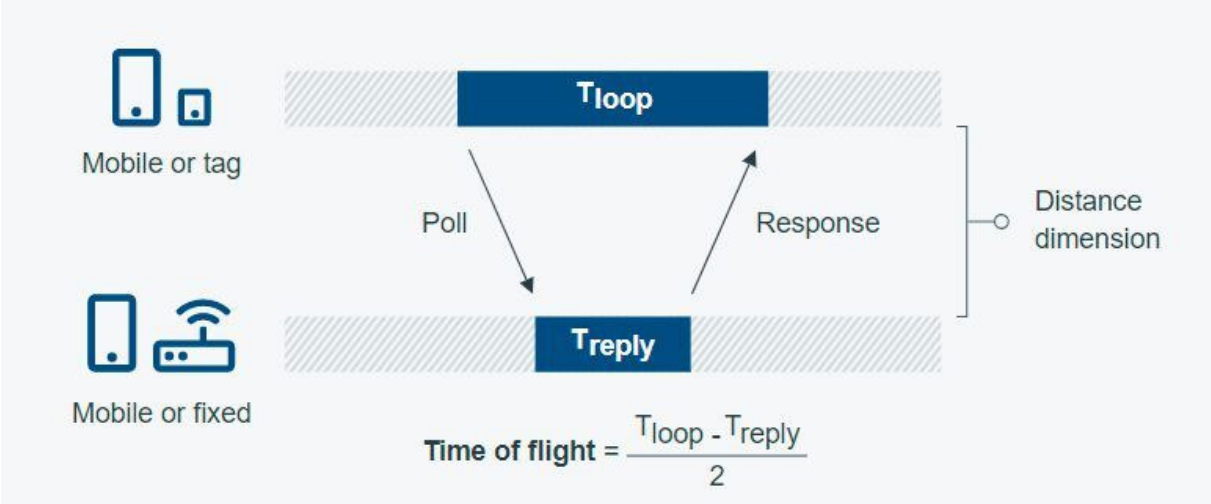


Abbildung 11: Funktionsweise Time-of-Flight [16]

Im Nachfolgenden wird eine Beispielrechnung mit fiktiven Werten durchgeführt, um die grundlegende Berechnung darzustellen, die im Hintergrund zwischen Fahrzeug und Schlüssel stattfindet.

fiktives Rechenbeispiel zur Anwendung der Formeln:

$Formel\ 1: ToF = \frac{T_{loop} - T_{reply}}{2}$

$Formel\ 2: Distanz\ = ToF\ \cdot c$

Dabei gilt:

- T_{loop} : Gesamtzeit für Hin- und Rückweg des Signals
- T_{reply} : Zeit, die der Schlüssel zur Verarbeitung des Signals benötigt
- *c* : Lichtgeschwindigkeit in Luft ≈ 299.792.458 m/s

Beispielhafte Werte:

- T_{loop} = 320 ns = 320 x 10^{-9} s
- T_{reply} = 120 ns = 120 x 10^{-9} s

Berechnung:

1. Time of Flight (ToF)

$$ToF = \frac{T_{loop} - T_{reply}}{2} = \frac{320 \times 10^{-9}\,\text{s} - 120 \times 10^{-9}\,\text{s}}{2} = \frac{200\ x\ 10^{-9}\ s}{2} = 100\ x\ 10^{-9}\ s$$

$$ToF\ = 100\ ns$$

2. Berechnung der Entfernung

Distanz = ToF *x c = 100 x* 10^{-9} s *x 299.792.458* m/s = *0,0000001* s *x 299.792.458* m/s

Distanz ≈ 29,98 m

Ergebnis:

Die berechnete Entfernung zwischen dem Fahrzeug und dem Schlüssel beträgt etwa 29,98 m.

Die Abbildung 12 zeigt den linearen Zusammenhang zwischen der Time-of-Flight (ToF) und der resultierenden Entfernung bei der Signalübertragung zwischen Fahrzeug und Funkschlüssel. Je länger die gemessene ToF, desto größer ist die ermittelte Entfernung:

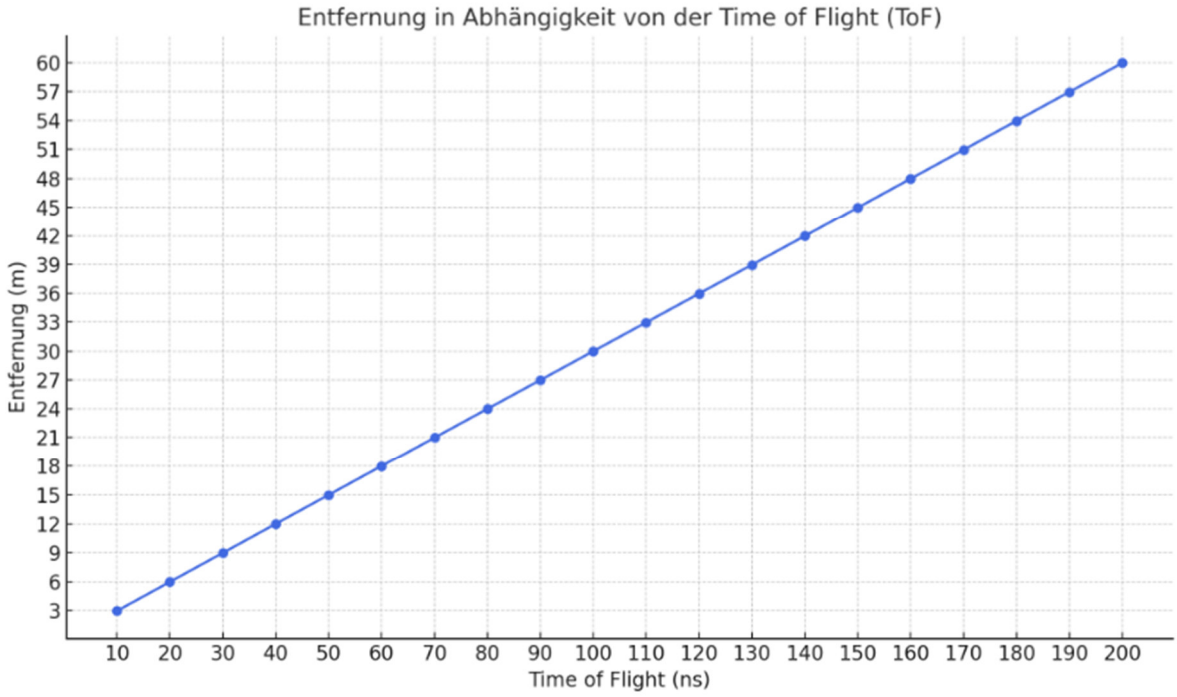


Abbildung 12: Entfernung in Abhängigkeit von ToF (eigene Darstellung)

Tabelle 3: Entfernung in Abhängigkeit von ToF (eigene Darstellung)

ToF in ns	Entfernung in m
10	3,00
40	11,99
70	20,99
100	29,98
130	38,97
160	47,96
190	56,96

Auswertung:

Die Entfernungsmessung basiert auf einer sehr kurzen Zeitdifferenz im Nanosekunden-Bereich, sodass kleinste Verzögerungen durch Signalverarbeitungen oder elektronische Manipulation, beispielsweise Relay-Angriffe, zu erheblichen Fehlern in der Entfernungsberechnung führen. So entstehen Sicherheitslücken im System, wenn ein Angreifer die ToF künstlich verlängern oder verkürzen kann, etwa durch Signalverlängerung oder Vorwegnahme. Die Lichtgeschwindigkeit als Multiplikator macht die Entfernungsmessung bereits sehr sensitiv gegen minimale zeitliche Abweichungen. Ein Unterschied von nur 1 ns entspricht fast 30 cm in der Distanzmessung. Die hohe Sensitivität gegenüber Zeitverzögerungen ist die wichtigste Schwachstelle bei schlüssellosen bzw. drahtlosen Zugangssystemen. Der Einsatz von UWB wird daher zunehmend als sicherste Methode für schlüssellose Fahrzeugzugangssysteme angesehen.

Tabelle 4: Darstellung von Fahrzeugherstellern und Ihren Keyless – Systemen (eigene Darstellung)

Hersteller	Produktname
Mercedes - Benz	Keyless Go (Keyless Entry/Go)
BMW	Komfortzugang bzw. Comfort Access
Audi	Komfortschlüssel/Keyless Entry & Go/ Advanced Key (bis Mai 2008)
Volkswagen / Škoda / Seat	Keyless Access/KESSY ("Keyless-Entry-Start-and-Exit-System")
PSA (Peugeot / Citroën)	Keyless System
Nissan	Intelligent Key
Toyota	Smart Entry & Start
Kia	Smart Key
Mitsubishi	Smart Key System
Ford	Ford Key Free-System
Renault	Keycard Handsfree Entry and Drive/ SES Smart Entry System
Volvo	Keyless Drive/Keyless Vehicle
Suzuki	Keyless Start
Aston Martin	Emotion Control Unit ECU
Mazda	LogIn (Keyless Entry)

5 Angriffe auf schlüssellose Zugangssysteme

Das Keyless-Go-System bei Fahrzeugen weist trotz seines Komfortgewinns erhebliche sicherheitstechnische Schwachstellen auf. Insbesondere gegenüber Angriffsmethoden, die auf der Ausnutzung drahtloser Funkübertragung basieren, beispielsweise Relay-Angriffe oder Störsender-Technik, erwies sich diese Technologie in ihrer ursprünglichen Implementierung als anfällig. Die zentrale Problematik liegt in der kontinuierlichen Aussendung von Authentifizierungsdaten durch den Transponder im Fahrzeugschlüssel, welcher permanent auf Abfragen des Fahrzeugsignals reagiert, ohne zusätzliche sicherheitsrelevante Bedingungen wie eine bewusste Nutzerinteraktion zu erfordern.

Ein wesentlicher Angriffspunkt ergibt sich aus der häufig fehlenden Trennung zwischen Öffnungs- und Schließbefehl. In vielen Systemen wird auf Funkeinheitscodes zurückgegriffen, die keine differenzierte Verschlüsselung oder zeitlich begrenzte Gültigkeit der übermittelten Codes implementieren. Diese Struktur erlaubt es Angreifern, mit einfachen technischen Mitteln Funksignale beim Betätigen der Verriegelungstaste abzufangen und später erneut zu übertragen. Diese Form des Angriffs wird Replay-Angriff genannt. Eine effektive Schutzmaßnahme stellt hingegen das Rolling-Code-Verfahren dar, bei dem sich die verwendeten Codes nach jeder Benutzung algorithmisch verändern. Dieses Verfahren basiert auf synchronisierten Zufallszahlgeneratoren und verhindert die Wiederverwendbarkeit abgefangener Signale.

Eine besonders große Bedrohung stellen Relay-Angriffe dar, bei denen das Signal des Schlüssels über mindestens zwei Relaisstationen in Echtzeit verlängert wird, wie in Abbildung 13 beispielhaft dargestellt.

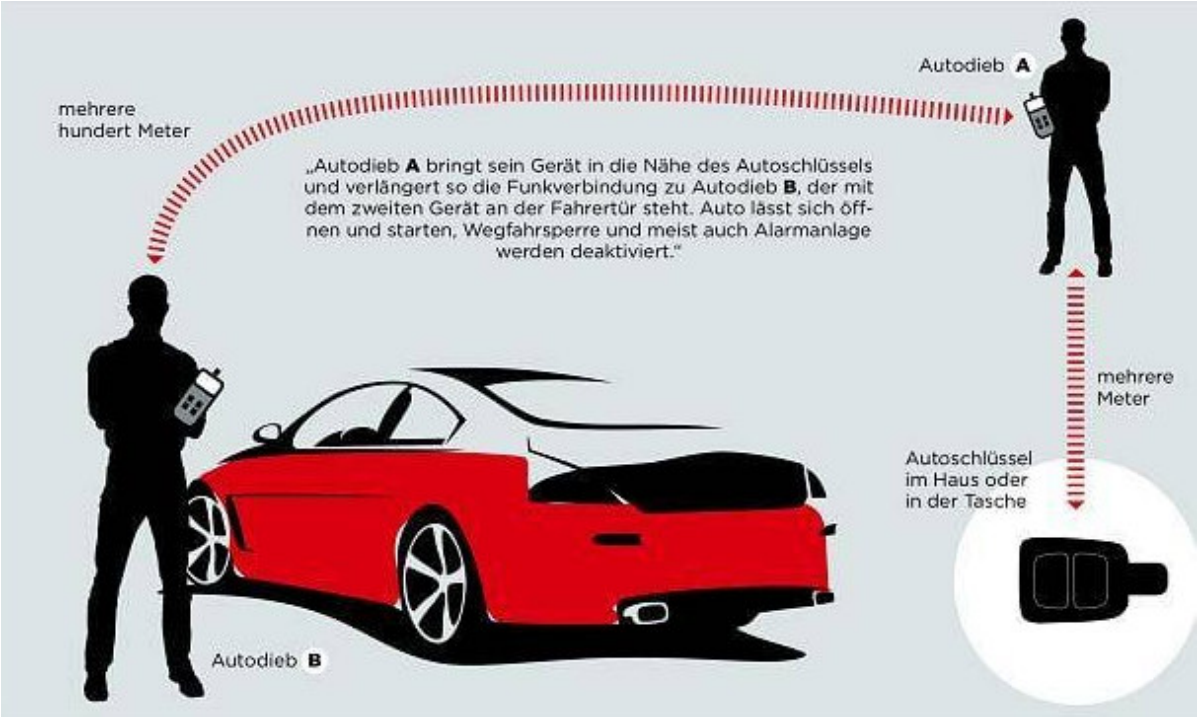


Abbildung 13: Beispiel RSA [18]

Angreifer können dabei das Signal aus der Wohnung oder Tasche des Fahrzeugnutzers erfassen, selbst durch bauliche Hindernisse wie Wände hindurch und über eine Funkbrücke an einen Komplizen am Fahrzeugstandort übertragen. Die Reichweite solcher Übertragungen kann bis zu 400 m betragen, wobei handelsübliche Repeater oder selbstgebaute Verstärkertechnologie verwendet wird. Das Fahrzeug interpretiert das empfangene Signal als legitimen Schlüssel in unmittelbarer Nähe, was zur automatischen Entriegelung der Türen oder zur Aktivierung der Startfunktion führt. Das Relay-Angriff-Szenario zählt zu den am häufigsten dokumentierten Angriffstechniken gegen moderne schlüssellose Zugangssysteme.

Die technische Grundlage dieser Verwundbarkeit liegt insbesondere in der physikalisch bedingten Reichweitenbegrenzung der verwendeten Niederfrequenzsignale im Bereich von 125 kHz. Hierbei beträgt die effektive Reichweite maximal zwei Meter. Fahrzeugdiebe nutzen gezielt diesen begrenzten Bereich, um durch elektronische Reichweitenverlängerung mittels Relaisstationen das System zu kompromittieren. Ein Angreifer mit dem ersten Gerät positioniert sich in unmittelbarer Nähe des Fahrzeugs, während sich eine zweite Person mit der zweiten Relaisstation nahe dem Schlüsselbesitzer aufhält. Durch diese Konstellation wird die Distanz zwischen Fahrzeug und Transponder künstlich überbrückt. Weder das Steuergerät des Fahrzeuges noch der

Transponder selbst sind in der Lage, die tatsächliche Entfernung zueinander zu bestimmen, da herkömmliche Keyless-Systeme keine Mechanismen zur Distanzmessung, wie zum Beispiel Laufzeitmessung, implementieren. Das Grundproblem besteht somit darin, dass sich die Systeme ausschließlich auf die Existenz eines gültigen Signals stützen, ohne die Echtheit der Signalquelle verifizieren zu können.

