Abschirmtests an RFID-Systemen

Michael Raith (B.Sc.), *Student*

Zusammenfassung

RFID-Systeme haben heutzutage einen immer größeren Anreiz: Zugangskontrolle, Bezahlsysteme, Diebstahlsicherung oder Identifikation (Personalausweis, Pass) sind nur einige Bespiele. RFID-Systeme erleichtern Tätigkeiten, bringen jedoch auch sicherheitsrelevante Probleme mit sich.

Datenschützern sind RFID-Systeme schon lange ein Dorn im Auge, da dadurch die Privatsphäre des Trägers leichter ausgespäht und ein Bewegungsprofil erstellt werden kann. Der Schutz dieser Systeme und indirekt des Trägers durch Dritte ist unerlässlich. Aktuelle Zugangskontroll- und Identifikationssysteme verwenden neueste Sicherheitsfunktionen und Verschlüsselungen. Ist dieser Schutz nicht ausreichend genug, können RFID-Schutzhüllen das Auslesen durch Dritte erschweren oder gar komplett verhindern.

Im Internet werden kommerzielle Hüllen Angeboten, die Schutz bieten sollen. Die Wirkung dieser Schutzhüllen wird in der vorliegenden Arbeit analysiert. Zusätzlich werden die abschirmenden Eigenschaften von weiteren Materialien untersucht.

Die Arbeit ist in der Vorlesung „Spezielle Themen der mobilen Kommunikation“ bei Prof. Dr. Joachim Charzinski entstanden.

Indexbegriffe

RFID, passive Transponder, aktive Transponder, Niederfrequenz, Messung, Datenschutz, Schutz vor Auslesen, Schutzhülle, Reichweite

1 Einführung

Die „**R**adio **F**requency **Id**entification“ Technologie – kurz RFID – erlaubt die kontaktlose Übertragung und Speicherung von Daten auf Transpondern. Die Systembestandteile eines RFID-Systems sind mindestens ein Lesegerät und ein Transponder (siehe Abbildung 1). RFID wird eingesetzt, um schnell und automatisiert Daten von Objekten zu lesen und diese entsprechend weiterzuverarbeiten. Ein Einsatzgebiet ist das Markieren, Überwachen und Erkennen von Objekten z.B. in der Automobilindustrie, Produktion oder Logistik. Dadurch können Objekte in einem System überwacht werden und es kann zusätzlich überprüft werden, ob diese Objekte zur richtigen Zeit am richtigen Ort eintreffen. RFID bietet im Gegensatz zu anderen eingesetzten Verfahren und Systemen – z.B. Daten per Hand aufschreiben, Schrifterkennung oder Barcodes – den Vorteil, dass Daten auf das Medium zurückgespeichert werden können. Bei Barcodes ist dies so nicht möglich, ggf. kann es aber durch Neuerstellung des Barcodes erreicht werden.

Abbildung 1: RFID Systemaufbau

Ein Vorgänger von RFID wurde bereits im zweiten Weltkrieg für die Freund-Feind-Erkennung in Flugzeugen eingesetzt. Die eigentliche Geburtsstunde von RFID liegt in den 1950er Jahren, als in einer Publikation von Stockmann [1] beschrieben wird, wie die Energie von Radiosignalen zur Betreibung von RFID-Transpondern verwenden werden kann. Einer der ersten Verwendungszwecke war die Artikelabsicherung bzw. Diebstahlsicherung mit sogenannten ”1-Bit-Transpondern”. Diese senden in der Nähe eines entsprechenden Lesegeräts ein Signal und lösen dadurch einen Alarm aus. Weitere Entwicklungen sind der Türöffner per Chipkarte oder die Markierung von Waren in logistischen Bereichen. Im Laufe der Jahre hat sich die RFID-Technologie weiter entwickelt: Heutzutage ist es möglich, RFID Transponder direkt auf Folien zu drucken. Dadurch wird eine billige Massenfertigung gewährleistet.

In den vergangenen Jahren haben sich vermehrt RFID-Gegner etabliert. Sie bemängeln die Möglichkeit, Bewegungen von Objekten und Personen mit Hilfe von RFID erfassen zu können, und den unzureichenden Schutz der Verbraucher vor diesen Systemen. Es kann vorkommen, dass RFID Transponder beim Kauf von Waren unzureichend deaktiviert werden, wodurch eine Verfolgung der Käufer möglich wird.

Heutzutage haben immer mehr Chipkarten auch einen integrierten RFID Transponder. Die wenigstens Karteninhaber sind über diese versteckten Funktionen informiert. Liegen zusätzlich die Daten in unverschlüsselter Form

michael.raith@hdm-stuttgart.de, Computer Science and Media (Master), Fakultät Druck und Medien, Hochschule der Medien, Nobelstraße 10, D-70569 Stuttgart

auf der Karte, haben Kriminelle ein leichtes Spiel. Lesegeräte können schon mit einfachen Mitteln selbst gebaut werden. In einem möglichen Szenario könnten Kriminelle in dichten Menschenansammlungen, z.B. in öffentlichen Verkehrsmitteln, so leicht an Daten gelangen, die für sie von Interesse sind.

Diese Arbeit behandelt die RFID-Technik und gibt einen kurzen Überblick über die Technik in Abschnitt 2. In Abschnitt 3 werden mögliche Angriffsszenarien auf RFID-Systeme und Transponder vorgestellt.

Für die in Abschnitt 4 beschriebenen Tests wurde das RFID-Entwicklungskit von Atmel eingesetzt. Dabei wird mit diesem RFID-Entwicklungskit die mögliche Auslesereichweite ermittelt, wie diese zu steigern ist und wodurch das Auslesen von RFID-Transpondern erschwert oder gar komplett verhindert werden kann.

Die Ergebnisse werden in Abschnitt 5 vorgestellt und bewertet.

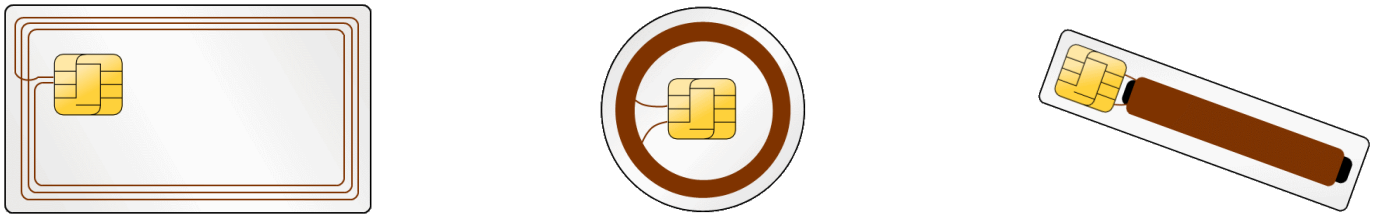
2 RFID Technik

2.1 Frequenzen & Reichweite

RFID Transponder werden heutzutage für die unterschiedlichsten Zwecke benutzt. Dafür gibt es verschiedene Frequenzbänder, die Vor- und Nachteile bieten. Eine Auflistung über die aktuell verwendeten Frequenzbänder, deren Reichweiten, Einsatzgebiete und Eigenschaften ist in Tabelle 1 zu finden.

2.2 Bauformen

RFID Transponder gibt es in vielen Größen und Ausführungen. Drei der verbreitetsten Formen sind in Abbildung 2 zu sehen. Viele moderne Zugangskontrollsysteme basieren auf Chipkarten- (2a) und „Münzen“-Transpondern (2b). Durch ihre relativ große Fläche kann im Vergleich zum Transponder in Abbildung 2c eine größere Antenne verwendet werden, wodurch die Reichweite und Übertragungsqualität gesteigert wird. Ein ebenfalls weit verbreiteter Transponder ist der Glaskolben (2c). Dieser ist sehr klein und kann direkt unter die Haut gepflanzt werden. Diese Transponder werden hauptsächlich für die Identifikation von Tieren eingesetzt. Es gibt jedoch auch schon Feldversuche, diese Transponder Menschen unter die Haut zu pflanzen [5], um z.B. Gesundheitsdaten darauf zu speichern.



(a) Chipkartenform (b) Münzen (c) Glaskolben

Abbildung 2: Verschiedene RFID Bauformen

(Der Chip in den Abbildungen dient nur zur Veranschaulichung und kann vom Original abweichen. Die Transponder in den Abbildungen sind nicht maßstabsgetreu.)