Eine zusätzliche Bedrohung ergibt sich aus dem Einsatz von tragbaren Funkstörsendern, die gezielt die Übertragung des Schließbefehls zwischen Schlüssel und Fahrzeug blockieren. Wird der Schließbefehl nach dem Verlassen des Fahrzeuges unterdrückt, bleibt das Fahrzeug unverschlossen. [1, 18, 24]

6 Versuche zu Relay-Angriffen auf Keyless-Systeme

6.1 Versuchskonzeption

Ziel der Versuchsreihe ist die praxisnahe Überprüfung der sicherheitstechnischen Anfälligkeit von Keyless-Systemen gegenüber einem gezielten Relay-Angriff unter realitätsnahen Bedingungen. Hierzu wurde ein von der Hochschule Mittweida ausgeliehenes, auf handelsüblichen Elektronikkomponenten basierendes Relais-System verwendet. Diese Geräte sind dazu in der Lage, die Kommunikation zwischen dem Fahrzeug und dem Fahrzeugschlüssel durch Funkverlängerung zu simulieren, um einen unautorisierten Zugang zum Fahrzeug zu ermöglichen. Als Versuchsgröße wurde die erfolgreiche oder nicht erfolgreiche Öffnung und Starten des Fahrzeuges ohne Originalschlüssel definiert. Einflussgrößen stellten das jeweilige Fahrzeugmodell sowie das Baujahr dar.

Für die Versuchsreihe wurden Fahrzeuge verschiedener Hersteller mit Keyless-Systemen ausgewählt:

- Mercedes-Benz
- Audi
- BMW
- Renault
- Ford
- Skoda

- Seat
- Toyota

Untersucht werden zehn serienmäßige Kraftfahrzeuge verschiedener Hersteller, ausgestattet mit werksseitig verbauten Keyless-Entry-Systemen. Die Fahrzeuge unterscheiden sich hinsichtlich ihrer Systemgenerationen, Funkschnittstellen, Schutzmechanismen sowie Einbaujahre. Ziel ist es, daraus Rückschlüsse auf die technische Weiterentwicklung und den aktuellen Stand der Sicherheitstechnik zu ziehen.

Die Versuchsdurchführung wurde unter reproduzierbaren Bedingungen gestaltet:

- Standort: möglichst störungsfreie Umgebung
- Abstand Schlüssel - Fahrzeug: 5 m bis 35 m (typischer Schlüsselstandort in realer Alltagssituation)
- Schlüsselstatus: liegend und unberührt um Inaktivität (Schlafmodus) zu provozieren
- Ausrichtung: Relais-Antennen auf/an Türgriff bzw. Fahrerseite ausgerichtet
- Wiederholungen: mind. 3 Versuche pro Fahrzeug

Die Versuche erfolgten mit ausdrücklicher Genehmigung der Fahrzeughalter. Es fand keine dauerhafte Beeinträchtigung der Fahrzeuge statt. Der Angriff basiert auf bloßer Signalreichweitenverlängerung.

Versuchsmatrix

Versuchs-Nr.	*Hersteller*	*Fahrzeug-modell*	*Entfernun-gen in m*	*Durchläufe*	*Umgebung*	*Erwartetes Ergebnis*
V01	Audi	A5 Cabrio-let	20, 25, 30	3	Große Halle	Tür ent-/verriegeln + Motorstart
V02	BMW	X1	15, 20, 25	3	Garage ges-chlossen	Tür ent-/verriegeln + Motorstart
V03	Renault	Captur	20, 25, 30	3	Hof auf Firmenge-lände	Tür ent-/verriegeln + Motorstart
V04	Ford	Kuga	15, 20, 25	3	Garage offen	Tür ent-/verriegeln + Motorstart
V05	Mercedes -Benz	CLS 400d	15, 20, 25	3	Carport	Motorstart
V06	Mercedes -Benz	E 300d	15, 25, 35	3	Garage geschlos-sen	Motorstart
V07	Mercedes -Benz	R 320 CDI	15, 25, 35	3	Großes Hofge-lände	Tür ent-/verriegeln + Motorstart
V08	Skoda	Kodiaq	15, 20, 25	3	Garage offen	Tür ent-/verriegeln + Motorstart
V09	Seat	Cupra Leon SP	15, 20, 25	3	Innenhof mit Hin-dernissen	Tür ent-/verriegeln + Motorstart
V10	Toyota	Corolla	10, 15, 20	3	Große Halle	Tür ent-/verriegeln + Motorstart

6.2 Relay-System Aufbau

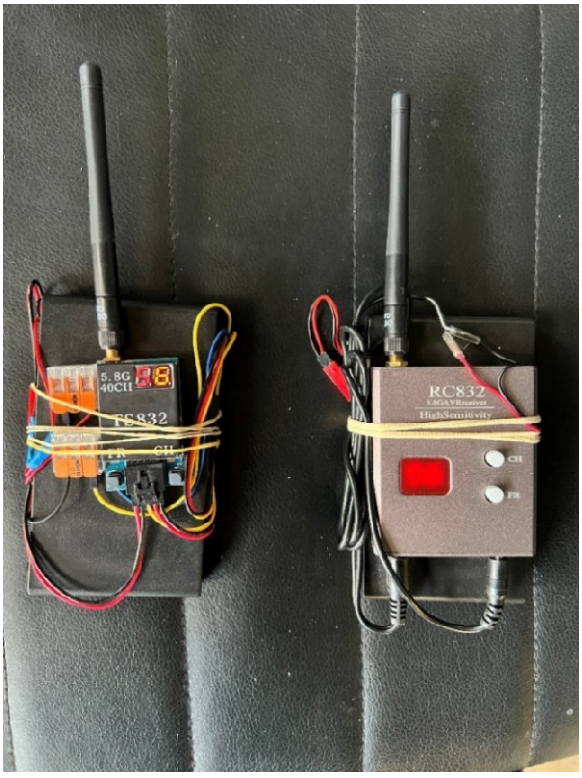


Abbildung 14: Relay-System Vorderseite (eigene Darstellung)

Abbildung 15: Relay-System Rückseite (eigene Darstellung)

Die in den Abbildungen 14 und 15 zu sehenden Relay-Geräte bestehen aus:

- Batteriepacks
- Transmitter
- Receiver
- RFID Antennen (125 kHz)

Tabelle 5: technische Daten Transmitter (eigene Darstellung) [19]

Transmitter : TS832 40 CH	
Arbeitsfrequenz	5,8 GHz
verfügbare Kanäle	40
Ausgangswiderstand	50 Ohm
Übertragungsentfernung	> 3000 m
Betriebsspannung	7-16 V
Versorgungsstrom	220 mA
Betriebstemperatur	-10 / +85 °C
Videobandbreite	0 - 8,0 MHz
Tonträgerfrequenz	6,5 MHz
Videoeingangspegel	0,8 ; 1,0 ; 1,2 Vp-p
Videoeingangswiderstand	75 Ohm
Audioeingangspegel	0,5 ; 2,0 Vp-p
Audioeingangswiderstand	10.000 Ohm

Tabelle 6: technische Daten Receiver (eigene Darstellung) [19]

Receiver: RC832	
Arbeitsfrequenz	5,8 GHz
verfügbare Kanäle	40
Stromversorgung	DC 12 V
Verbrauchsstrom	200 mA
Antennenwiderstand	50 Ohm
Videowiderstand	75 Ohm
Antennengewinn	2 dB
Audioträger	6,5 MHz
Videoformat	NTSC/PAL
Dimension	80 x 65 x 15 mm
Gewicht	85 g

Abbildung 16: Transmitter [19]

Abbildung 17: Receiver [19]

6.3 Versuchsvorbereitung

Die Vorbereitung der Versuchsreihe stellt eine essenzielle Voraussetzung für die technische und methodische Belastbarkeit der Untersuchungsergebnisse dar. Um reproduzierbare und valide Resultate sicherzustellen, wurden im Vorfeld mehrere organisatorische, technische und fahrzeugspezifische Maßnahmen durchgeführt.

Zunächst wurde ein Relay-System organisiert, welches in der Lage ist, ein typisches Funksignal zwischen Fahrzeug und Schlüssel zu verlängern. Zudem sollte es ein System sein, welches aus handelsüblichen Komponenten besteht, um das Sicherheitsrisiko von Keyless-Systemen, selbst bei einem Einsatz von einem einfachen Relay-System, zu verdeutlichen. Zum Einsatz kam ein von der Hochschule Mittweida bereitgestelltes System, welches auf handelsüblichen Elektronikkomponenten basiert und sowohl die niederfrequenten Aktivierungssignale als auch die hochfrequenten Antwortsignale über eine relaisgestützte Verbindung überträgt. Vor Beginn der eigentlichen Testreihen wurde das Relay-System in Betrieb genommen und hinsichtlich Funktionalität, Signalstabilität und Reichweite getestet. Darüber hinaus wurde die Stromversorgung geprüft.

Für die experimentelle Untersuchung wurde eine Auswahl an Versuchsfahrzeugen verschiedener Hersteller, Modellreihen und Baujahre getroffen. Ausschlaggebend war die werkseitige Verfügbarkeit eines funkbasierten schlüssellosen Zugangssystem. Die Diversität der ausgewählten Fahrzeuge diente dem Ziel, unterschiedliche technische Realisierungen der Zugangskontrolle sowie generationsspezifische Schutzmaßnahmen abbilden zu können. Zur Vermeidung potenzieller Störungen infolge schwacher Batteriespannung wurde im Vorfeld jeder Versuchsdurchführung der Ladezustand des Fahrzeugschlüssels überprüft. Die Verfügbarkeit der Versuchsfahrzeuge wurde durch individuelle Terminabsprachen mit den jeweiligen Fahrzeugeigentümern koordiniert. Dabei wurde sichergestellt, dass das Fahrzeug für die Dauer der Versuchsdurchführung uneingeschränkt zur Verfügung stand und sich keine weiteren Fahrzeugschlüssel desselben Fahrzeuges im Einflussbereichs des Systems befanden.

Da die Position der LF-Antennen sowie der UHF-Sende-/Empfangseinheiten fahrzeugspezifisch variiert, wurde im Vorfeld eine gezielte technische Recherche durchgeführt, um die korrekte Positionierung der Relay-Komponenten während des Versuches zu gewährleisten.

6.4 Versuchsdurchführung

Die Versuchsreihe folgt einem experimentellen Design mit kontrollierten Variablen zur Gewährleistung reproduzierbarer Ergebnisse. Als unabhängige Variable ist der Erfolg des Relay-Angriffs in Form von erfolgreich/nicht erfolgreich für die Funktionen Türöffnung und Motorstart definiert. Unabhängige Variablen umfassen:

- Fahrzeugtyp und Hersteller
- Baujahr des Fahrzeuges
- Art des verbauten Keyless-Systems
- Vorhandensein von UWB-Technologie oder Bewegungssensoren
- Testentfernung zwischen Schlüssel und Fahrzeug

Die Auswahl der zehn Testfahrzeuge erfolgte nach einer zweckmäßigen und systematischen Strategie, welche verschiedene Hersteller, Baujahre und Keyless-Technologien abdeckt.

Es erfolgte eine standardisierte Vorbereitung pro Testfahrzeug vor Ort:

- Alle Türen verschlossen und Zündung aus
- Funktionstest des originalen Fahrzeugschlüssel
- Positionierung von Fahrzeug, Relay-System und Personen

Standardisierter und systematischer Ablauf einer Versuchsreihe:

1. Normalen Keyless-Betrieb ohne Relay-System testen, inkl. Verifikation aller vorhandenen Fahrzeugfunktionen (Türöffnung, Motorstart, Heckklappe)
2. Positionierung Transmitter-Einheit am Türgriff-Sensor
3. Positionierung Receiver-Einheit bei ruhendem Schlüssel
4. Aktivierung des Relay-Systems
5. Versuch Türöffnung in allen Distanzvariationen/Testentfernungen
6. Versuch Heckklappe in allen Distanzvariationen/Testentfernungen
7. Versuch Motorstart in allen Distanzvariationen/Testentfernungen
8. Dokumentation der Versuchsergebnisse

In allen Versuchsdurchführungen wurde eine Wartezeit berücksichtigt, sodass das System und der Schlüssel in den Sleep-Mode wechseln. Des Weiteren wurden Beobachtungen durchgeführt wie zum Beispiel:

- LED-Blinkmuster
- akustische Signale
- Display-Anzeigen, Warnleuchten oder Sprach-Ausgaben
- ungewöhnliche Verzögerungen oder Reaktionen

V01 - Audi A5 Cabriolet (BJ: 2015)

Abbildung 18: V01 - Audi A5 (eigene Darstellung)

- Keyless-System: Keyless Entry & Go (Komfortschlüssel)
- Funktion: Öffnen/Schließen der Türen und Starten des Motors ohne aktive Betätigung des Schlüssels; Zugang durch Berührung des Türgriffsensors, Motorstart per Startknopf neben dem Schalthebel
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: keine Ultra-Wide-Band-Technologie (UWB)

Versuchsablauf:

- drei Versuchsdurchführungen: 20 m, 25 m, 30 m
- Testumgebung: Große Halle mit Hallentoren ohne Hindernisse
- Abstand: Schlüssel 20 bis 30 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich öffnen und schließen, Türgriffsensor reagierte zuverlässig ohne erkennbare Fehlfunktionen
- Motorstart war ebenfalls möglich, kurze Meldung "Schlüssel nicht erkannt"
- 3/3 Versuche waren erfolgreich
- keine UWB-Integration, somit keine wirksame Schutzmaßnahme gegen RSA

V02 - BMW X1 (BJ: 2020)

Abbildung 19: V02 - BMW X1 (eigene Darstellung)

- Keyless-System: Komfortzugang
- Funktion: Öffnen/Schließen der Türen und Starten des Motors ohne aktive Betätigung des Schlüssels; Zugang durch Berührung des Türgriffsensors, Motorstart per Startknopf
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: Ultra-Wide-Band-Technologie (UWB) verbaut, wodurch das Funksignal nach kurzer Zeit der Inaktivität abgeschaltet wird

Versuchsablauf:

- drei Versuchsdurchführungen: 15 m, 20 m, 25 m
- Testumgebung: geräumige Garage mit geschlossenem Garagentor
- Abstand: Schlüssel 15 bis 25 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich nicht öffnen, Türgriffsensor reagierte nicht auf verlängertes Signal
- Motorstart war ebenfalls nicht möglich, Meldung "Schlüssel nicht erkannt"
- 0/3 Versuche waren erfolgreich
- UWB-Integration, somit wirksame Schutzmaßnahme gegen RSA erkennbar

V03 - Renault Captur (BJ: 2015)

Abbildung 20: V03 - Renault Captur (eigene Darstellung)

- Keyless-System: Keycard Handsfree
- Funktion: Öffnen und Schließen der Türen ohne aktive Betätigung der Schlüsselkarte durch Betätigung der Entriegelungstaste am Türgriff, Motorstart über Start-Knopf möglich
- Technische Umsetzung: LF-Antennen in den Türgriffen und im Innenraum, UHF-Kommunikation mit Schlüsselkarte
- Besonderheiten: keine Ultra-Wide-Band-Technologie (UWB)

Versuchsablauf:

- drei Versuchsdurchführungen: 20 m, 25 m, 30 m
- Testumgebung: weiträumiger Firmenhof mit Fahrzeugen als Hindernisse
- Abstand: Schlüssel 20 bis 30 m vom Fahrzeug entfernt, Receiver mit geringem Abstand an Schlüsselkarte gehalten
- Transmitter an LF-Antennen im Bereich des Türgriffs und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich verzögerungsfrei öffnen und schließen, Entriegelungstaste auf Türgriff reagierte zuverlässig ohne erkennbare Fehlfunktionen
- Motorstart war ebenfalls möglich, keine Fehlermeldung
- 3/3 Versuche waren erfolgreich
- keine UWB-Integration, somit keine wirksame Schutzmaßnahme gegen RSA

V04 - Ford Kuga (BJ: 2021)

Abbildung 21: V04 - Ford Kuga (eigene Darstellung)