2.3 Speicherkapazität

Bevor auf die Speicher im Detail eingegangen werden kann, müssen noch zwei grundlegende Transponder-Typen unterschieden werden [4, Kap. 2.6.4]:

- **Read-Only-Transponder (ROM[1])**: Diese Transponder werden bei der Herstellung programmiert und können danach nur noch mit einem Lesegerät ausgelesen werden. Diese Variante ist in der Herstellung kostengünstig.
- **Read-Write-Transponder (RAM[2] oder EEPROM[3])**: Diese Transponder können mit individuellen Daten nach der Herstellung beschrieben werden. Dadurch steigt der Anwendungsbereich dieser Transponder, jedoch sind die Herstellungskosten höher.

RFID-Transponder mit ROM-Speichertechnologie werden vor allem zum Markieren von Objekten verwendet. Dabei wird die Transponder-ID in Zusammenhang mit dem Objekt in einer zentralen Datenbank gespeichert. Ein weiteres Beispiel für Transponder mit ROM-Speicher ist der Diebstahlschutz von Produkten.

1. **R**ead-**O**nly-**M**emory
2. **R**andom-**A**ccess-**M**emory
3. **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory

Tabelle 1: RFID Frequenzen, Reichweiten, Einsatzgebiete und Eigenschaften
([2], [3, Kap. 4.4.1, 4.4.2] und [4, Kap. 2.3, 2.6.1, 2.6.2])

Frequenz	**Frequenzbereich**	**Reichweite** [a]	**Einsatzbereiche**	**Vorteile**	**Nachteile**
Niederfrequenz (LF)	100 - 135 kHz	10-15 cm	Zugangskontrolle, Logistik, Tieridentifikation	• Einsatz von günstigen Transpondern • durchdringt gut nicht-metallische Gegenstände z.B. Wasser oder organisches Material • Frequenzband weltweit verfügbar	• große Transponder-Bauformen • geringe Datenkapazität • geringe Übertragungsgeschwindigkeit
Hochfrequenz (HF)	13,56 MHz	1,5 m	Lagerverwaltung, Logistik, Büchereien, Pakete, Gepäckkontrolle	• Einsatz von günstigen Transpondern • höhere Datenkapazität • Frequenzband weltweit verfügbar	• hohe Dämpfung durch metallische Umgebung • Lesereichweite beschränkt • große Reichweiten erfordern große Antennen
Ultrahochfrequenz (UHF)	860 - 960 MHz	7 m	Logistik, Nachverfolgung, Handel	• große Reichweite • einfaches Antennendesign • kostengünstig	• schlechte Durchdringung von Wasser und organischen Materialien
Mikrowellen (MW) Superultrahochfrequenz (SUHF)	2,45 GHz, 5,8 GHz	10 m	Mautsysteme [b]	• hohe Datenübertragung • hohe Reichweite	• große Bauform • hohe Kosten • aktiver Transponder, benötigt Stromversorgung

a. bei aktiven Transpondern kann die Reichweite höher liegen
b. Einsatz für sich schnell bewegende Objekte z.B. Autos, LKWs

Sollen jedoch Daten zurück auf den Chip geschrieben werden, benötigt dieser einen wieder beschreibbares Speichermedium. In einem passiven RFID-Chips kommen hauptsächlich EEPROM-Speicher mit einer Kapazität von 16 Byte bis 8 kByte zum Einsatz. Handelt es sich um einen aktiven RFID-Chip, können RAM Speichermodule verwendet werden (diese benötigen eine kontinuierliche Stromversorgung). Dadurch sind beliebige Speicherkapazitäten möglich. Üblicherweise werden jedoch Kapazitäten im Bereich von 256 Byte bis 64 kByte angeboten.

Zusätzlich gibt es zu den ROM, RAM oder EEPROM Speichermodulen Prozessoren, die kryptografische Operationen auf die Daten im Speicher ausführen z.B. um eine verschlüsselte Antwort an das Lesegerät zurückzusenden.

2.4 Energieversorgung

RFID-Chips können auf zwei unterschiedliche Weisen mit Energie versorgt werden [4, Kap. 2.4]:

- ***Passive* Transponder** werden erst beim Lesevorgang über das Lesegerät mit Energie versorgt. Die Reichweite bei diesen Transpondern ist geringer, da nicht nur die Daten übertragen werden müssen, sondern auch die Energie in den Empfänger induziert werden muss. Aus diesem Grund muss das Lesegerät besonders leistungsstark sein. Abbildung 3 enthält einen Beispiel-Aufbau eines passiven Transponders.
- ***Aktive* Transponder** besitzen eine Energiequelle (Batterie). Diese Transponder sind so lange inaktiv, bis sie von einem Lesegerät ein Aktivierungssignal erhalten. Die Reichweite ist bei aktiven Systemen um ein Vielfaches größer, da die Transponder mit einer höheren Leistung Daten zurück an das Lesegerät schicken können.

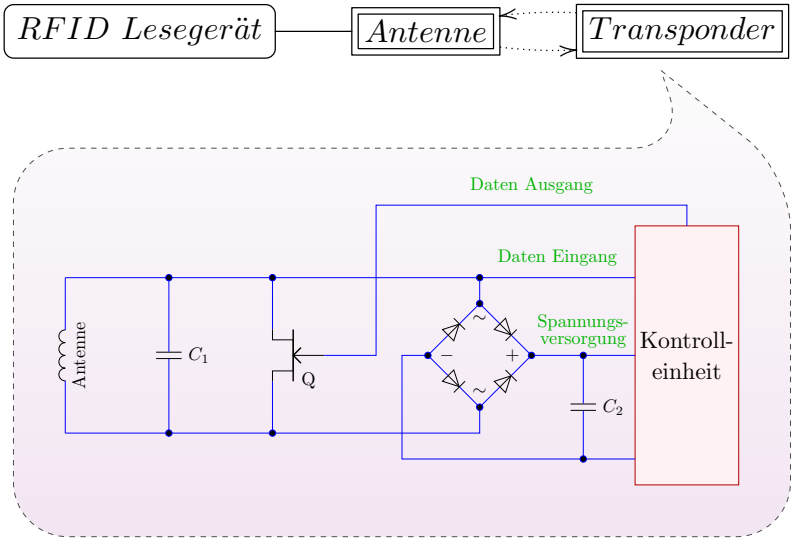


Abbildung 3: RFID Energierversorgung, Beispiel: passiver Transponder (vgl. [6])

2.5 Übertragunsverfahren

Für die Kommunikation zwischen Lesegerät und Transponder gibt es drei unterschiedliche Übertragungsverfahren: Halbduplex, Vollduplex und sequentielle Datenübertragung.

- **Halbduplex**: Das Lesegerät und der Transponder senden bei dieser Datenübertragung die Daten abwechselnd. Bei diesem Verfahren wird häufig Lastmodulation eingesetzt, die das Feld des Lesegeräts beeinflusst. Das Lesegerät empfängt anhand dieser Veränderungen im Feld Daten des Transponders.
- **Vollduplex:** Bei der Vollduplex-Übertragung senden Lesegerät und Transponder gleichzeitig Daten. Die gleichzeitige Übertragung wird durch unterschiedliche Frequenzen oder Codemodulation erreicht.
- **Sequentiell**: Bei Systemen mit sequentieller Datenübertragung wird nur während des Sendevorgangs des Lesegeräts Energie an den Transponder übertragen. Um Antwortdaten zurück an das Lesegerät zu schicken, benötigt der Transponder einen Energiepuffer (Kondensator) oder der Transponder muss aktiv gestützt sein (z.B. durch eine Batterie).

Die Voll- und Halbduplex Übertragung haben eines gemeinsam: Das Lesegerät sendet kontinuierlich ein Feld für die Energieversorgung des Transponders aus, welches unabhängig von der Richtung des Datenflusses ist. Dies gilt jedoch nur für passive Transponder, da aktive Transponder z.B. durch eine Batterie gestützt sind und dadurch keine induzierte Energie für den Betrieb benötigen.

Die drei Übertragungsverfahren sind in Abbildung 4 dargestellt.

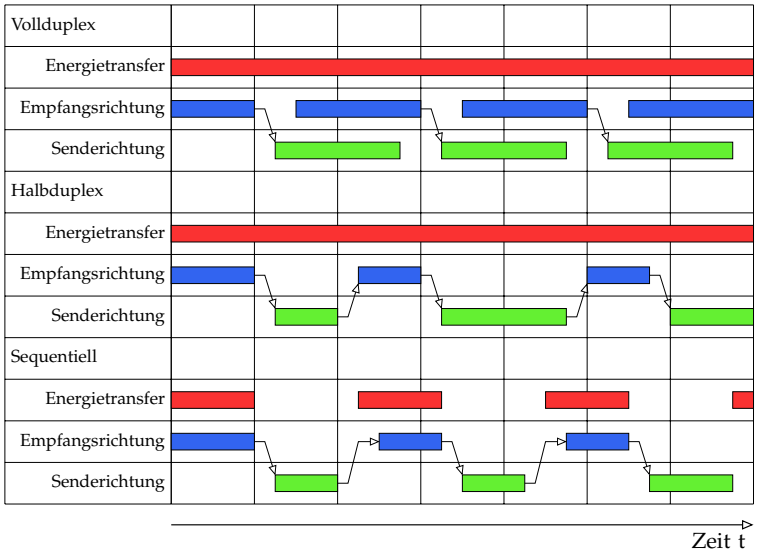


Abbildung 4: Voll-, Halbduplex und sequentielle Datenübertragung (vgl. [4, Kap. 3.2])

2.6 Sicherheit

Heutzutage werden Zugänge zu geschützten Bereichen vermehrt mit Hilfe von RFID-Systemen realisiert. Um das Ausspähen von Transpondern und das unbemerkte Kopieren von sensiblen Daten zu vermeiden, müssen solche Zugangssysteme mit kryptografischen Funktionen ausgestattet sein. Deshalb ist es wichtig, dass Dritte keinen Lese-, geschweige denn Schreibzugriff auf den Transponder erlangen. Außerdem dürfen sich Dritte nicht mit Transponder-Kopien am System autorisieren.

Um die Echtheit von Transponder-Daten zu gewährleisten, kann z.B. nur der Lesezugriff auf einen Transponder erlaubt werden. Die Transponder werden bei der Herstellung initial mit den gewünschten Daten beschrieben und können danach nicht mehr verändert werden. Zusätzliche Sicherheit kann erreicht werden, wenn das Lesegerät dem Transponder eine Signatur sendet, die aus gegebenen Daten generiert wird z.B. Name, Vorname, ... die aufgedruckt auf der RFID-Karte stehen. Diese Signatur wird mit einer bereits vorhandenen und nicht veränderbaren Signatur im Transponder-Chip verglichen. Stimmen die Signaturen überein, gibt der Transponder zusätzliche Daten frei und sendet diese zurück an das Lesegerät. Dieses Verfahren wird *Challenge-Response-Verfahren* genannt und kommt u.a. beim deutschen ePass eingesetzt [7] zum Einsatz.

Soll hingegen die komplette Datenübertagung vor Dritten geschützt werden, muss ein Verschlüsselungsverfahren eingesetzt werden. Dazu können sowohl symmetrische als auch asymmetrische Verschlüsseungsverfahren eingesetzt werden. Hierbei ist zu beachten, dass die Anschaffungskosten für solche Systeme höher sind. Außerdem sind RFID-Systeme mit kompromittierter Verschlüsselung oder gestohlenen asymmetrischen Schlüsseln nicht mehr sicher und müssen ggf. komplett ersetzt werden. Deutsche Forscher der Universität Bochum haben erst vor kurzem „Mifare“ Transponder mit 3DES[4] Verschlüsselung geknackt[5] [8].

Für RFID-Systeme die z.B. in Industrieanlagen verwendetet werden, sind Sicherheitsfunktionen in der Regel überflüssig und würden nur die Anschaffungskosten unnötig erhöhen.

3 Angriffe

In den vergangenen Jahren hat der Einsatz von RFID-Systemen stark zugenommen. Die billige Massenproduktion der Transponder hat diesen Trend begünstigt. Weltweit haben sich jedoch auch immer mehr Bürgerinitiativen gebildet, die strengere RFID-Gesetzte und Richtlinien für den Verbraucherschutz fordern. In den USA wurde bereits der Versuch unternommen, ein RFID-Gesetz zu verabschieden [4, Kap. 8].

Mit Hilfe selbstgebauter Lesegeräte kann auf viele Transponder lesend zugegriffen werden. Dritte können dadurch aus einer näheren Entfernung sehr leicht an Daten von Interesse gelangen. Um sich vor ungewolltem Auslesen zu schützen, gibt es verschiedene Angriffsmethoden, um RFID-Transponder außer Funktion zu setzten.

Die einfachste Art, Transponder anzugreifen und zu zerstören, ist mechanische Gewalt z.B. ein Schlag mit einem Hammer oder Durchtrennen der Antenne. Diese Angriffe sind jedoch nur wirksam, falls der Transponder lokalisiert

4. 3DES oder Triple-DES ist ein Verschlüsselungsverfahren, bei dem ein Datenblock mit dem „**D**ata **E**ncryption **S**tandard“-Algorithmus dreimal mit verschiedenen Schlüsseln verschlüsselt wird.

5. Bei diesem Versuch haben die Forscher *Oswald* und *Paar* den Schlüssel über eine Seitenkanalattacke (Messung des Stromverbrauchs beim ver- und entschlüsseln) geklaut, wodurch die Schutzmaßnahmen des Transponders umgangen wurden.

werden kann. Transponder können jedoch auch in Kleidungsstücken oder sonstigen Materialien versteckt sein. Da einige Transponder sogar den härtesten Malträtierungen standhalten z.B. industriellen Waschmaschinen, bedarf es raffinierterer Angriffe. Deshalb werden in diesem Abschnitt einige kritische Angriffe vorgestellt, um Transponder kontaktlos zu manipulieren, zu stören oder zu zerstören.

3.1 Störfelder

Heutzutage gibt es eine Vielzahl von Anwendungenen, die mit Funkwellen arbeiten. Dabei werden sich Überschneidungen oder Überlagerungen dieser Frequenzbänder ergeben. Es gibt Fälle, in denen Frequenzbänder absichtlich und mit destruktiven Absichten überlagert werden. Mit ausreichender Leistung können RFID-Systeme mit Hilfe eines „Störsenders“ beeinträchtigt oder komplett außer Funktion gesetzt werden.

Um ein Lesegerät zu stören, bedarf es einiger Anstrengungen: Der Störsender sollte mindestens den gleichen Abstand, Leistung und Antennendurchmesser besitzen. Die optimale Position des Störsenders ist in der Nähe des zu störenden Lesegeräts. Da dies nicht immer möglich ist, muss bei einem Störsender das Produkt aus Sendeleistung und Antennengewinn die durch den größeren Abstand zur störenden Antenne verursachte Dämpfung kompensieren.

Transponder können hingegen einfacher gestört werden, da diese normalerweise nur wenige Milliwatt Leistung an ihrer Antenne aufnehmen und mit noch geringerer Leistung Antwortdaten senden.

Hinweis: Ein Störsender stellt eine Funkanlage dar. Der Betrieb solcher Anlagen ist in einigen Länder ohne Genehmigung illegal.

3.2 Mitlesen der Daten

RFID-Systeme arbeiten mit unterschiedlichen Frequenzen, Leistungen und Auslesereichweiten (siehe Tabelle 1). Ein Angreifer könnte in der Nähe des eigentlichen Lesegeräts sein eigenes Lesegerät aufstellen und so die Übertragung mithören. Die maximalen Reichweiten von LF-Systemen sind mit 10–15 cm (ISO 14443)[6], die von HF-Systemen mit 1,5 m (ISO 15693)[7] spezifiziert. Diese Reichweiten-Spezifikationen gelten nur für den bestimmungsgemäßen Gebrauch von RFID-Systemen / -Transpondern und nicht für selbst gebaute Antennen und sonstige selbst entwickelte elektronische Geräte.

Laut der Studie [9] ist es bereits mit passiven Abhörverfahren[8] möglich, Transponder über mehrere Meter hinweg auszulesen.

3.3 Täuschen

RFID-Systeme können auf zwei Arten getäuscht werden:

1) Den Transpondern wird ein Lesegerät vorgegaukelt, das von Angreifern betrieben wird. Unzureichend geschützte Transponder können dadurch wertvolle Informationen preisgeben.
2) Das Lesegerät bekommt manipulierte Transponder zu lesen. Dieser Fall wird im nächsten Abschnitt 3.4 näher erläutert.