- Keyless-System: Ford Key Free-System
- Funktion: Öffnen/Schließen der Türen und Starten des Motors ohne aktive Betätigung des Schlüssels; Zugang durch Berührung des Türgriffsensors, Motorstart per Startknopf
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: Bewegungssensor im Schlüssel (Motion Sensor Key Fob) verbaut, Schlüssel wechselt nach 40 Sekunden Inaktivität in einen Stromsparmodus, kein Signalaustausch mehr

Versuchsablauf:

- drei Versuchsdurchführungen: 15 m, 20 m, 25 m
- Testumgebung: geräumige Garage mit offenem Garagentor
- Abstand: Schlüssel 15 bis 25 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich nicht öffnen, Türgriffsensor reagierte nicht
- Motorstart war ebenfalls nicht möglich, Meldung "Schlüssel nicht erkannt"
- 0/3 Versuche waren erfolgreich
- UWB-Integration, somit erkennbare Schutzmaßnahme gegen RSA

V05 - Mercedes Benz CLS 400d (BJ: 2021)

Abbildung 22: V05 - Mercedes Benz CLS 400d (eigene Darstellung)

- Keyless-System: Keyless-Go Start-Funktion (Startknopf im Innenraum), kein Keyless Entry an Türgriffen
- Funktion: Starten des Motors ohne aktive Betätigung des Fahrzeugschlüssels per Startknopf im Innenraum
- Technische Umsetzung: LF/UHF-Kommunikation zwischen Schlüssel und Fahrzeug, aber keine Türgriffsensoren für schlüssellosen Zugang
- Besonderheiten: Zentralverriegelung und Türen müssen manuell mit Schlüsselfernbedienung geöffnet werden, Motorstart per Knopfdruck

Versuchsablauf:

- drei Versuchsdurchführungen: 15 m, 20 m, 25 m
- Testumgebung: offener Carport mit Bäumen und Büschen als Hindernisse
- Abstand: Schlüssel 15 bis 25 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Innenraum gehalten

Versuchsergebnis:

- Fahrzeug manuell mit Schlüssel entriegelt
- Motorstart war problemlos möglich, keine Fehlermeldung ersichtlich
- 3/3 Versuche waren erfolgreich
- Türgriffsensoren für Keyless Entry nicht verbaut, daher keine klassische RSA möglich, jedoch nach Zugang zum Fahrzeug möglich

V06 - Mercedes Benz E 300d (BJ: 2021)

Abbildung 23: V06 - Mercedes Benz E 300d (eigene Darstellung)

- Keyless-System: Keyless-Go Start-Funktion (Startknopf im Innenraum), kein Keyless Entry an Türgriffen
- Funktion: Starten des Motors ohne aktive Betätigung des Fahrzeugschlüssels per Startknopf im Innenraum
- Technische Umsetzung: LF/UHF-Kommunikation zwischen Schlüssel und Fahrzeug, aber keine Türgriffsensoren für schlüssellosen Zugang
- Besonderheiten: Zentralverriegelung und Türen müssen manuell mit Schlüsselfernbedienung geöffnet werden, Motorstart per Knopfdruck

Versuchsablauf:

- drei Versuchsdurchführungen: 15 m, 25 m, 35 m
- Testumgebung: enge, vollständig geschlossene Garage
- Abstand: Schlüssel 15 bis 35 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend) mit Garage und Büschen als Hindernisse
- Transmitter an LF-Antennen im Innenraum gehalten

Versuchsergebnis:

- Motorstart war problemlos möglich, keine Fehlermeldung ersichtlich
- 3/3 Versuche waren erfolgreich
- Türgriffsensoren für Keyless Entry nicht verbaut, daher keine klassische RSA möglich, jedoch nach Zugang zum Fahrzeug möglich
- geschlossene Garage hatte keinen negativen Einfluss auf simulierte RSA

V07 - Mercedes Benz R 320 CDI (BJ: 2008)

Abbildung 24: V07 - Mercedes Benz R 320 CDI (eigene Darstellung)

- Keyless-System: Keyless-Go (Innen- und Außenzugang)
- Funktion: Schlüsselloses Öffnen und Schließen aller Türen sowie Starten des Motors per Start-Knopf, solange sich der berechtigte Schlüssel in Fahrzeugnähe oder Innenraum befindet
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit Fahrzeugchlüssel
- Besonderheiten: keine Ultra-Wide-Band-Technologie (UWB), Entriegelungstaste und Türgriffsensor im Türgriff kombiniert

Versuchsablauf:

- drei Versuchsdurchführungen: 15 m, 25 m, 35 m
- Testumgebung: großes Hofgelände ohne Hindernisse
- Abstand: Schlüssel 15 bis 35 m vom Fahrzeug entfernt, Receiver mit geringem Abstand an Fahrzeugchlüssel gehalten
- Transmitter an LF-Antennen im Bereich des Türgriffs und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich verzögerungsfrei öffnen und schließen, Entriegelungstaste auf Türgriff reagierte zuverlässig ohne erkennbare Fehlfunktionen
- Motorstart war ebenfalls möglich, keine Fehlermeldung erkennbar
- 3/3 Versuche waren erfolgreich
- keine UWB-Integration, somit keine wirksame Schutzmaßnahme gegen RSA

V08 - Skoda Kodiaq (BJ: 2023)

Abbildung 25: V08 - Skoda Kodiaq (eigene Darstellung)

- Keyless-System: KESSY
- Funktion: Öffnen/Schließen der Türen und Starten des Motors ohne aktive Betätigung des Schlüssels; Zugang durch Berührung des Türgriffsensors, Motorstart per Startknopf
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: keine Ultra-Wide-Band-Technologie (UWB)

Versuchsablauf:

- drei Versuchsdurchführungen: jeweils 15 m, 20 m, 25 m
- Testumgebung: geräumige Garage mit offenem Garagentor
- Abstand: Schlüssel 15 bis 25 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich nach einigen Versuchen öffnen
- Motorstart war nicht möglich, Meldung "Schlüssel nicht gefunden"
- 2/3 Versuche Türen zu öffnen waren erfolgreich
- 0/3 Versuche Motor zu starten waren erfolgreich
- möglicherweise Innenraumantenne nicht optimal getroffen für Motorstart

V09 - Seat Cupra Leon SP (BJ: 2021)

Abbildung 26: V09 - Seat Cupra Leon SP (eigene Darstellung

- Keyless-System: KESSY
- Funktion: Öffnen und Schließen aller Türen sowie Starten des Motors per Startknopf ohne aktive Schlüsselbetätigung möglich
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: separate Antennen für Heckklappe, selektive Entriegelung möglich (z.B. nur Fahrertür oder nur Heckklappe)

Versuchsablauf:

- drei Versuchsdurchführungen: jeweils 15 m, 20 m, 25 m
- Testumgebung: Innenhof mit Fahrzeugen als Hindernisse
- Abstand: Schlüssel 15 bis 25 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff, Heckklappe und Innenraum gehalten

Versuchsergebnis:

- Fahrzeugtür ließ sich nicht öffnen, allerdings die Heckklappe
- Motorstart war problemlos möglich, keine Fehlermeldung
- 0/3 Versuche Türen zu öffnen waren erfolgreich
- 3/3 Versuche Motor zu starten waren erfolgreich
- 3/3 Versuche Heckklappe zu öffnen waren erfolgreich
- möglicherweise LF-Antennen im Türgriffbereich nicht optimal getroffen

V10 - Toyota Corolla (BJ: 2019)

Abbildung 27: V10 - Toyota Corolla (eigene Darstellung)

- Keyless-System: Smart Entry & Start
- Funktion: Öffnen/Schließen der Türen und Starten des Motors ohne aktive Betätigung des Schlüssels; Zugang durch Berührung des Türgriffsensors, Motorstart per Startknopf
- Technische Umsetzung: LF-Antennen in den Türgriffen, Kofferraum und im Innenraum, UHF-Kommunikation mit dem Schlüssel
- Besonderheiten: keine Ultra-Wide-Band-Technologie (UWB)

Versuchsablauf:

- drei Versuchsdurchführungen: jeweils 10 m, 15 m, 20 m
- Testumgebung: geschlossene Werkstatthalle mit zahlreichen Hindernissen
- Abstand: Schlüssel 10 bis 20 m vom Fahrzeug entfernt, Receiver neben Schlüssel gelegt (ruhend)
- Transmitter an LF-Antennen im Türgriff und Innenraum gehalten

Versuchsergebnis:

- Fahrzeug ließ sich in allen Versuchen verzögerungsfrei öffnen
- Motorstart war nicht möglich, Meldung "Schlüssel nicht gefunden"

- 3/3 Versuche Türen zu öffnen waren erfolgreich
- 0/3 Versuche Motor zu starten waren erfolgreich
- möglicherweise technische Trennung der Authentifizierung für Zugang und Start oder Innenraumantenne nicht optimal getroffen

6.5 Versuchsergebnisse und Auswertung

Die Ergebnisse der zehn getesteten Fahrzeuge zeigt eine hohe Erfolgsquote bei den simulierten Relay-Angriffen. Von den untersuchten Fahrzeugen konnten 30 % vollständig kompromittiert werden, das bedeutet sowohl Türöffnung als auch Motorstart waren erfolgreich. Weitere 50 % der Testfahrzeuge erwiesen sich partiell anfällig, wobei hier entweder die Türöffnung oder der Motorstart gelang. 20 % der getesteten Fahrzeuge zeigten eine vollständige Resistenz gegen die simulierten Relay-Angriffe.

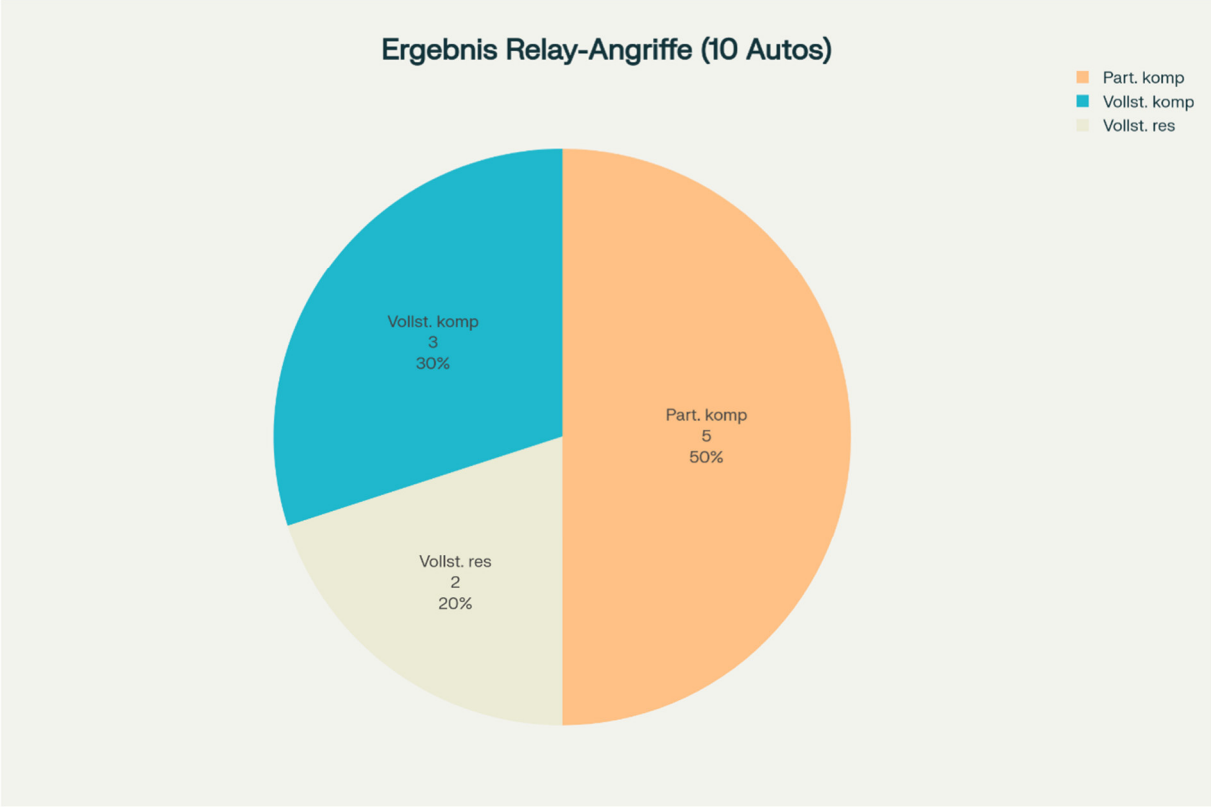


Abbildung 28: Darstellung Ergebnisse aus Versuch (eigene Darstellung)

In Abbildung 28 lässt sich verdeutlicht sehen, dass 80 % der getesteten Fahrzeuge mindestens eine Sicherheitslücke aufweisen, die von Angreifern potenziell ausgenutzt werden kann. Nicht zu vernachlässigen ist, dass selbst bei partiell erfolgreichen Angriffen erhebliche Sicherheitsrisiken bestehen, da bereits der Zugang zum Fahrzeuginnenraum oder die Möglichkeit des Motorstarts kritische Schwachstellen darstellen.

In Abbildung 29 werden die Fahrzeuge nach ihrem Schutzlevel kategorisiert, um die Sicherheitslevel deutlicher darzustellen.

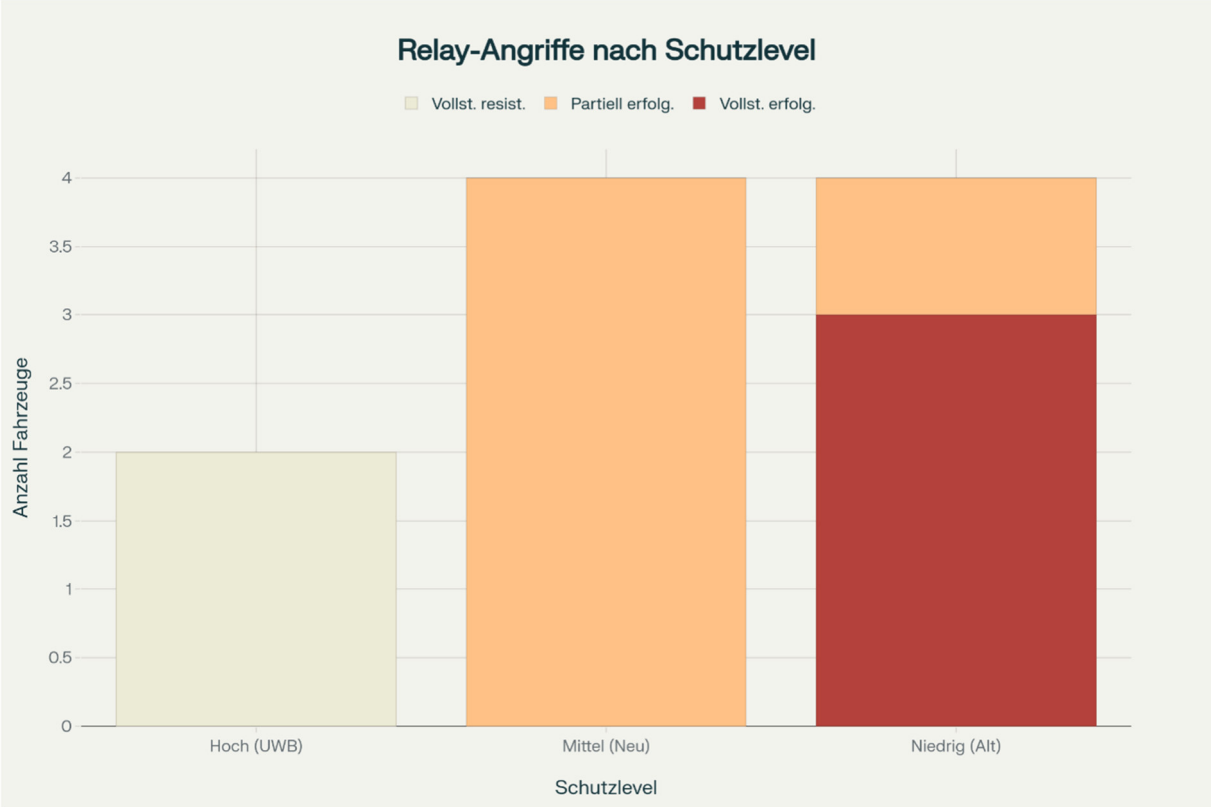


Abbildung 29: Einteilung in Schutzlevel (eigene Darstellung)

Die Fahrzeuge, welche über Ultra-Wideband-Technologie und/oder Bewegungs-sensoren verfügen, zeigten sich in den Tests als vollständig resistent gegen die simulierten Relay-Angriffe und werden somit im Sicherheitslevel Hoch eingestuft. Dies betrifft ausschließlich die Testfahrzeuge V02 und V04.