3.4 Transponder kopieren

Durch Eins-zu-Eins-kopieren können exakte Kopien von Transpondern angefertigt werden. Auf viele Transponder, die zur Identifikation oder Verfolgung von Objekten dienen, kann ohne weiteres lesend zugegriffen werden. Diese Transponder senden, sobald sie in der Nähe eines entsprechenden Lesegerätes sind, ihre Seriennummer oder einzigartige Kennung aus. Aus diesen Information lassen sich mit der entsprechenden Hardware problemlos Kopien anfertigen. Diese Transponder-Klone können wiederum in das Feld eines Lesegeräts gehalten werden, wodurch sie dem Lesegerät den echten Transponder vorgaukeln. Dadurch kann Verwirrung z.B. in einem Transport- oder Logistik-System entstehen, da es anscheinend ein Objekt zwei Mal gibt. Bei einer unzureichenden Implementierung der Transponder-Verwaltungssoftware sind auch komplette Ausfälle des Systems vorstellbar.

Handelt es sich bei dem kopierten Transponder um ein Zugangskontrollsystem und ist dieser Transponder unzureichend kryptografisch geschützt, können die Ausmaße des Schadens verheerend sein: Unbefugte erhalten Zugriff zu geschützten Bereichen, beim Manipulieren von Daten können im schlimmsten Fall sogar Identitäten gefälscht werden. Das Manipulieren von Daten ist in einigen Fällen sogar relativ einfach möglich, da einige Transponder ohne Passwort oder Schlüsselabfrage den (Schreib-) Zugriff auf geschützte Bereiche erlauben.

6. ISO 14443 (Proximity Coupling): Die Norm beschreibt den Systemaufbau und Kommunikation der Komponenten. Einsatzgebiet: Zugriffskontrollsysteme, Smart Labels.
7. ISO 15693 (Vicinity Coupling): Ähnlich wie ISO 14443, jedoch mit höherer Reichweite und Übertragungsrate.
8. „passives Abhören“ → mithören von Signalen ohne selbst Signale zu senden

Das Gefährliche an diesem Angriff ist, dass der Angreifer keinen physischen Kontakt zu dem zu klonenden Transponder benötigt. Um sich effektiv vor Klonen zu schützen, sollten Transponder mit sicherheitsrelevanten Daten und Funktionen nur in Kombination mit kryptografischen Eigenschaften eingesetzt werden ([4, Kap. 8.1.1.3]). Zusätzlich können abschirmende Hüllen den Endbenutzer vor ungewollten Lesezugriffen schützen (siehe 4.6).

3.5 Entfernung des Transponders

RFID-Transponder dienen zur Identifikation von Objekten, zum Abspeichern Objekt-bezogener Daten und zum Abgleich dieser Daten z.B. mit einem Datenbanksystem. Ein sehr einfacher Angriff ist das Entfernen des Transponders von seinem Objekt. Dadurch ist die Zuordnung zwischen Objekt und den Informationen über das Objekt nicht mehr gegeben. Automatisierte Systeme können dadurch beeinträchtigt oder komplett außer Funktion gesetzt werden. Diese Art des Angriffs könnte für den Diebstahl von Waren verwendet werden.

3.6 Aushebeln des Diebstahlschutzes

Mit Hilfe von absorbierenden Materialien, z.B. mit dem vorgestellten Cryptalloy oder der Aluminiumfolie (siehe Abschnitt 4.6), können theoretisch Diebstahlschutz-Transponder manipuliert werden. Dazu wird der Transponder der Ware oder des Objekts lokalisiert und dieser mit Hilfe einer Schutzhülle vor dem Lesegerät versteckt. Dadurch können theoretisch Transponder außer Funktion gesetzt und die Ware ohne weiteres gestohlen werden. Dies ist nur eine theoretische Annahme, die aufgrund unzureichender Mittel und einer ungeeigneten Testumgebung nicht überprüft werden konnte.

3.7 Transponder unerlaubt deaktivieren

RFID Transponder, die für den Diebstahlschutz eingesetzt werden, besitzen einen so genannten „kill"-Befehl. Dadurch kann der Transpondern beim Kauf eines Produktes deaktiviert werden, so dass beim Verlassen des Geschäfts kein Alarm ausgelöst wird. Ein Angreifer könnte sich diesen Befehl zu Nutze machen und Transponder im Geschäft deaktivieren, wodurch ein unbemerkter Diebstahl möglich ist. Dieser Angriff ist jedoch nur bedingt möglich, da zur Ausführung autorisierte RFID-Schreib-/Lesegeräte nötig sind.

3.8 Zu hohe induzierte Leistung

RFID-Systeme arbeiten mit einer geringen Sendeleistung von einigen Milliwatt. Bei einem induktiven RFID-System werden die Daten und die Energie über eine Spule im Lesegerät und Transponder über das Medium Luft gesendet und empfangen. Spulen in alltäglichen Geräten, z.B. in Transformatoren, können bei hoher Leistung warm werden oder im schlimmsten Fall komplett zerstört werden. Theoretisch sollte es möglich sein, Transponder mit einer zu hohen Leistung außer Kraft zu setzen oder gar komplett zu zerstören. Ein starker elektromagnetischer Impuls sollte dazu ausreichend sein. Dadurch ergibt sich jedoch ein weiteres Problem: Welche Strahlungsleistung halten Menschen als Träger oder andere empfindliche Gegenstände in der Gegenwart der Transponder aus?

Mit Hilfe eines Mikrowellenofens sollte ein Transponder zerstört werden können, wobei bei diesem Ansatz eher der Chip auf dem Transponder direkt zerstört wird als über die induzierte Leistung. Dieser Ansatz ist zudem fraglich, da im alltäglichen Leben außerhalb eines geschützten Mikrowellengeräts zusätzlich zum Transponder höchstwahrscheinlich auch der Träger Schaden nehmen kann.

Für induktive RFID-Systeme sind für die Transponder laut ISO 14443 oder ISO 15693 bei einer Frequenz von 13,56 MHz eine maximale Feldstärke von 12 A/m spezifiziert [4, Kap. 8.1.1.1]. Wird dieser Wert überschritten, kann die induzierte Leistung und die dadurch entstehende Wärme nicht mehr abgeführt werden, wodurch der Transponder letztendlich zerstört wird.

Der so genannte „Zapper" ist ebenfalls ein häufig diskutiertes Gerät, um RFID-Transponder außer Funktion zu setzten. Dazu wird eine Einweg-Fotokamera benötigt und der Kamerablitz dieser Kamera durch eine Spule ersetzt [10]. Diese Spule wird nun in die Nähe eines Transponders gebracht und mit der hohen Leistung der Blitzelektronik entladen. Für einen kurzen Moment erzeugt die Spule dadurch ein sehr großes elektromagnetisches Feld, welches den Transponder zerstört.

3.9 DoS-Attacke

Bei einer DoS[9]-Attacke wird das System mit Anfragen überflutet, so dass das Lesegerät überfordert ist und die eigentlichen Lesevorgänge nicht mehr stattfinden können.

9. Bei einer „**D**enial **o**f **S**ervice"-Attacke wird ein System (un-) gewollt durch Überlastung außer Funktion gesetzt.

In RFID-Systemen wird dazu ein so genannter „Blocker"-Tag eingesetzt. Dieser gaukelt dem Lesegerät eine Vielzahl an Transpondern vor. Das Lesegerät merkt dies und versucht mit Anti-Kollisions-Algorithmen die Transponder nacheinander auszulesen. Da die Transponder nur Pseudo-Transponder des Blocker-Tags sind, benötigt die Abfrage aller Transponder viel Zeit. Dadurch ist das Lesegerät für einen längeren Zeitraum außer Funktion gesetzt.

Eine weitere Methode ist das Versenden von fehlerhaften Datenpaketen oder falschen Prüfsummen. Durch diese Pakete ist das Lesegerät ebenfalls eine Zeit lang blockiert.

3.10 Angriffe auf Hintergrundsysteme

Es gibt Transponder, sogenannte „Tags", die nur für die Identifikation von Objekten dienen. Diese Tags können nur gelesen werden und enthalten in der Regel eine einfache Nummern- oder Zeichenfolge. Ein Tag wird einmalig an einem System registriert und mit dem zugehörigen Objekt in einer Datenbank vermerkt.

Ein weiterer Angriff könnte nun unabhängig von den Transpondern oder Lesegeräten auf die Hintergrundsysteme gerichtet sein. Werden in der Verwaltungsdatenbank Einträge und Zuordnungen manipuliert, so ist eine korrekte Identifikation von Objekten nicht mehr möglich. Objekte und Zugehörigkeiten können umdeklariert werden, ihren Besitzer wechseln, das System verwirren und komplett außer Funktion setzen.

Da diese Art von Angriff nur einen indirekten Zusammenhang mit RFID-Systemen hat, wird an dieser Stelle nur die Problematik erwähnt und nicht im Detail erläutert.

4 TESTS & MESSUNGEN

In den folgenden Versuchen wird untersucht, auf welche Distanzen sich moderne RFID Transponder auslesen lassen und wie mit herkömmlichen Mitteln die Reichweite der Antenne erhöht werden kann.

Der nächste Schritt ist der Schutz der RFID Transponder vor ungewolltem Auslesen (z.B. durch Dritte). Dazu wird der Transponder mit unterschiedlichen Materialien umgeben und die abschirmende Wirkung untersucht (siehe 4.6).

4.1 Atmel RFID Entwicklungskit

In den Versuchen wird das Atmel Entwicklungskit „LF RFID Application Kit ATA2270-EK1" eingesetzt, dass einen einfachen Einstieg in die Entwicklung von RFID Systemen bietet. Das Entwicklungskit besteht u.a. aus einer Hauptplatine mit einem Display, einem Joystick zum Navigieren durch die Menüs und IO-Anschlüssen. Zusätzlich liegen bereits RFID-Transponder unterschiedlichster Typen und Bauarten bei.

Das System ist so vorkonfiguriert, dass nur die Antenne und eine Stromversorgung angeschlossen werden muss. Über das Menü können direkt einfache Funktionen im Entwicklungskit ausgeführt werden, z.B. das Einrichten eines RFID-Tags oder Lese- / Schreiboperationen auf RFID-Transpondern. Zusätzlich kann das Entwicklungskit mit anderen Atmel Komponenten z.B. über JTAG[10] oder mit einem PC über die serielle Schnittstelle verbunden werden.

Das Entwicklungskit hat folgende Eigenschaften:

- Frequenz 125kHz (LF)
- Unterstützte Transponder: U2270B, e/TK5530, T/TK5551, T5554, ATA5558, T5557, ATA5567, ATA5570, ATA5577, ATA5575

4.2 RFID Transponder

Bei den nachfolgenden Tests werden die beiden Transponder *ATA5577* und *ATA5558* eingesetzt. Der Transponder *ATA5577* (Transponder 1) liegt in Chipkarten-Form vor (siehe 2a) und ist somit ideal für die geplanten Tests, da diese Bauform sehr weit verbreitet ist (Zugangskontrolle, Chipkarten). Der zweite Transponder *ATA5558* (Transponder 2) ist ein „Tag" und liegt in Münzen-Form vor (siehe 2b). Dieser wird u.a. für die Identifikation und Verfolgung von Objekten verwendet.

4.3 Versuchsaufbau

Bei den Versuchen geht es darum zu messen, wie oft ein Transponder aus der Entfernung r und den Winkeln α und β ausgelesen werden kann. Die Antenne bleibt bei den Versuchen an einer festen Position. Daraus ergibt sich der Versuchsaufbau wie in Abbildung 5 und Abbildung 6 vereinfacht zu sehen ist. Der blaue Strich in Abbildung 6 unterhalb der skizzierten Antenne stellt die Antennenebene dar.

10. Der JTAG-Anschluss („**J**oint **T**est **A**ction **G**roup") wird zum Debuggen und Testen von elektronischen Hardwareschaltungen verwendet. Dadurch wird der Entwicklungsprozess und evtl. später die Wartung von Hardware erleichtert.

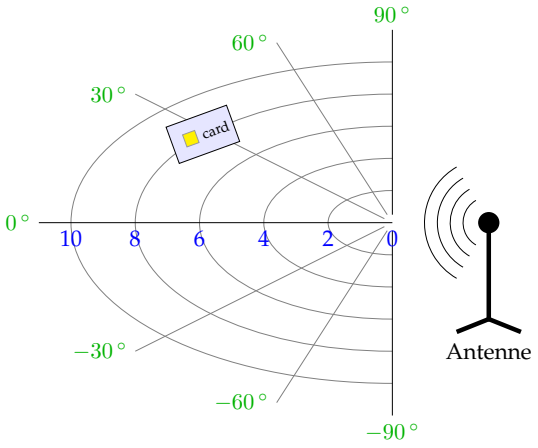


Abbildung 5: Der Transponder wird in unterschiedlichen Entfernungen r und Wickeln α zur Antenne gehalten.

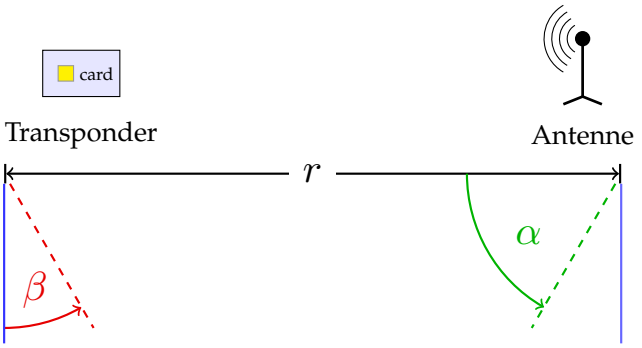


Abbildung 6: Die Lesbarkeit des Transponders wird in zwei unterschiedlichen Winkeln α, β und der Entfernung r zur Antenne gemessen.

4.4 Durchführung

Die folgenden Test werden auf das Auslesen von RFID-Transpondern beschränkt. Dazu werden die Transponder mit Hilfe des Atmel Entwicklungskits initialisiert und mit Testdaten beschrieben. Diese dienen zur Verifikation des richtigen Transponders in der Reichweite der Antenne.

Im nächsten Schritt werden die zwei Transponder in unterschiedlichen Konfigurationen getestet:

- In Standardeinstellungen (Aufbau wie im Entwicklungskit vorgegeben), wobei der Transponder in zwei unterschiedlichen Winkeln β von $0°$ und $90°$ zur Antenne gebracht wird. Dadurch sollen zwei Transponder-Vergleichswerte erreicht ermittelt werden: *1*) Optimale Position horizontal zur Antenne ($\beta = 0°$) und *2*) ungünstiger Fall senkrecht zur Antenne ($\beta = 90°$).
- Verbesserte Antenne
- Abschirmung des Transponders

Die Transponder werden dazu jeweils in einer unterschiedlichen Entfernung r und dem Winkel α jeweils 20-mal in das Antennenfeld gebracht (siehe Abbildung 5, Abbildung 6). Der Winkel β variiert dabei nur im Testfall „Standardeinstellungen“. Gemessen wird, wie oft der Transponder in der jeweiligen Konfiguration ausgelesen werden kann.

Das Entwicklungskit wird auf den „auto read Modus“ gestellt, so dass Transponder kontinuierlich im Feld des Lesegerät erkannt und ausgelesen werden.

4.5 Antennenverbesserung

Bei der im Entwicklungskit beigefügten Antenne handelt es sich um eine Standard-Rundantenne oder auch „Leiterschleife“ genannt. In diesem Test wird versucht, die Lesereichweite mit einem handelsüblichen Küchensieb zu erhöhen.

In einigen Internet-Foren wird beschrieben, wie die Reichweite von WLAN- oder UMTS-Sticks mit Hilfe eines einfachen metallischen Kückensiebs gesteigert werden kann. Dabei soll das Sieb die Funkstrahlen reflektieren und wie eine Art Parabolspiegel wirken.

4.6 Abschirmung

In diesem Test geht es darum, mit welchen Mitteln das (ungewollte) Auslesen von RFID-Transpondern verhindert werden kann. Da in Zukunft immer mehr Personen RFID-Transponder z.B. in Form von Chipkarten (ePerso, Zugangskarte, Studentenausweis, ...) mit sich führen werden, ist es essentiell, sich vor ungewollten Zugriffen Dritter zu schützen. Dazu werden herkömmliche Materialien als auch kommerzielle Produkte auf ihre abschirmende Wirkung untersucht und verglichen.