Die Testfahrzeuge V05, V06, V08 und V09 repräsentieren die neueren Fahrzeug-generationen ab Baujahr 2020 ohne Ultra-Wideband-Technologie und zeigten ausnahmslos eine partielle Kompromittierung. Bei diesen Fahrzeugen gelang zwar nicht die vollständige Kompromittierung, jedoch waren spezifische Funktionen angreifbar

gegenüber den simulierten Relay-Angriffen. Somit werden diese im mittleren Schutzlevel eingestuft.

Im niedrigen Schutzlevel eingestufte Fahrzeuge sind überwiegend ältere Fahrzeuggenerationen, welche sich, ausgenommen V10, als vollständig kompromittierbar darstellten. Diese Testfahrzeuge V01, V03 und V07 konnten ohne Probleme sowohl entriegelt als auch gestartet werden. Auch beim V10 konnte zumindest eine partielle Kompromittierung festgestellt werden.

Betrachtet man die Ergebnisdarstellung, ist abzuleiten, dass ein erfolgreicher Motorstart mittels Relay-Angriffes häufiger erfolgreich war als das Entriegeln der Fahrzeugtür. Während 60 % der getesteten Fahrzeuge über den Relay-Angriff gestartet werden konnten, war es bei nur 50 % der Fahrzeuge möglich eine erfolgreiche Entriegelung zu erzielen. Dies deutet unter anderem auf unterschiedliche Sicherheitsstrukturen hin, bei denen Motorstart und Fahrzeugentriegelung über separate Authentifizierungs-mechanismen verfügen. Bei der chronologischen Betrachtung der Versuchsfahrzeuge zeigt sich eine deutliche Entwicklung der Sicherheit von Keyless-Systemen über die Jahre. Während sich die Testfahrzeuge der Baujahre bis 2015 ausnahmslos als vollständig kompromittierbar zeigten, treten ab den getesteten Fahrzeugen mit einem Baujahr ab 2019 nur noch partielle Anfälligkeiten auf. Dies deutet darauf hin, dass die Automobilhersteller auf die bekannten Bedrohungen reagiert haben, jedoch noch keine flächendeckende Implementierung von Ultra-Wideband-Technologie oder vergleichbare Schutzmaßnahmen erfolgte.

Ergebnisdarstellung

Versuchs-Nr.	*Hersteller*	*Fahrzeug-modell*	*Baujahr*	*Key-less Innen*	*Keyless Außen*	*Tür öff-nen*	*Motorstart*	*Versuchsergebnis*
V01	Audi	A5 Cabriolet	2015	✓	✓	✓	✓	Erfolgreich
V02	BMW	X1	2020	✓	✓	✗	✗	Nicht Erfolgreich
V03	Renault	Captur	2015	✓	✓	✓	✓	Erfolgreich
V04	Ford	Kuga	2021	✓	✓	✗	✗	Nicht Erfolgreich
V05	Mercedes - Benz	CLS 400d	2021	✓	✗	✗	✓	Erfolgreich
V06	Mercedes - Benz	E 300d	2021	✓	✗	✗	✓	Erfolgreich
V07	Mercedes - Benz	R 320 CDI	2008	✓	✓	✓	✓	Erfolgreich
V08	Skoda	Kodiaq	2023	✓	✓	✓	✗	Teilweise Er-folgreich
V09	Seat	Cupra Leon SP	2021	✓	✓	✗	✓	Teilweise Er-folgreich
V10	Toyota	Corolla	2019	✓	✓	✓	✗	Teilweise Er-folgreich

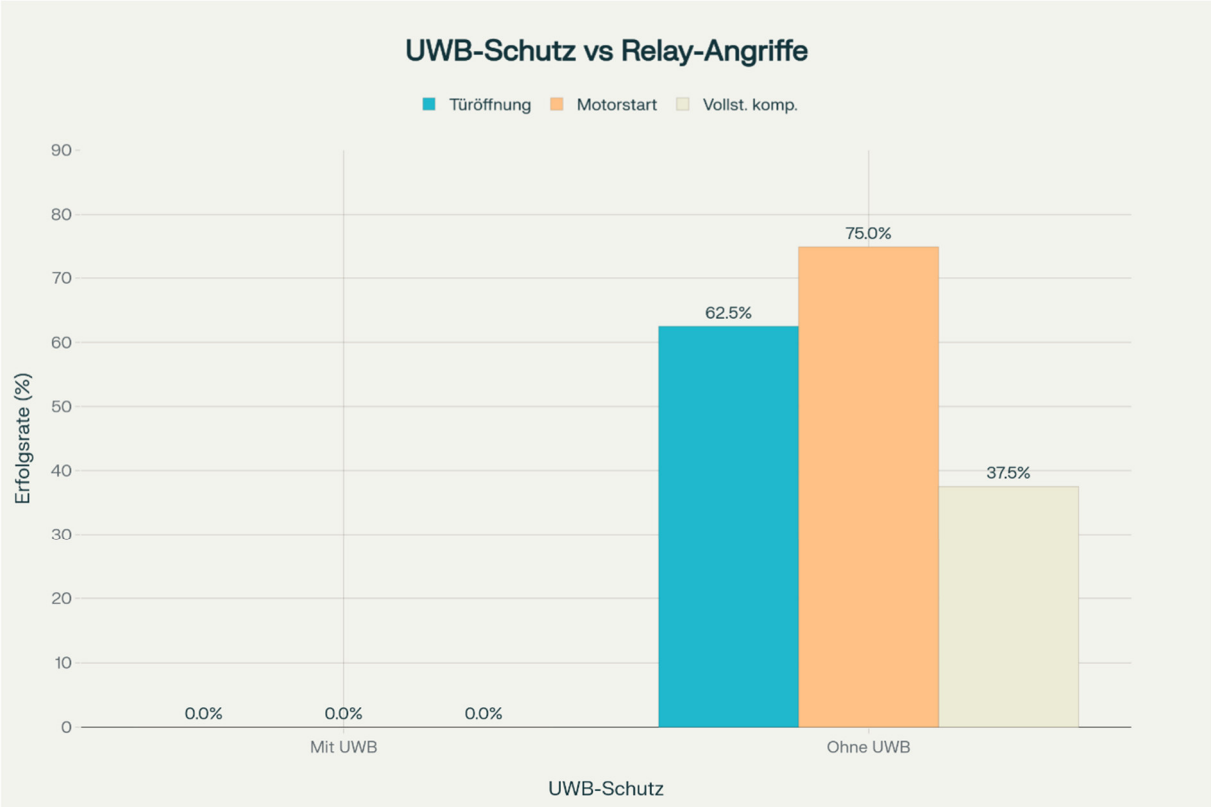


Abbildung 30: Vergleich UWB in Bezug auf Relay-Angriff (eigene Darstellung)

Die Auswertung in Abbildung 30 verdeutlicht, dass die Integration von Ultra-Wideband-Technologie oder Bewegungssensoren im Fahrzeugschlüssel eine wirksame Barriere gegen gängige Relay-Angriffe darstellt und die fundamentale Schwachstelle von Relay-Angriffen darstellt. Die Testfahrzeuge ohne Ultra-Wideband-Technologie zeigten Erfolgsraten von 62,5 % bei erfolgreicher Türentriegelung und 75 % bei erfolgreichem Motorstart, während Ultra-Wideband-geschützte Fahrzeuge eine Erfolgsrate von 0 in allen Kategorien aufwiesen.

7 Fehlerbetrachtung

Die Durchführung von sicherheitstechnischen Angriffstests auf Keyless-Systemen ist mit einer Vielzahl potenzieller Fehlerquellen verbunden. Für eine methodisch belastbare Auswertung ist daher eine differenzierte Betrachtung der Fehlertypen gemäß messtechnischer Systematik erforderlich. Die Fehler werden im Folgenden in drei Hauptkategorien unterteilt: grobe Fehler, systematische Fehler und zufällige Fehler.

Grobe Fehler sind massive Abweichungen vom erwarteten Messwert, welche durch offensichtliche Verstöße gegen die Versuchsvorschrift, menschliche Fehlbedienungen oder erhebliche Störungen entstehen. Sie unterscheiden sich fundamental von anderen Fehlertypen dadurch, dass sie vermeidbar sind und bei ordnungsgemäßer Versuchsdurchführung nicht auftreten sollten. Grobe Fehler führen zu Messwerten, welche so weit von der Realität abweichen, dass diese das Ergebnis vollständig verfälschen. Diese Fehlerart ist also dadurch charakterisiert, dass sie einzelne Messungen komplett disqualifiziert und nicht durch statistische Methoden korrigiert werden kann. Der betroffene Versuch muss somit vollständig wiederholt werden. [20]

Grobe Fehler in der durchgeführten Versuchsreihe sind:

- Relay-Geräte nicht eingeschaltet oder nicht korrekt synchronisiert
- falscher Funkkanal am Receiver
- Vertauschung von Sender und Empfänger der Relay-Einheiten
- Unbeabsichtigtes Bestätigen des Original-Fahrzeugschlüssel während des Tests
- Platzierung der LF-Antenne außerhalb der Reichweite des Fahrzeug-Türgriffsensors
- vollständiger Ausfall der Hardware (z.B. Akku der Geräte sind entladen)

Systematische Fehler sind reproduzierbare Abweichungen, welche unter gleichen Messbedingungen konstant auftreten und die Messungen konsistent in eine Richtung verfälschen. Sie entstehen durch Unvollkommenheit des Messsystems, der Methodik oder konstante Umwelteinflüsse. Charakteristisch ist, dass diese Fehler durch Wiederholung der Messung nicht erkannt werden können, da diese bei jedem Durchgang in gleicher Weise auftreten. Systematische Fehler beeinträchtigen die Richtigkeit der Messungen, während die Präzision unbeeinflusst bleibt. Sie können nur durch Vergleich mit anderen Messverfahren oder durch gezielte Kalibration identifiziert werden. [20]

Systematische Fehler in der durchgeführten Versuchsreihe sind:

- fehlende Kalibrierung
- Impedanzfehler zwischen Antennen und Receiver / Transmitter
- elektromagnetische Störfelder durch HF-Störquellen wie WLAN oder Mobilfunk
- Verwendung eines ungeeigneten Funkkanals (z.B. durch Interferenz durch andere Geräte im 2,4 GHz-Bereich)
- Antennenpositionsfehler
- Bauartbedingte Dämpfung der Signalstärke durch Abschirmung im Gehäuse
- Relay-Gerät mit zu geringer Sendeleistung

Zufällige Fehler sind Schwankungen, welche durch unvorhersehbare und nicht kontrollierbare Einflüsse entstehen. Diese beeinträchtigen die Präzision der Messungen, während die Richtigkeit unverändert bleibt. Sie folgen häufig einer Gauß´schen Normalverteilung und können durch mathematisch-statistische Verfahren korrigiert werden. [20]

Zufällige Fehler in der durchgeführten Versuchsreihe sind:

- temporäre Reflexionen oder Streuung von Funksignalen durch bewegliche Objekte wie zum Beispiel Personen oder Fahrzeuge
- geringfügige Verschiebung der Antennenausrichtung durch Handbewegungen
- menschliche Bediener-Reaktionszeit beim Türgriff-Test
- variable Verarbeitungszeiten in der Fahrzeug-ECU

8 Präventionsmaßnahmen und Zukunftsperspektiven

8.1 Technologische Gegenmaßnahmen gegen moderne Diebstahl-methoden

Eine der effektivsten Maßnahmen gegen moderne Diebstahlmethoden ist die Implementierung verbesserter Verschlüsselungstechniken. Moderne Sicherheits-systeme setzen auf symmetrische und asymmetrische Verschlüsselungsalgorithmen, die eine Manipulation der Fahrzeugkommunikation erschweren. Bei symmetrischen Verschlüsselungsverfahren wird ein und derselbe Schlüssel sowohl für die Ver- als auch für die Entschlüsselung von Daten verwendet. Dies ermöglicht eine besonders performante Datenverarbeitung mit geringen Latenzzeiten und niedrigem Rechenaufwand, Eigenschaften die insbesondere in Echtzeitanwendungen wie z.B. Türöffnung oder Motorstartfreigabe von zentraler Bedeutung im Fahrzeugbereich sind. Im Gegensatz dazu verwenden asymmetrische Verfahren zwei mathematisch miteinander verknüpfte Schlüssel: einen öffentlichen und einen privaten Schlüssel. Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können ausschließlich mit dem privaten Schlüssel entschlüsselt werden und umgekehrt. Dies ermöglicht unter anderem eine sichere Authentifizierung zwischen Fahrzeug und Schlüsselgerät, ohne dass ein geheimer Schlüssel über das Netzwerk übertragen werden muss.

Ein zentrales Sicherheitselement in der drahtlosen Fahrzeugkommunikation ist das Rolling-Code-Verfahren. Dabei wird bei jeder Interaktion zwischen Fahrzeugschlüssel und Steuergerät, zum Beispiel beim Betätigen der Funkfernbedienung, ein neuer, zufällig generierter Code verwendet. Dieser Code basiert auf einem vorher festgelegten Algorithmus und einem gemeinsamen Startwert. Durch die Verwendung von synchronisierten Sequenzzählern kann das Steuergerät des Fahrzeuges den jeweils gültigen Code berechnen und mit dem empfangenen Signal abgleichen. Das Verfahren verhindert erfolgreich Replay-Angriffe, bei denen Angreifer aufgezeichnete Kommunikationsdaten jederzeit nach Aufnahme erneut senden können, um unbefugt Zugriff zum Fahrzeug zu erlangen. Trotz dieser Fortschritte bleibt das Risiko technischer Angriffe bestehen, insbesondere im Hinblick auf die bereits detaillierte Signalverlängerungsangriffe/Relay-Angriffe.

Zukünftige Entwicklungen könnten auf Quantenkryptographie basieren, die aufgrund ihrer hohen Sicherheit als nahezu unüberwindbar gilt bzw. nicht unbemerkt manipuliert

werden können. Das Prinzip basiert auf Quantenschlüsselverteilung (Quantum Key Distribution). Hier werden Verschlüsselungsschlüssel durch den Austausch von Quantenzuständen, z.B. Photonen erstellt. Eine wichtige Eigenschaft ist, dass jeder Versuch, diese Quantenzustände auszulesen, sie verändert. Das bedeutet, dass ein Abhör- oder Abfangversuch sofort erkannt wird. Im Rahmen der Quantenschlüsselverteilung können Sender und Empfänger ein gemeinsames Schlüsselpaar generieren, wobei jeder Versuch, die Quantenzustände zu messen, die Übertragung irreversibel stört. Diese Störung ist detektierbar, was es erlaubt, kompromittierte Schlüssel zu verwerfen und auf eine sichere Verbindung zu bestehen oder auf einen Manipulationsversuch hinweisen. Mit Quantenkryptographie könnten also Fahrzeugschlüssel und das Fahrzeug selbst mit einem abhörsicheren Quantenschlüssel kommunizieren. Jeder Manipulationsversuch wäre sofort erkennbar, da der Schlüssel verändert werden würde.

Trotz der vielversprechenden Perspektiven befindet sich die Quantenkryptographie derzeit noch in der Entwicklungs- und Erprobungsphase. Einsatzgebiete beschränken sich aktuell vor allem auf stationäre Hochsicherheitsanwendungen, beispielsweise in Finanzinstitutionen und Regierungsstellen. Die Implementierung in hochmobile Systeme wie Kraftfahrzeuge stellt derzeit noch eine erhebliche technologische Herausforderung dar. Ein zentrales Problem ist die Integration in mobile, drahtlose Netzwerke, da die hochsensible Quantenkommunikation unter Bewegung und bei wechselnden atmosphärischen Bedingungen fehleranfällig ist. Zudem ist die Übertragung von Quantenzuständen bisher in der Regel auf Glasfaserleitungen oder Freiraumoptik mit direkter Sichtverbindung angewiesen. Die Echtzeitkommunikation zwischen einem Fahrzeugschlüssel und einem sich bewegenden Fahrzeug erfordert jedoch robuste und miniaturisierte Systeme, die mit den physikalischen Anforderungen der Quantenkommunikation vereinbar sind. Darüber hinaus ist die Kostenstruktur dieser Technologie derzeit für den Automotive-Massenmarkt noch nicht tragbar. [1, 21]

Die Automobilindustrie arbeitet passend dazu an der Einführung von Secure Element Chips. Diese sind physikalisch abgesicherte Mikrocontroller, die zur sicheren Speicherung und Verarbeitung kryptographischer Schlüssel, digitale Zertifikate sowie sicherheitsrelevanter Programme entwickelt wurden. Sie sind resistent gegenüber physischen Angriffen wie Spannungsmanipulationen, Temperaturänderungen und elektromagnetischer Abstrahlung. Diese Chips bieten also eine zusätzliche Sicherheitsschicht.

Anwendung findet dies beispielsweise in den bereits entwickelten und eingesetzten Digital Car Keys (siehe Abbildung 31). Hierbei handelt es sich um einen digitalen Fahrzeugschlüssel, welcher auf dem Smartphone des Fahrzeugeigentümers gespeichert wird und den klassisch physischen Schlüssel durch eine digitale und softwarebasierte Lösung ersetzt. Die Speicherung erfolgt innerhalb einer geschützten Hardwareumgebung, entweder in einem integrierten Secure Element, wie z.B. in Apple-Geräten oder in einem eingebettetem Secure Element des Fahrzeuges. Damit lässt sich das Fahrzeug unter anderem öffnen, verschließen und starten. Zusätzlich ist es möglich, mit integrierten Konnektivität-Funktionen einige Komfortfunktionen zu realisieren wie z.B. das Einstellen einer bestimmten Temperatur im Fahrzeug aus der Ferne (analog dazu vergleichbar mit Standheizungsfernbedienung), Fahrzeugeinstellungen vorzunehmen wie etwa die Farbe der Ambiente-Beleuchtung einzustellen oder das Fahrzeug von außen fernzusteuern, um in enge Parklücken zu gelangen. Hierbei kann die Verwendung des digitalen Fahrzeugschlüssels durch ausgewählte Personen mit zuvor definierten Einstellungen und Einschränkungen genutzt und geteilt werden, z.B. eine temporäre Befugnis einer Person lediglich auf das Öffnen und Schließen des Fahrzeuges zur Ablage von Gegenständen im Fahrzeug.

Der Digital Car Key basiert auf drei verschiedene Funktechnologien: NFC, UWB und Bluetooth. Durch diese Kombination von UWB, Bluetooth und NFC kombiniert mit der Erkennung bzw. Auswertung von Signalen des ToF-Systems ist der Missbrauch hierbei nahezu ausgeschlossen. [22]

Abbildung 31: Beispiel digitaler Fahrzeugschlüssel [22]

GPS-Tracker und Telematiksysteme haben sich als wirkungsvolle Instrumente zur Diebstahlprävention und -verfolgung etabliert. Diese Systeme ermöglichen die Echtzeitüberwachung des Fahrzeugs und können bei unbefugten Bewegungen sofort eine Warnmeldung ausgeben. Einige Tracker verfügen über Geofencing-Funktionen, die eine Benachrichtigung auslösen, sobald das Fahrzeug eine vordefinierte Zone verlässt. In Kombination mit Mobilfunktechnologien können gestohlene Fahrzeuge schnell lokalisiert und wiederbeschafft werden. Die Integration solcher Systeme in die Fahrzeugarchitektur wird zunehmend standardisiert, insbesondere in höherpreisigen Fahrzeugsegmenten. Ein Beispiel hierfür ist Mercedes ME-Connect von Mercedes-Benz, wobei das Fahrzeug in der Me-Connect App verknüpft wird und der Fahrzeugeigentümer somit jederzeit seine Fahrzeugdaten wie Kilometerstand, Füllstand des Tankes oder aktuelle Position des Fahrzeuges anzeigen lassen kann. Darüber hinaus lässt sich das Fahrzeug so auch entriegeln und verriegeln.

Auch zu betrachten sind einfache, aber verbreitete mechanische Schutzeinrichtungen bzw. zusätzliche manuelle Sicherungssysteme, wie Lenkrad- oder Gangschaltungsschlösser. Diese bieten zwar einen gewissen Schutz vor ungewollter Verwendung des Fahrzeuges und als zusätzlicher Zeitfaktor für Diebe, da die Umgehung jeder

Schutzeinrichtung Zeit kostet, sind jedoch häufig leicht zu umgehen. Mechanische Sicherungen können durch physische Gewalt oder den Einsatz von Schneidwerkzeugen überwunden werden. Zudem fehlt es diesen Systemen oft an einer Abschreckungswirkung, da sie in der Wahrnehmung der Täter als antiquiert gelten.

8.2 Aktuelle Trends der Fahrzeugüberwachung und Diebstahlprävention

Biometrische Zugangssysteme wie Fingerabdruck- oder Gesichtserkennung bieten eine vielversprechende Alternative zu traditionellen Schlüsselsystemen. Diese Technologien ermöglichen eine eindeutige Identifizierung des Fahrzeugnutzers und sind deutlich schwieriger zu manipulieren. Zusätzlich bieten diese Systeme einen gewissen Komfort, weil das Fahrzeug den Nutzer identifiziert und alle Einstellungen vom jeweiligen Nutzer übernimmt. Dies kann eine bevorzugte Temperatur sein, Sitzposition, Spiegelpositionen, Motor/Getriebe oder Fahrwerkseinstellungen oder z.B. der Lieblingsradiosender. Einige Hersteller experimentieren bereits mit multi-faktoriellen Authentifizierungssystemen, die biometrische Daten mit traditionellen Sicherheitsmethoden kombinieren. Diese Ansätze könnten in Zukunft die Sicherheit erheblich erhöhen, jedoch bleibt die Herausforderung, solche Systeme kosteneffizient und robust gegen Umwelteinflüsse zu gestalten. Künstliche Intelligenz (KI) wird zunehmend in Fahrzeugüberwachungssystemen eingesetzt, um verdächtige Aktivitäten frühzeitig zu erkennen. KI-Algorithmen können beispielsweise ungewöhnliche Bewegungsmuster oder Manipulationsversuche an der Fahrzeugsoftware identifizieren und die Alarmfunktion auslösen. Darüber hinaus können KI-Systeme kontinuierlich lernen und sich an neue Bedrohungsszenarien anpassen, was sie zu einer dynamischen und zukunftssicheren Lösung macht.

Zukünftige Entwicklungen könnten in Richtung Blockchain-Technologien gehen, die eine dezentrale und manipulationssichere Speicherung von Fahrzeugdaten ermöglichen. Solche Technologien könnten nicht nur den Diebstahlschutz verbessern, sondern auch die Nachverfolgung gestohlener Fahrzeuge erleichtern. Das Grundprinzip der Blockchain basiert auf Dezentralität, Unveränderlichkeit, Transparenz und effiziente Vorgänge. Die Daten werden nicht in einer zentralen Datenbank, sondern auf mehreren Knoten im Netzwerk gespeichert. Jede Transaktion wird in einem Block gespeichert, der kryptographisch mit dem vorherigen Block verbunden ist. Eine

nachträgliche Manipulation ist nahezu unmöglich. Alle Teilnehmer des Netzwerkes können die Daten einsehen und prüfen, was die Sicherheit erhöht (siehe Abbildung 32). [23]

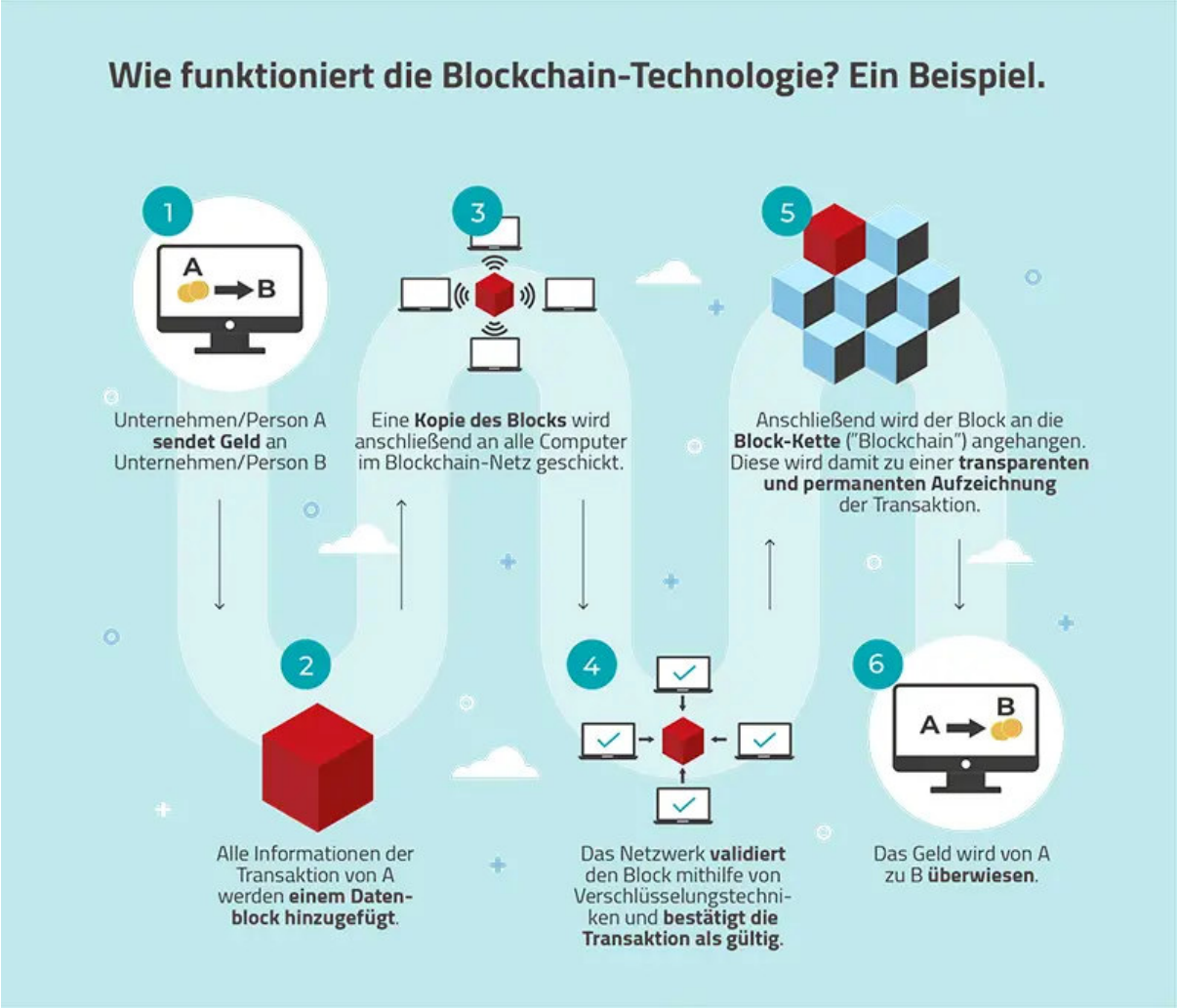


Abbildung 32: Funktionsweise Blockchain-Technologie [23]

Im Zusammenhang mit schlüssellosem Zugang zum Fahrzeug würde jeder Zugriff z.B. durch einen digitalen Schlüssel auf das Fahrzeug in der Blockchain gespeichert werden. Nur berechtigte Nutzer, deren Schlüssel in der Blockchain verifiziert sind, können das Fahrzeug öffnen und starten. Dadurch würden Manipulationsversuche, wie das Abfangen von Funksignalen deutlich erschwert werden. Zudem kann Blockchain sicherstellen, dass Over-the-Air-Updates bzw. Software-Updates für das Fahrzeug authentisch und nicht von Hackern manipuliert wurden sind. Zudem würde transparent dokumentiert werden, wann und welche Änderungen am Fahrzeug bzw. dessen Software durchgeführt wurden sind. Herausfordernd sind hierbei der Rechenaufwand, Netzwerklatenz und die Integration. Blockchain-Systeme benötigen aufgrund ihrer

Komplexität hohe Rechenressourcen, was im Fahrzeug mit begrenzter Hardware anspruchsvoll ist. Aufgrund der dezentralen Struktur kann es zu Verzögerungen in der Kommunikation kommen, was im Widerspruch zu modernen und vernetzten Fahrzeugen steht, da hier die schnelle Kommunikation entscheidend ist. [1]

Hilfreiche Präventionsmaßnahmen sind die Verwendung eines OBD-Schlosses oder der Einbau eines Zusatz-Batterie-Trennschalters. Dadurch wird die Ausnutzung der OBD-Schnittstelle verhindert und man kann das Fahrzeug stromlos schalten und somit verhindern, dass es gestartet oder elektronisch manipuliert werden kann. Ein geschickter Einbau eines solchen Zusatz-Schalters ist zu empfehlen, sodass der Dieb nicht erkennt, warum das Fahrzeug nicht anspringt. Während in dieser Arbeit vorrangig elektronische Sicherheitssysteme im Fokus stehen, sind mechanische Sicherungen weiterhin äußerst wirksam, da viele Diebe auf Geschwindigkeit setzen und eine zusätzliche physische Barriere den Zeitaufwand deutlich erhöhen kann. Beispiele hierfür sind Lenkradkrallen, Gangschaltungssperren oder Radkrallen. Die Kombination aus verschiedenen mechanischen Sicherungen kann besonders effektiv sein. Generell ist es zu empfehlen, das Fahrzeug an einem sicheren Ort zu parken, da der Standort des Fahrzeuges eine entscheidende Rolle in der Diebstahlprävention einnehmen kann. So ist es empfehlenswert, belebte und beleuchtete Parkplätze sowie wenn möglich Garagen und gesicherte Parkhäuser zu bevorzugen, da Fahrzeuge an dunklen und abgelegenen Straßen leichter angreifbar sind. Abschreckend im Alltag sind Überwachungskameras oder Attrappen solcher.

Im Falle einer Totalentwendung bestehen ebenfalls im Nachgang zur Wiederauffindung des Fahrzeuges einige Möglichkeiten, wie zum Beispiel die Ortung über einen im Fahrzeug versteckten GPS-Tracker. Einige Systeme bieten zusätzlich eine Bewegungserkennung, welche eine Warnung an das Endgerät sendet und warnt sobald das Fahrzeug ohne Berechtigung bewegt wird. Auch eine Individualisierung des Fahrzeuges kann erheblich zur Diebstahlprävention beitragen. Hierbei sind die daraus folgenden auffälligen Fahrzeugdetails wie zum Beispiel eine spezielle Folierung, Kennzeichen oder Umbauten der Karosserie eine große Hilfe für das Wiederauffinden des Fahrzeuges. Ebenso kann man auch die präventiven Maßnahmen der Polizei nutzen, indem man sein Fahrzeug beispielsweise in polizeiliche Präventionslisten eintragen lässt. Einige Länder bieten spezielle Registrierungen für gestohlene Fahrzeuge an. Ein

Aufkleber wie "Dieses Fahrzeug ist polizeilich registriert" kann als Abschreckung dienen, auch wenn keine tatsächliche Registrierung vorliegt.