Bei den zu testenden Materialien gibt es drei unterschiedliche Testszenarien:

- Das Material umschließt den Transponder (Hülle)
- Das Material wird *vor* den Transponder (zwischen Antenne und Transponder) gehalten
- Das Material wird *hinter* den Transponder gehalten (an die der Antenne abgewandten Seite des Transponders)

Dadurch wird getestet, ob z.B. mit einer Hülle die größtmögliche Abschirmung erreicht wird oder ob schon die Anwesenheit eines abschirmenden Materials in der Nähe des Transponders ausreichend ist.

4.6.1 Aluminiumfolie

Eine der einfachsten Abschirmungen vor elektromagnetischen Strahlen, die in jedem Haushalt existiert, ist Aluminiumfolie. In einem Experiment wird diese Folie auf ihre abschirmende Wirkung hin untersuchen.

4.6.2 Aluminiumfolie in Geldbeutel

In einem weiteren Test soll untersucht werden, ob Aluminiumfolie in der großen Außentasche eines handelsüblichen Geldbeutels aus Kunstfasern ebenfalls eine gute abschirmende Wirkung zeigt. Um die Ergebnisse nicht zu verfälschen, enthält der Geldbeutel nur den Transponder. Zum Vergleich wird Transponder 1 einmal ohne und mit Aluminiumfolie in den Geldbeutel gesteckt.

4.6.3 Kupferfolie

Als weiteres Material wird die abschirmende Wirkung von Kupfer getestet. Kupfer ist weit verbreitet in der Elektroindustrie und wird dort als elektrischer Leiter eingesetzt.

4.6.4 Cryptalloy

„Cryptalloy“ soll laut des Herstellers *Kryptronic Technologies* besonders gut vor unbefugtem Auslesen eines Transponders schützen [11]. Das Material soll bereits in unmittelbarer Nähe zum Transponder abschirmend wirken. In einem weiteren Test wird dieses Material ebenfalls untersucht.

5 ERGEBNISSE

Die Tests wurden alle mit dem Atmel Entwicklungskit „LF RFID Application Kit ATA2270-EK1“ durchgeführt. Da es sich hierbei um ein Niederfrequenz RFID System (NF) handelt, können die Ergebnisse bei anderen Systemen (HF, UHF und MW/SUHF, siehe Tabelle 1) variieren oder gar komplett abweichen.

Bei einigen Tests wird das abschirmende Material vor und hinter dem Transponder positioniert. Aus diesem Grund beginnen in diesen Tests die Ergebnisse erst ab dem Abstandswert $r = 4cm$, da die eingesetzte Rundantenne einen Radius von fast $4cm$ besitzt. Sofern es aus Platzgründen möglich ist, werden die Tests bereits ab einem Abstand von $r = 2cm$ durchgeführt. Deshalb gibt es bei den Material-Abschirmungs-Tests nur bei einem Winkel von $\alpha = 0°$ und $r = 2cm$ Ergebnisse. In den Randbereichen hätte die große Antennenfläche von Transponder 1 oder der Kontakt des abschirmenden Materials mit der Antenne das Ergebnis womöglich verfälscht.

5.1 Standardeinstellungen

5.1.1 Variante 1, $\beta = 0°$

Die Ergebnisse in Abbildung 7a und 7b zeigen deutlich, dass die Lesereichweite, wie im Atmel Entwicklungskit beschrieben, für das frontale Auslesen bei 10 cm liegt. Aufgrund der größeren Antenne von Transponder 1 kann dieser sogar bis zu einer Entfernung von $r = 14cm$ unter optimalen Bedingungen ausgelesen werden.

Auffällig ist, dass Transponder 2 frontal nur auf eine sehr nahe Entfernung von $r = 4cm$ und auf $r = 10$ gut ausgelesen werden kann. Die allgemein schlechtere Ausleserate scheint bei Transponder 2 in der durch die Bauform bedingten kleineren Antenne zu liegen.

Zum Rand, d.h. beim Überschreiten der Lesereichweite, fallen bei beiden Transponder-Typen die Ausleseraten stark ab.

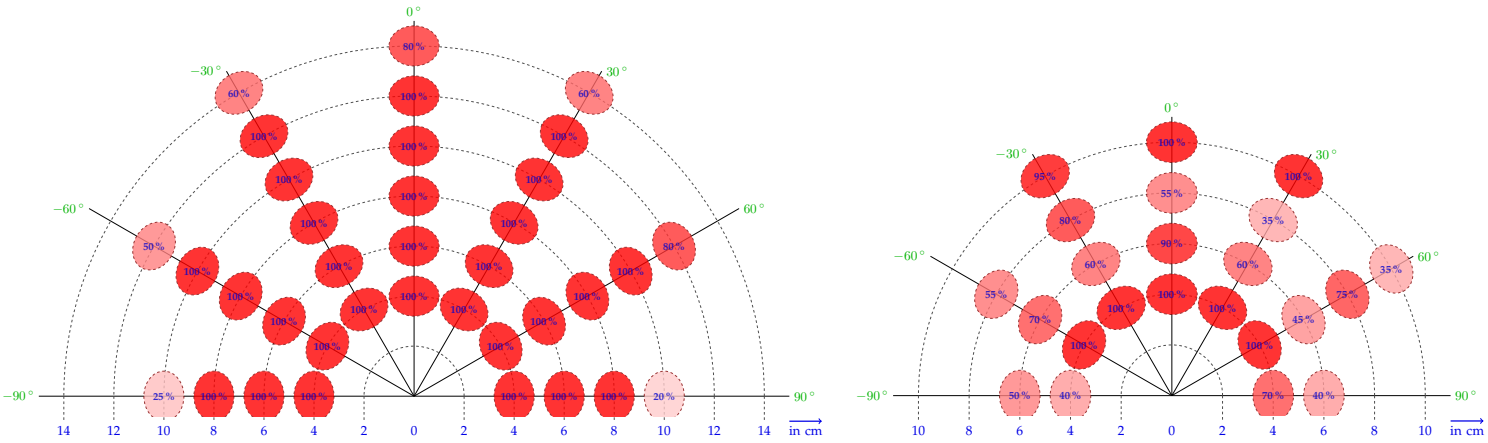
5.1.2 Variante 2, $\beta = 90°$

In der zweiten Variante wird der Transponder senkrecht zur Antenne gebracht. In diesem sehr ungünstigen Fall trifft das Feld des Lesegeräts nicht mehr frontal auf den Transponder.

Transponder 1 lässt sich im Winkel von $\alpha = [-30°, 30°]$ sehr schlecht und nur sehr nahe an der Antenne ($r >= 4cm$) auslesen (siehe Abbildung 8a). Transponder 2 ließ sich aufgrund der geringen Antennengröße überhaupt nicht im Bereich $\alpha = [-30°, 30°]$ auslesen (siehe Abbildung 8b). Erst im Randbereich bei einer Entfernung von $r = [6, 10]$ war das Auslesen erfolgreich.

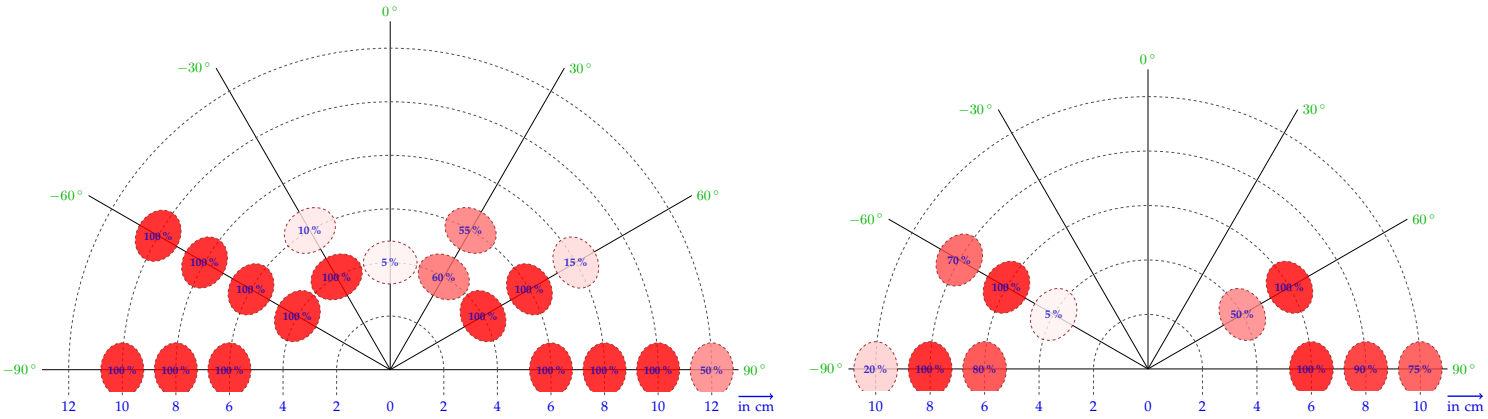
Erstaunlicherweise sind die Ergebnisse für beide Transponder im Randbereich bei $\beta = 90°$ genauso gut oder sogar besser als bei $\beta = 0°$.