9 Fazit

Die vorliegende Arbeit befasst sich mit der sicherheitstechnischen Bewertung schlüsselloser Zugangssysteme (Keyless-Systeme) in Kraftfahrzeugen, insbesondere im Hinblick auf ihre Anfälligkeit gegenüber Relay-Angriffen. Anhand eines historischen und technischen Überblicks sowie einer empirischen Untersuchung an Serienfahrzeugen konnte gezeigt werden, dass trotz erheblicher Fortschritte in der automobilen Sicherheit zentrale Schwachstellen bestehen, die aus Sicht des Diebstahlschutzes als kritisch einzustufen sind.

Die historische Betrachtung verdeutlichte den Wandel von überwiegend mechanischen Angriffsmethoden hin zu elektronisch basierten Angriffen, ausgelöst durch die zunehmende Integration elektronischer Komponenten. Während die Einführung der elektronischen Wegfahrsperre in den 1990er Jahren einen deutlichen Rückgang der Diebstahlzahlen bewirkte, eröffneten neuere Komforttechnologien wie Keyless-Systeme zugleich neue Angriffsvektoren. Im theoretischen Teil wurde dargelegt, dass Keyless-Systeme auf bidirektionaler Funkkommunikation zwischen Transponderschlüssel und Fahrzeug beruhen und bei unzureichender Absicherung eine besondere Anfälligkeit für Relay-Angriffe aufweisen. Dabei nutzen Angreifende handelsübliche Geräte, um die Reichweite der Funkverbindung zu verlängern und dem Fahrzeug die Nähe des legitimen Schlüssels vorzutäuschen.

Die im Rahmen dieser Arbeit durchgeführte Versuchsreihe bestätigte die hohe praktische Relevanz dieser Angriffsmethodik. Von zehn untersuchten Fahrzeugen konnten acht kompromittiert werden. Lediglich zwei Fahrzeuge mit Ultra-Wideband-Technologie erwiesen sich als resistent. Dieses Ergebnis verdeutlicht die besondere Bedeutung von Ultra-Wideband als derzeit wirksamste Schutzmaßnahme. Die Ergebnisse zeigen klar, dass Keyless-Systeme ohne ergänzende Schutzmechanismen als sicherheitskritisch einzustufen sind. Der geringe technische Aufwand für einen erfolgreichen Angriff stellt ein erhebliches Risiko für Fahrzeugbesitzende, Hersteller und Versicherungsunternehmen dar. Der Komfortgewinn solcher Systeme steht somit in einem deutlichen Spannungsverhältnis zur damit verbundenen Gefährdungslage. Die Analyse

bestehender Präventionsansätze verdeutlicht zudem, dass viele Maßnahmen entweder von den Nutzenden abhängen oder sich noch in der Entwicklung befinden. Eine nachhaltige Lösung kann nur durch strukturelle Verbesserungen in der Systemarchitektur erreicht werden. Im Vordergrund steht dabei die konsequente Integration von Ultra-Wideband oder vergleichbaren Entfernungsmesstechnologien sowie der Einsatz kryptografisch gesicherter Verfahren.

Zusammenfassend lässt sich festhalten, dass schlüssellose Zugangssysteme ohne aktive Schutzmechanismen als hochgradig unsicher gelten. Die empirischen Ergebnisse dieser Arbeit bestätigen die praktische Relevanz der Problematik. Als wirksamste Gegenstrategie erweist sich derzeit die Ultra-Wideband-Technologie. Die Sicherheit moderner Fahrzeugsysteme muss daher nicht allein über Komfortmerkmale, sondern in gleichem Maße über ihre Widerstandsfähigkeit gegenüber Angriffen definiert werden.

V. Literaturverzeichnis

[1] PISTORIUS, LAURA; POLSTER, HEIKO; LABUDDE, DIRK: Relay Station Attacks on Different RFID Access Systems (2023), verfügbar unter: https://ieeexplore.ieee.org/document/10387965 , abgerufen am 30.09.2025

[2] Pro-Lok Store für Slim Jim verfügbar unter: https://www.pro-lok.com/shop/pro-lok/automotive/auto-entrycar-opening/slim-jims/super-slim-jim-car-opening-tool/?srsltid=AfmBOootESQLmwS2wEz8dl2GMje3UeCtkfpbsR-bLqIO1RgmuYjpop6aY , abgerufen am: 29.07.2025

[3] Heni-Werkzeuge Shop für Montagekissen verfügbar unter: https://www.heni-werkzeuge.de/shop/product/heni%2031%20478/druckkissen%20luftkissen%20zum%20t%C3%BCr%C3%B6ffnen%20etc./ , abgerufen am 29.07.2025

[4] Spiegel Kultur Zeitungsartikel verfügbar unter: https://www.spiegel.de/kultur/negativer-hammer-a-c8e161e3-0002-0001-0000-000013520262, abgerufen am: 29.07.2025

[5] Golf 4 - Forum zum Thema Fahrzeugschlüssel verfügbar unter: https://www.golf4.de/interieur/148748-auf-klappschluessel-umbauen-anleitung-bilder.html , abgerufen am 29.07.2025

[6] KEM-Konstruktion Artikel verfügbar unter: https://automobilkonstruktion.industrie.de/elektronik-software/aptiv-bordnetzkonzept-sichert-stromversorgung-autonomer-fahrzeuge/ , abgerufen am 29.07.2025

[7] Programmheft für Key-Emulator verfügbar unter: https://agentgrabber.com/wp-content/uploads/2024/01/ISKRA-3_SMK_eng-3.pdf , abgerufen am 29.07.2025

[8] Autokeydevices - Shop für Key-Emulator verfügbar unter: https://www.autokeydevices.com/radio-devices/iskra-3-smart-key-emulator/ , abgerufen am 29.07.2025

[9] Gesamtverband der Versicherer Bericht über Diebstahlzahlen verfügbar unter: https://www.gdv.de/gdv/statistik/autodiebstahl, abgerufen am 29.07.2025

[10] Statista Beitrag verfügbar unter: https://de.statista.com/statistik/daten/studie/2100/umfrage/entwicklung-der-anzahl-von-diebstaehlen-kaskoversicherter-pkw/, abgerufen am 29.07.2025

[11] Allianz Zentrum für Technik Artikel über elektronische Wegfahrsperre verfügbar unter: https://www.azt-automotive.com/de/themen/AnforderungeneWS, abgerufen am 29.07.2025

[12] Straßenverkehrs-Zulassungs-Ordnung (StVZO) §38a Sicherungseinrichtungen von Kraftfahrzeugen verfügbar unter: https://www.gesetze-im-internet.de/stvzo_2012/__38a.html, abgerufen am: 29.07.2025

[13] Bauportal Artikel über RFID verfügbar unter: https://bauportal.bgbau.de/bauportal-42023/thema/branchenuebergreifend/wie-rfid-die-bauindustrie-revolutionieren-koennte , abgerufen am 29.07.2025

[14] Funktionsweise Rolling Code als Simulation verfügbar unter: https://harryli0088.github.io/rolling-code/ , abgerufen am 29.07.2025

[15] HELLA Artikel zu Keyless-Go verfügbar unter: https://www.hella.com/techworld/de/technik/elektrik-und-elektronik/keyless-go/ , abgerufen am 29.07.2025

[16] Industry of Things Artikel über Ultra-Wideband verfügbar unter: https://www.industry-of-things.de/mehr-als-tracking-hier-kommt-uwb-in-der-industrie-zum-einsatz-afb83a26e6ba7c69890fe2fd1c4c6fb6b/ , abgerufen am 29.07.2025

[17] IEEE-Standard 802.15.4z verfügbar unter: https://ieeexplore.ieee.org/document/9179124 , abgerufen am 29.07,2025

[18] PLATTNER, GEORG: Arbeit über Keyless Entry Systeme für das Kuratorium für Verkerhrsicherheit verfügbar unter: https://www.kfv.at/wp-content/uploads/2020/07/Endbericht-KeylessGo-FINAL.pdf , abgerufen am 29.07.2025

[19] AKKTEK Shop für Transmitter und Receiver Kit verfügbar unter: https://www.akktek.com/akk-ts832-rc832.html?srsltid=AfmBOopWJuxxy4FdKP9rj_gLIgHD0RSBQ9MMaJoczn0FlbaKGoeGWXQO , abgerufen am 29.07.2025

[20] Vortragsfolien zu Fehlerbetrachtung von Uni Rostock verfügbar unter: https://www.bio.uni-rostock.de/storages/uni-rostock/Alle_MNF/Chemie_Ludwig/Lehre/Grundpraktikum_Bachelor/02_Fehlerbetrachtung.pdf , abgerufen am 29.07.2025

[21] Artikel vom Frauenhofer Institut über Kryptografie verfügbar unter: https://www.sit.fraunhofer.de/de/presse/details/news-article/show/kryptografie-fuer-das-auto-der-zukunft/, abgerufen am 29.07.2025

[22] NFCW Online-Artikel über Hyndai Smartphone Schlüssel verfügbar unter: https://www.nfcw.com/2021/01/19/370164/hyundai-to-let-drivers-use-their-iphone-to-unlock-their-vehicle/, abgerufen am 29.07.2025

[23] Polizei Sachsen Online-Artikel über Kfz-Diebstahl verfügbar unter: https://www.polizei.sachsen.de/de/24209.htm, abgerufen am 29.07.2025

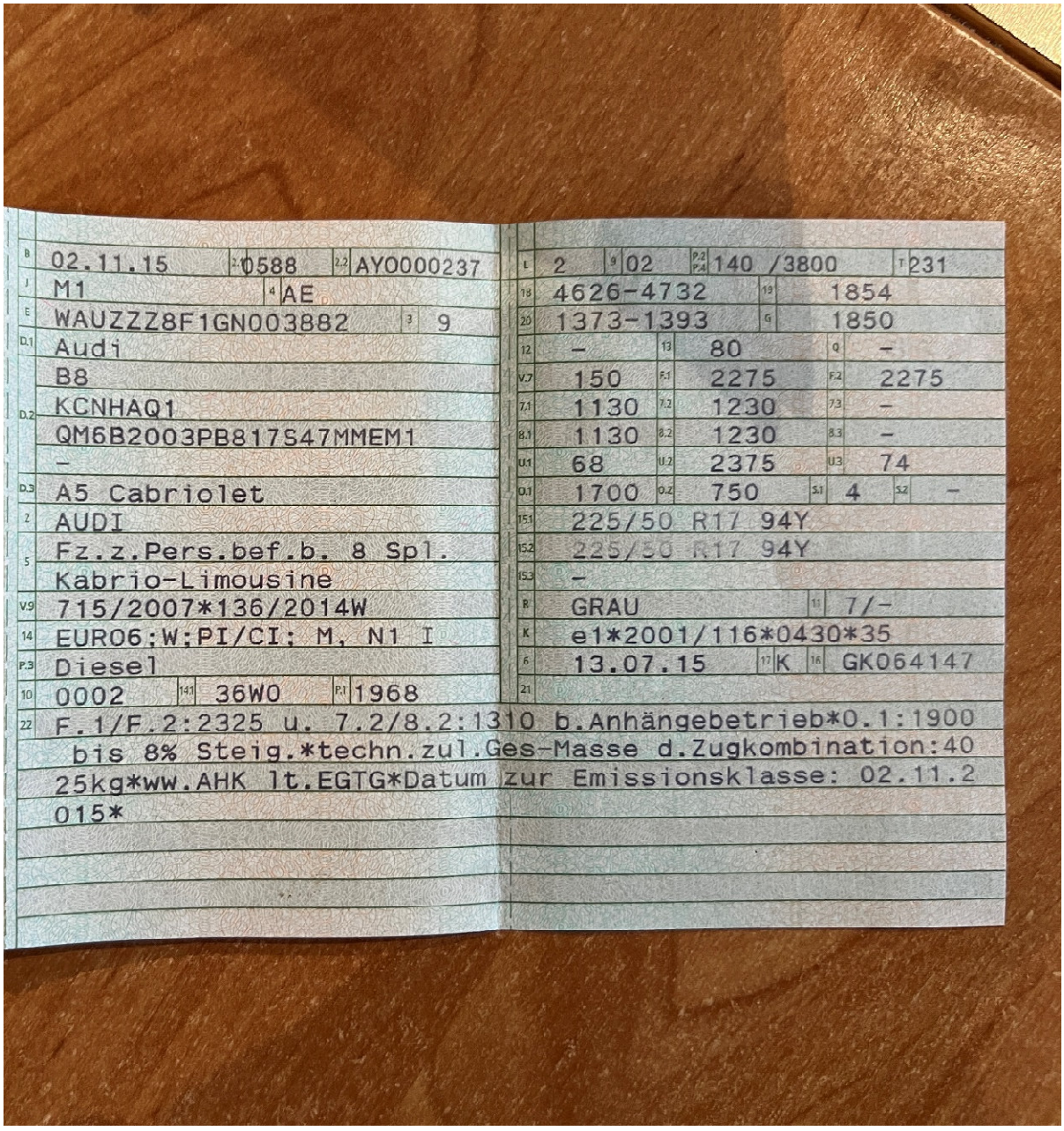
[24] FRANCILLON AURELIEN, DANEV BORIS, CAPKUN SRDJAN Arbeit über Relay-Angriffe für die ETH Zürich verfügbar unter: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/42365/eth-4572-01.pdf , abgerufen am 29.07.2025

[25] Statistiken zur deutschen Versicherungswirtschaft vom Gesamtverband der Versicherer verfügbar unter: https://www.gdv.de/resource/blob/152652/4a475238113e764d7dcfb9fd0f54dff1/statistiken-zur-deutschen-versicherungswirtschaft-taschenbuch-data.pdf , abgerufen am 29.07.2025

[26] Spiegel - Artikel über Autodiebstähle verfügbar unter: https://www.spiegel.de/auto/aktuell/statistik-autodiebstaehle-in-deutschland-1989-bis-1996-a-48511.html , abgerufen am 29.07.2025