Ein Grund hierfür ist die Bauart der Antenne: In den Test wird eine sogenannte „Leiterschleife“ eingesetzt. Bei dieser Antenne verlaufen die Feldlinien bei $\alpha = \pm 90°$ horizontal zur Antenne. Ist der Transponder in einem Winkel von $\beta = 90°$, treffen die Feldlinien dadurch optimal auf die Antenne des Transponders. Dadurch ist das Auslesen in den Randbereichen möglich.



(a) Transponder 1 (b) Transponder 2

Abbildung 7: Messergebnisse in Standardeinstellungen, $\beta = 0°$



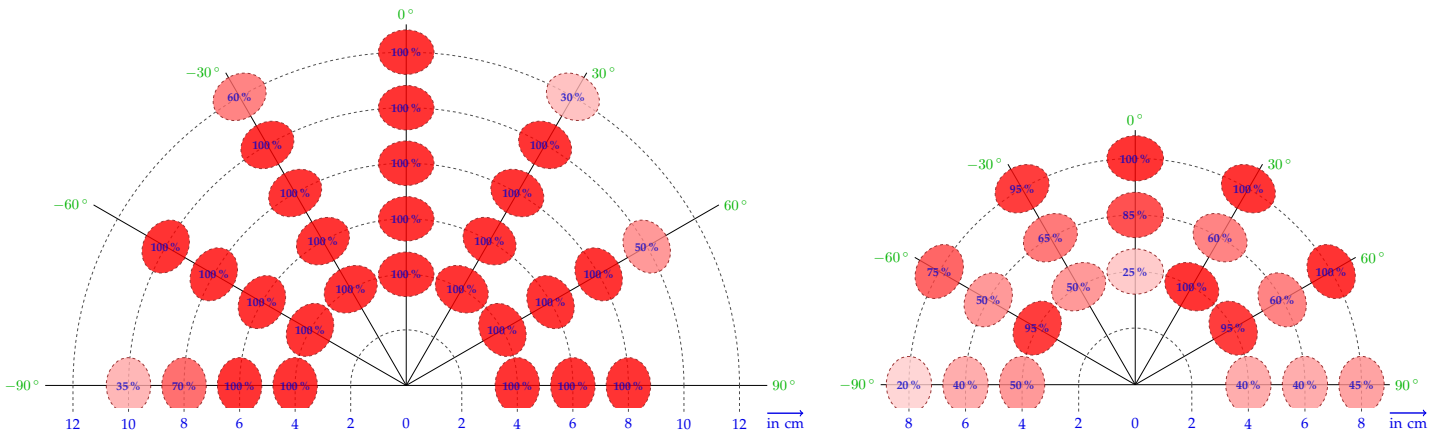
(a) Transponder 1 (b) Transponder 2

Abbildung 8: Messergebnisse in Standardeinstellungen, $\beta = 90°$

5.2 Antennenverbesserung durch Sieb

Metallische Materialien sind optimal, um RFID-Felder zu stören oder gar komplett zu dämpfen.

Die Ergebnisse des Tests „Antennenverbesserung mit Sieb“ stützen diese Annahme. Die Ergebnisse in Abbildung 9a sind schlechter als der Test mit Standardeinstellungen. Der Vergleich mit Abbildung 7a zeigt eine Verschlechterung der Leserate um den Faktor $\sim 1{,}2$. Für den zweiten Transponder fallen die Ergebnisse in Abbildung 9b ähnlich negativ aus. Dieser Test ist im Vergleich zu den Ergebnissen in Abbildung 7b um den Faktor $\sim 1{,}1$ schlechter. Außerdem zeigt sich sogar eine „Fokussierung“ des Magnetfeldes bei $r \approx 8$ cm für Transponder 2.



(a) Transponder 1 (b) Transponder 2

Abbildung 9: Antennenverbesserung mit Sieb

5.3 Abschirmung

Wie bereits in 5.2 erwähnt wurde, sind metallische Materialien besonders gut geeignet, um magnetische Felder zu dämpfen. Es ist deshalb zu erwarten, dass metallische Folien oder Materialien das magnetische Feld beeinträchtigen werden.

In den Ergebnissen ist der Testfall „Transponder 2 in Hülle aus *Material-X*“nicht als Abbildung vorhanden, da für alle Materialien das Signal zum Transponder komplett gedämpft und somit das Auslesen verhindert wurde.

5.3.1 Aluminiumfolie

Die Ergebnisse in Abbildung 10 zeigen, dass bereits eine Hülle aus herkömmlicher Haushalts-Aluminiumfolie die Auslesereichweite stark vermindern kann. Wird Transponder 2 mit Aluminiumfolie abgeschirmt, kann dieser aufgrund der Münzen-Bauform und der geringeren Antennengröße überhaupt nicht mehr ausgelesen werden.

Die weiteren Ergebnisse in Abbildung 11 und Abbildung 12 zeigen, dass die reine Anwesenheit einer metallischen Folie bereits die Lesereichweite vermindert. Wird die Aluminiumfolie zwischen Antenne und Transponder 1 in einem Abstand von 1 cm zum Transponder gebracht, vermindert sich die Auslesereichweite um den Faktor $\sim 2{,}2$. Ist die Folie hinter Transponder 1 angebracht, reduziert sich die Auslesereichweite immerhin noch um den Faktor $\sim 1{,}8$. Die Ergebnisse sind für die Anwesenheit einer metallischen Folie noch relativ gut. Dies liegt höchstwahrscheinlich an der größeren Antenne von Transponder 1.

Transponder 2 hat hingegen eine kleinere Antenne, wodurch die Auslesereichweite um den Faktor $\sim 2{,}3$ (vor dem Transponder) und um den Faktor $\sim 3{,}6$ (hinter dem Transponder) verringert wird.

Interessant an den Ergebnissen ist, dass bei Transponder 1 das Signal stärker verringert wird, wenn die Aluminiumfolie zwischen Antenne und Transponder gebracht wird. Für Transponder 2 sind die Ergebnisse genau umgekehrt.