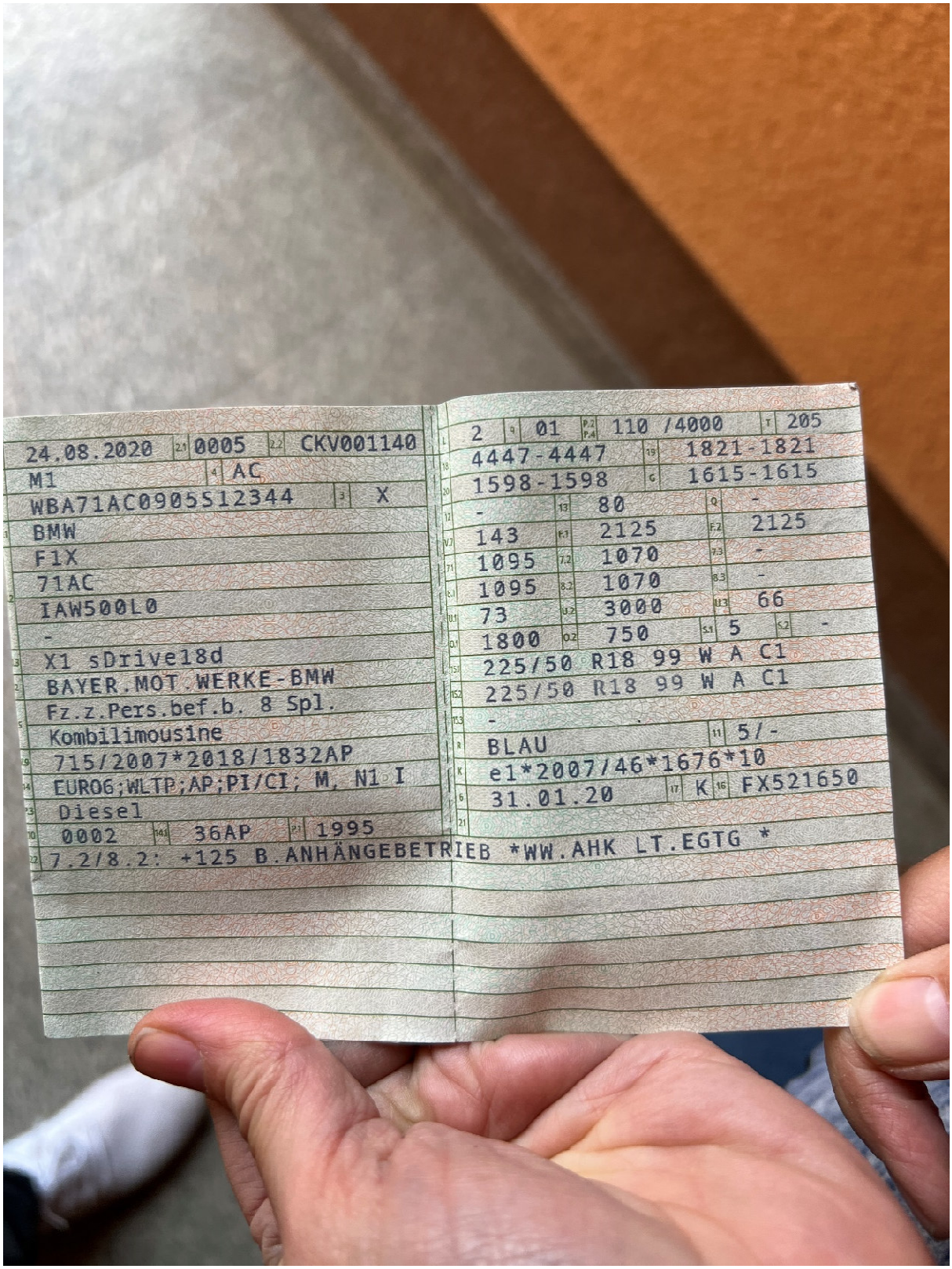
VI. Anlagen

Anlage 1: Zulassungsbescheinigung Teil 1 vom V01-Fahrzeug Audi A5 Cabriolet [eigene Darstellung]

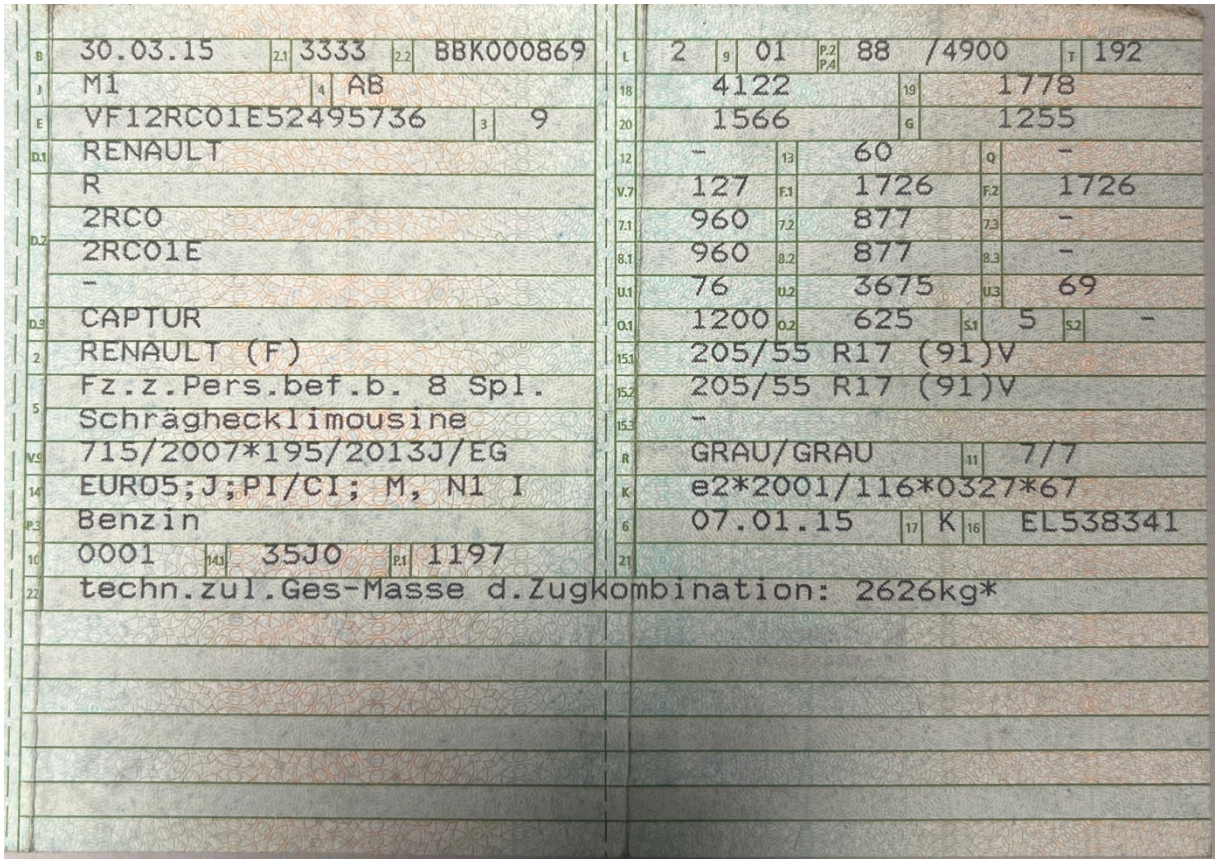


Anlage 2: Foto Innenraum vom V01-Fahrzeug Audi A5 Cabriolet [eigene Darstellung]

Anlage 3: Zulassungsbescheinigung Teil 1 vom V02-Fahrzeug BMW X1 [eigene Darstellung]



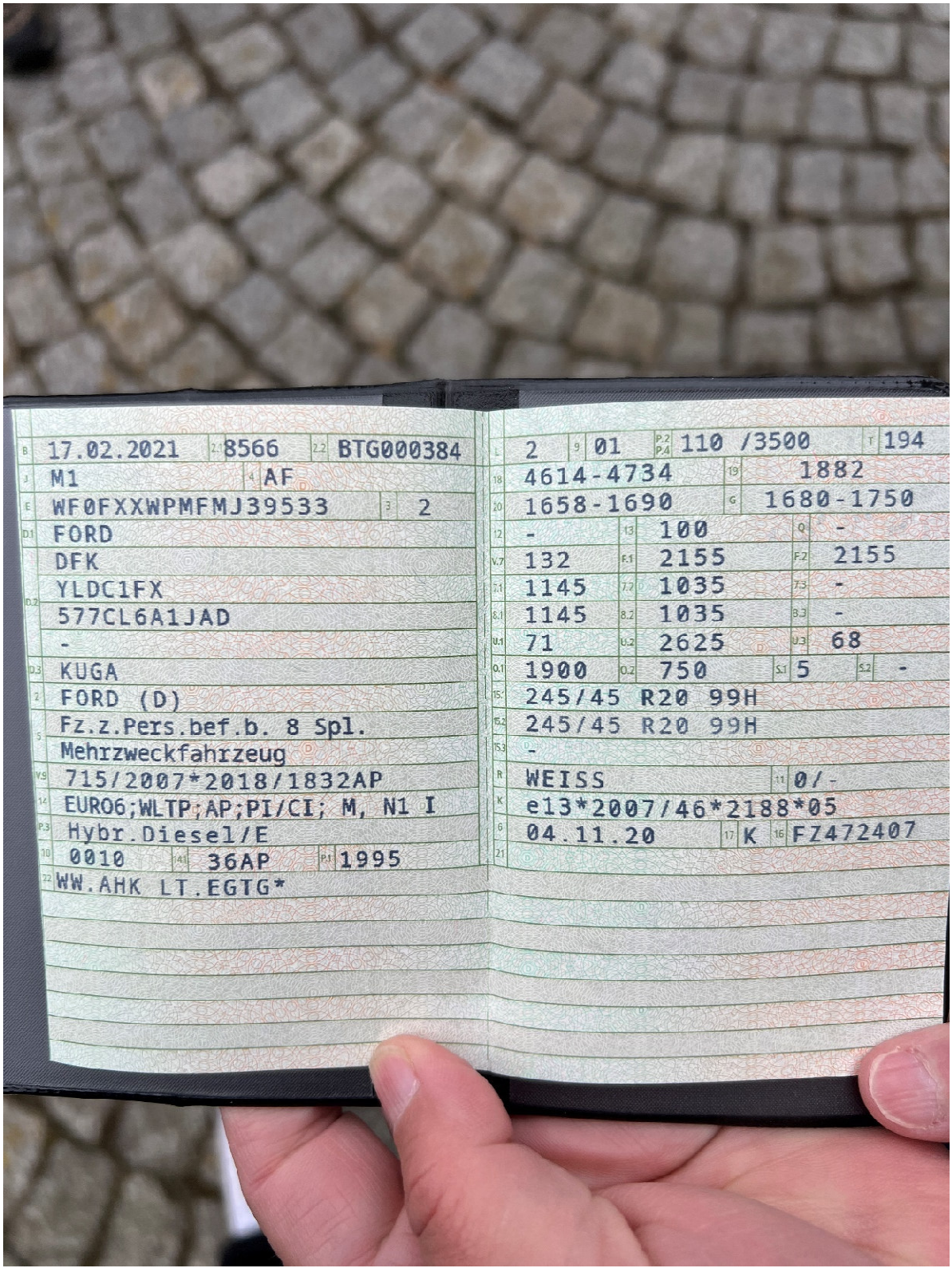
Anlage 4: Zulassungsbescheinigung Teil 1 vom V03-Fahrzeug Renault Captur [eigene Darstellung]



B	30.03.15	2.1	3333	2.2	BBK000869	L	2	9	01
J	M1	4	AB			18	4122		
E	VF12RC01E52495736	3	9			20	1566		
D.1	RENAULT					12	-	13	60
	R					V.7	127	F.1	1726
D.2	2RC0					7.1	960	7.2	877
	2RC01E					8.1	960	8.2	877
	-					U.1	76	U.2	3675
D.3	CAPTUR					0.1	1200	0.2	625
2	RENAULT (F)					15.1	205/55 R17 (91)V		
5	Fz.z.Pers.bef.b. 8 Spl.					15.2	205/55 R17 (91)V		
	Schrägheck limousine					15.3	-		
V.9	715/2007*195/2013J/EG					R	GRAU/GRAU	11	7/7
14	EURO5;J;PI/CI; M, N1 I					K	e2*2001/116*0327*67		
P.3	Benzin					6	07.01.15	17	K
10	0001	14.1	35JO	P.1	1197	21			
22	techn.zul.Ges-Masse d.Zugkombination: 2626kg*								

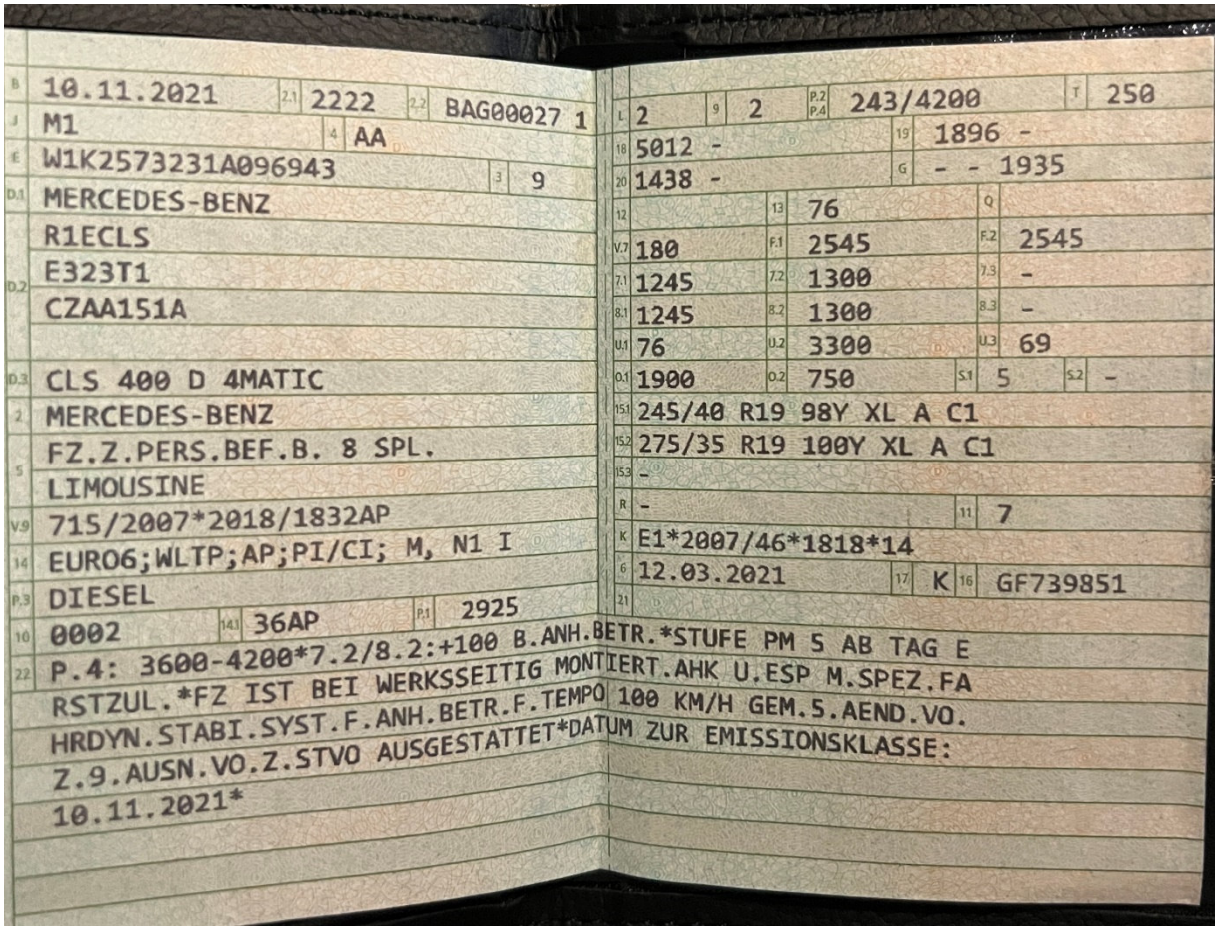
T	192				
19	1778				
G	1255				
Q	-				
F.2	1726				
7.3	-				
8.3	-				
U.3	69				
S.1	5	S.2	-		
16	EL538341				

Anlage 5: Zulassungsbescheinigung Teil 1 vom V04-Fahrzeug Ford Kuga [eigene Darstellung]

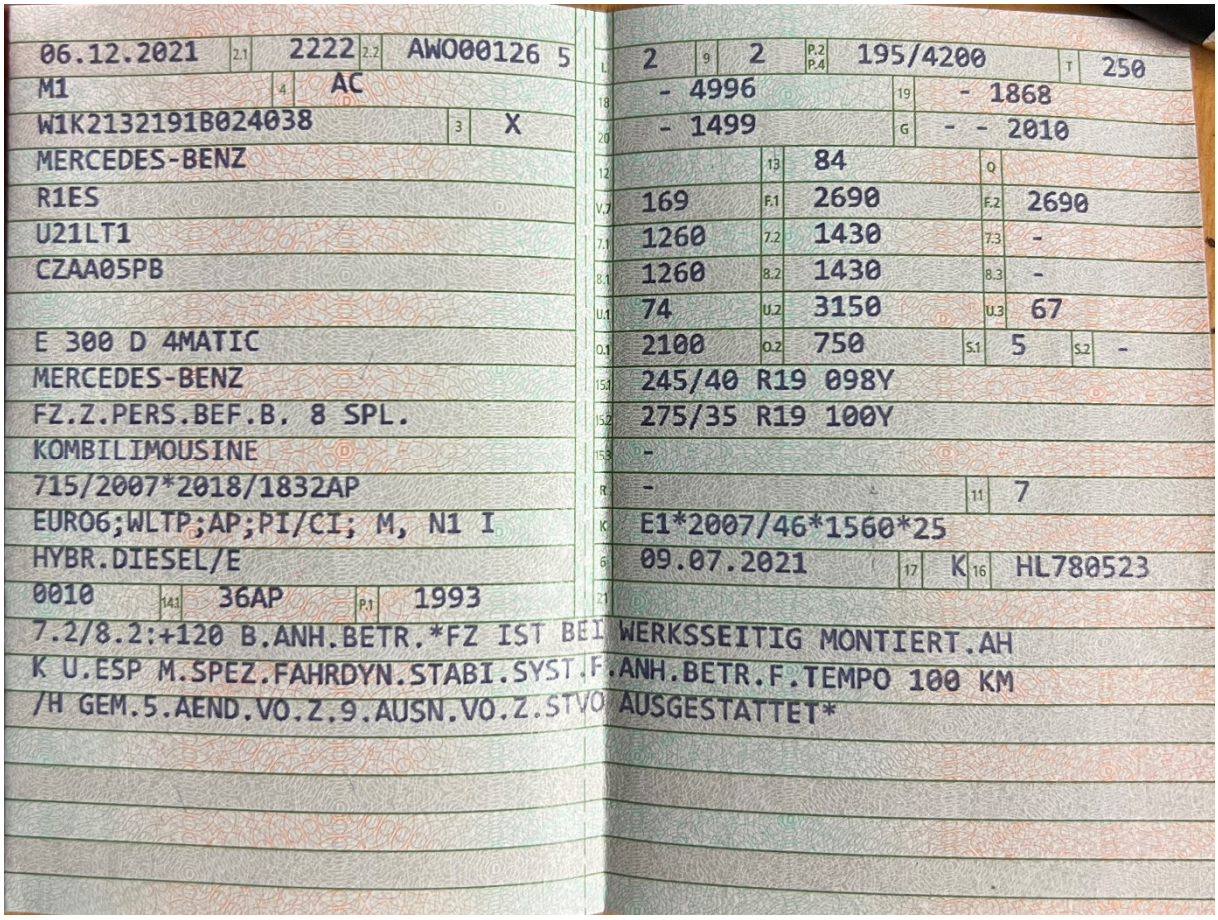


Anlage 6: Heckansicht vom V04-Fahrzeug Ford Kuga [eigene Darstellung]

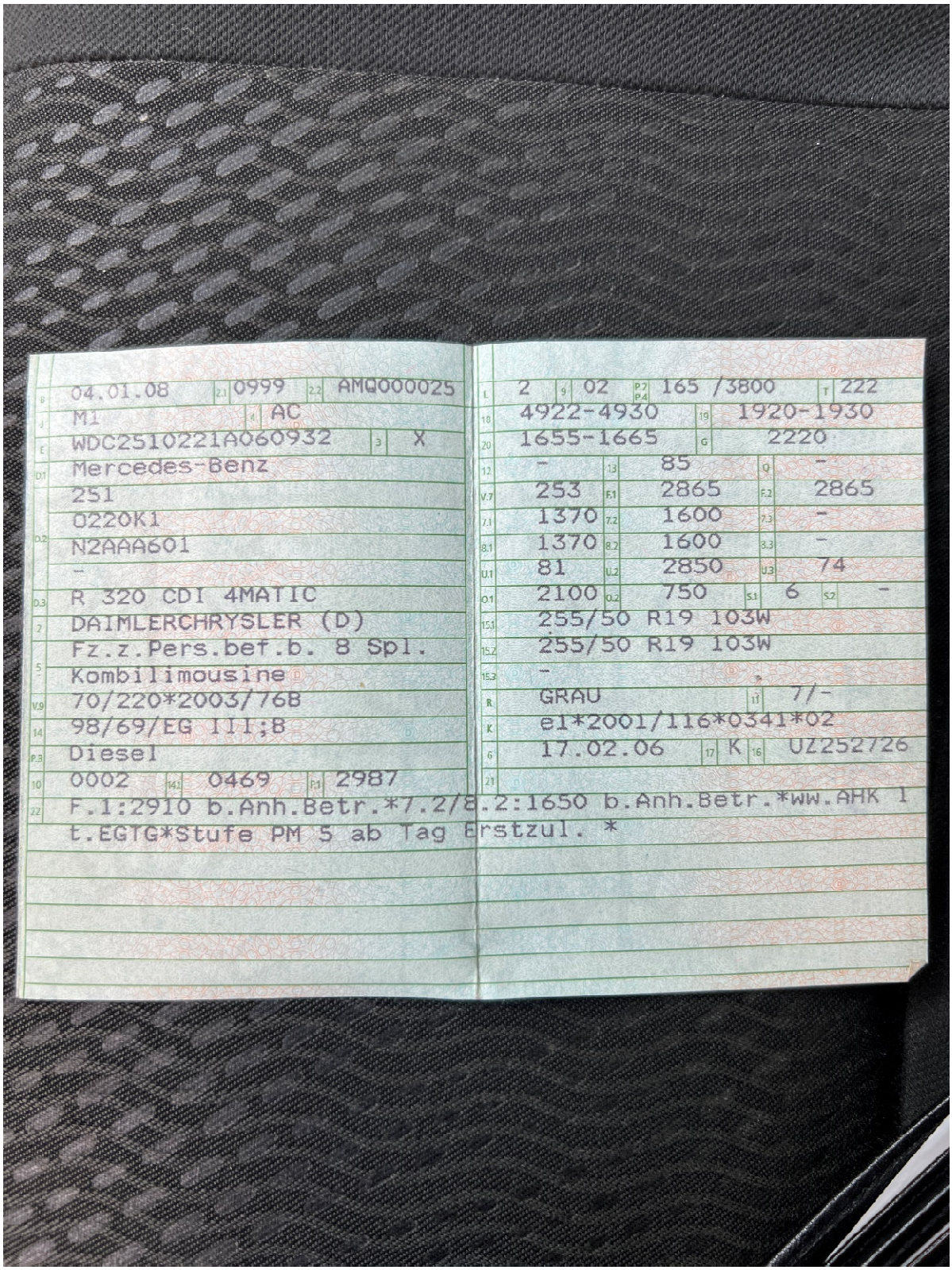
Anlage 7: Zulassungsbescheinigung Teil 1 vom V05-Fahrzeug Mercedes Benz CLS 400d [eigene Darstellung]



Anlage 8: Zulassungsbescheinigung Teil 1 vom V06-Fahrzeug Mercedes Benz E 300d [eigene Darstellung]



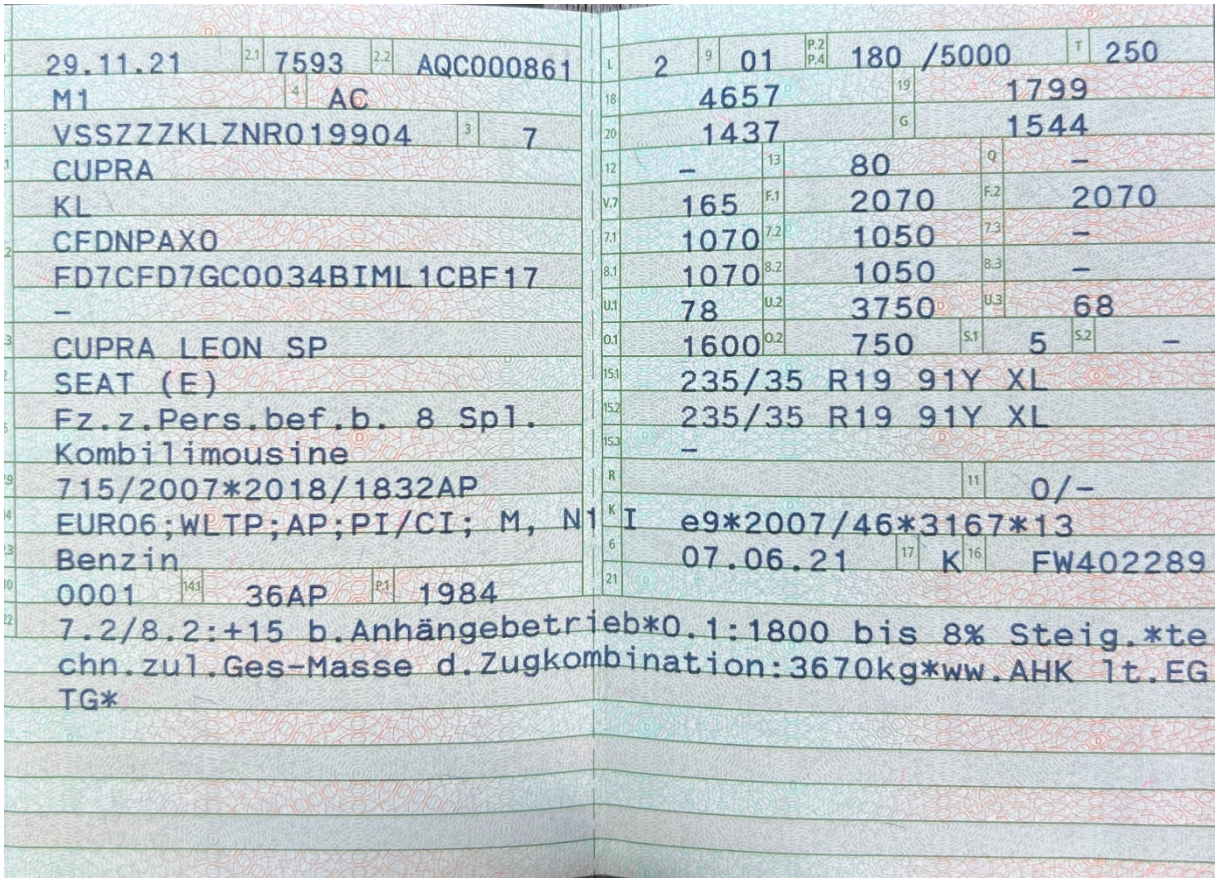
Anlage 9: Zulassungsbescheinigung Teil 1 vom V07-Fahrzeug Mercedes Benz R 320 CDI [eigene Darstellung]



Anlage 10: Heckansicht vom V07-Fahrzeug Mercedes Benz R 320 CDI [eigene Darstellung]

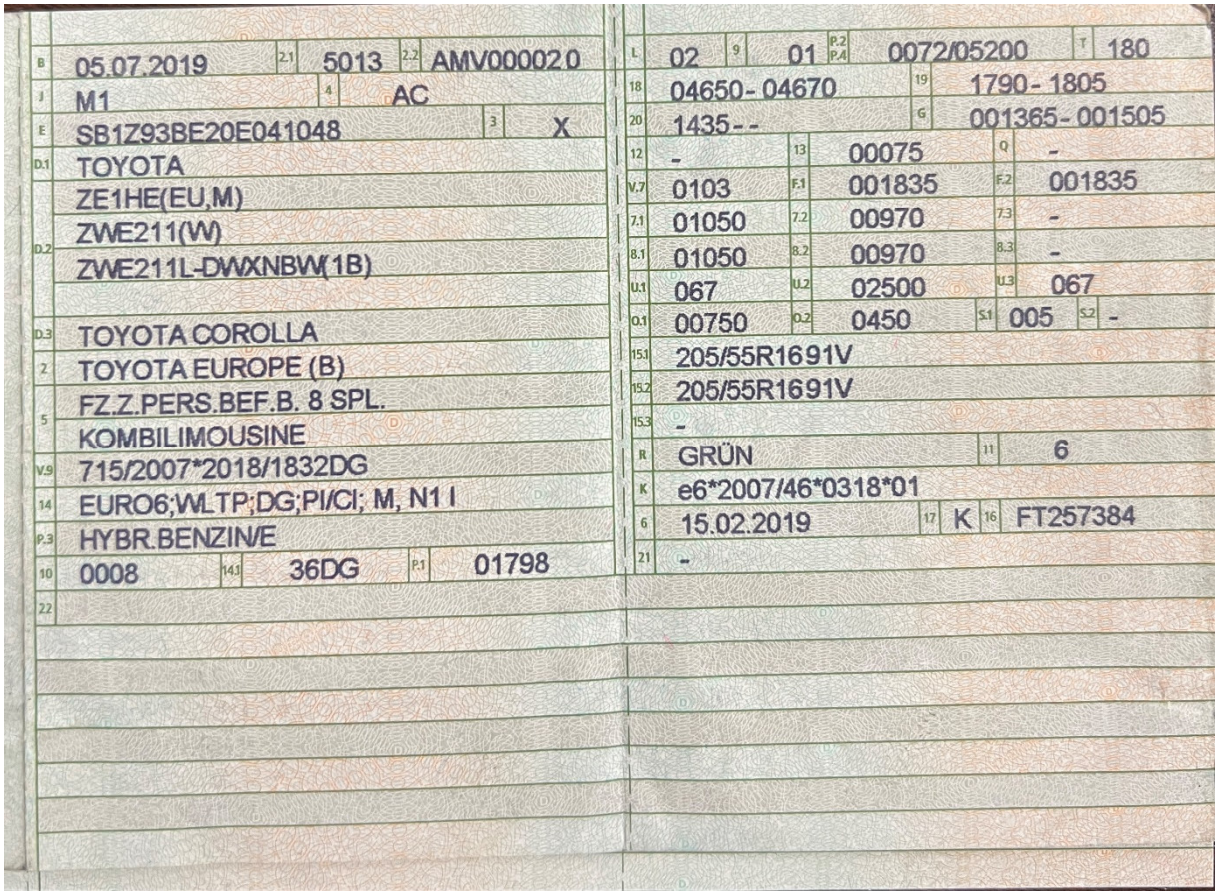
Anlage 11: Zulassungsbescheinigung Teil 1 vom V08-Fahrzeug Skoda Kodiaq [eigene Darstellung]

Anlage 12: Zulassungsbescheinigung Teil 1 vom V09-Fahrzeug Seat Cupra Leon SP [eigene Darstellung]



Anlage 13: Start-/Stopp-Knopf und gekennzeichnete Fläche für Schlüsselerkennung im Getränkehalter vom V09-Fahrzeug Seat Cupra Leon SP [eigene Darstellung]

Anlage 14: Zulassungsbescheinigung Teil 1 vom V10-Fahrzeug Toyota Corolla [eigene Darstellung]



B	05.07.2019	2.1	5013	2.2	AMV00002.0	L	02	9	01
J	M1	4	AC			18	04650 - 04670		
E	SB1Z93BE20E041048	3	X			20	1435 - -		
D.1	TOYOTA					12	-	13	00075
	ZE1HE(EU,M)					V.7	0103	F.1	001835
D.2	ZWE211(W)					7.1	01050	7.2	00970
	ZWE211L-DWXNBW(1B)					8.1	01050	8.2	00970
						U.1	067	U.2	02500
D.3	TOYOTA COROLLA					O.1	00750	O.2	0450
2	TOYOTA EUROPE (B)					15.1	205/55R16 91V		
5	FZ.Z.PERS.BEF.B. 8 SPL.					15.2	205/55R16 91V		
	KOMBILIMOUSINE					15.3	-		
V.9	715/2007*2018/1832DG					R	GRÜN		
14	EURO6;WLTP;DG;PI/CI; M, N1 I					K	e6*2007/46*0318*01		
P.3	HYBR.BENZIN/E					6	15.02.2019		
10	0008	14.1	36DG	P.1	01798	21	-		
22									

P.2 P.4	0072/05200	T	180						
19	1790 - 1805								
G	001365 - 001505								
Q	-								
F.2	001835								
7.3	-								
8.3	-								
U.3	067								
S.1	005	S.2	-						
11	6								
17	K	16	FT257384						