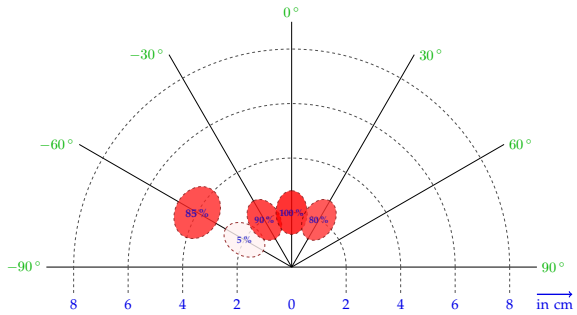
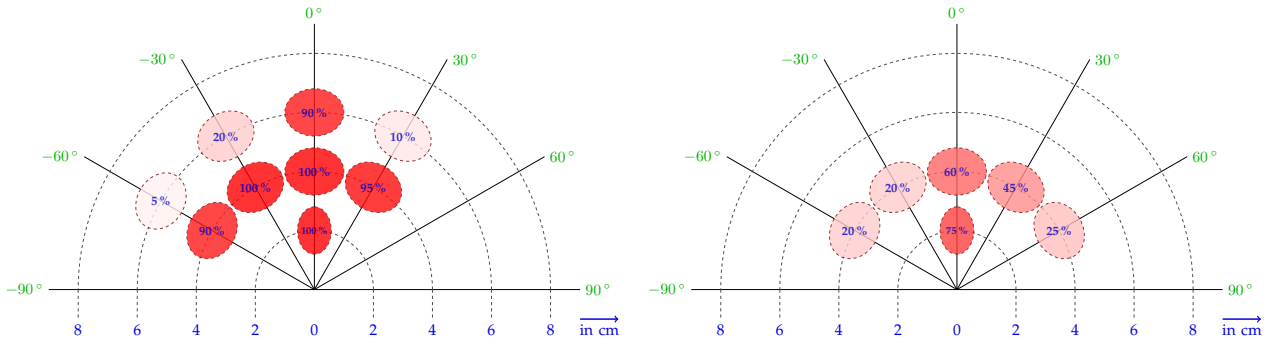
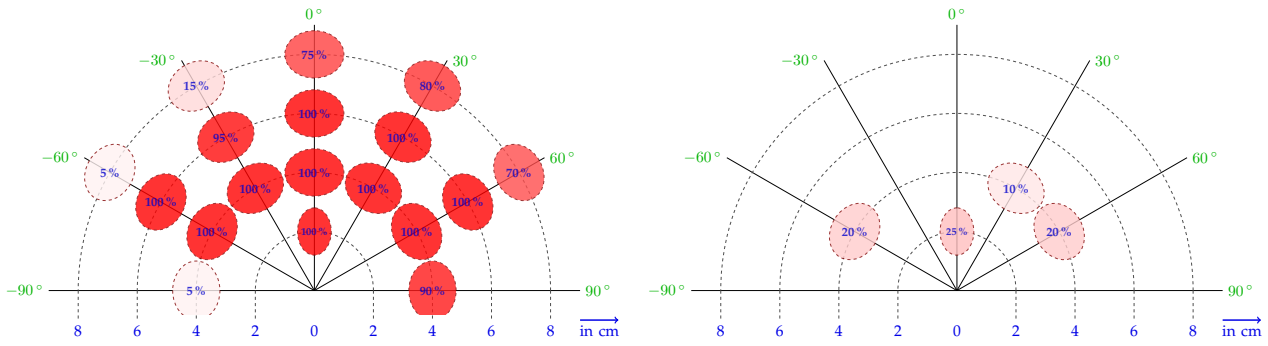


Abbildung 10: Aluminiumhülle, Transponder 1



(a) Transponder 1 (b) Transponder 2

Abbildung 11: Aluminiumfolie vor Transponder



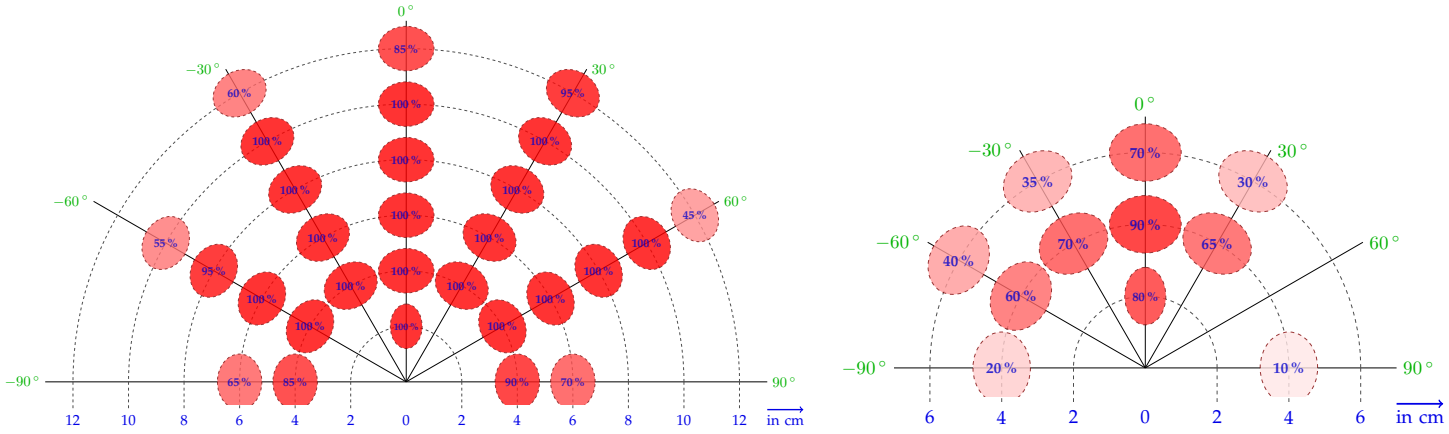
(a) Transponder 1 (b) Transponder 2

Abbildung 12: Aluminiumfolie hinter Transponder

5.3.2 Aluminiumfolie in Geldbeutel

In Abbildung 13a ist der Referenzwert zu sehen, bei dem der Transponder ohne Aluminiumfolie im Geldbeutel steckt. Abbildung 13b enthält das Ergebnis für den Geldbeutel mit Aluminiumfolie-Auskleidung.

Die Ergebnisse zeugen deutlich, dass ein Stück Aluminiumfolie in der Außentasche eines Geldbeutels die Auslesereichweite drastisch reduzieren kann. Das einzige Ergebnis das in Abbildung 13b nicht erklärt werden kann, ist die Lücke bei $\alpha = 60°$.



(a) Geldbeutel ohne Auskleidung (b) Geldbeutel mit Aluminiumfolie ausgekleidet

Abbildung 13: Testergebnisse: Aluminiumfolie in Geldbeutel

5.3.3 Kupferfolie

Eine Hülle aus Kupferfolie (siehe Abbildung 14) oder eine Kupferfolie vor dem Transponder scheint besonders effektiv das magnetische Feld beider Transponder Typen zu stören (siehe Abbildung 15). Das Material vor dem Transponder dämpft das Feld so gut, dass die Auslesereichweite für Transponder 1 um den Faktor $\sim 3{,}4$ und für Transponder 2 um den Faktor $\sim 4{,}5$ verringert wird.

Wird die Kupferfolie hinter den Transponder gehalten (siehe Abbildung 16), sind die Ergebnisse für Transponder 1 ähnlich wie bei den anderen Folien. Transponder 2 hingegen wird mit Aluminiumfolie besser gedämpft als mit Kupferfolie.

Bei diesen Tests befindet sich das Material im Nahfeld, wodurch der Induktionseffekt auftritt. Dabei wird Spannung in das Material induziert, die sofort über die Kupferfolie kurzgeschlossen wird. Dadurch bildet sich ein Gegenfeld zum Feld des Lesegeräts.

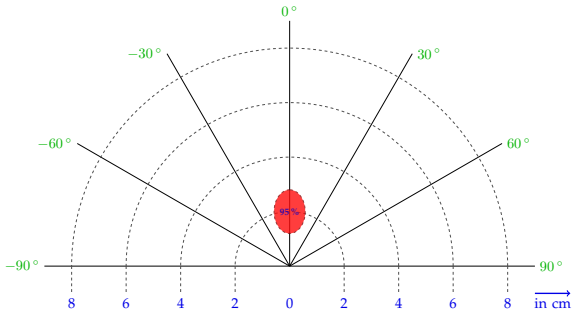
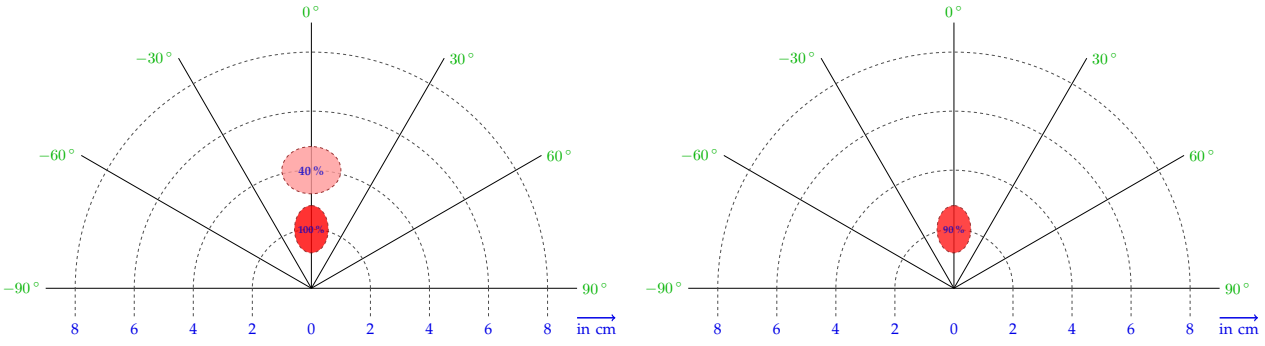
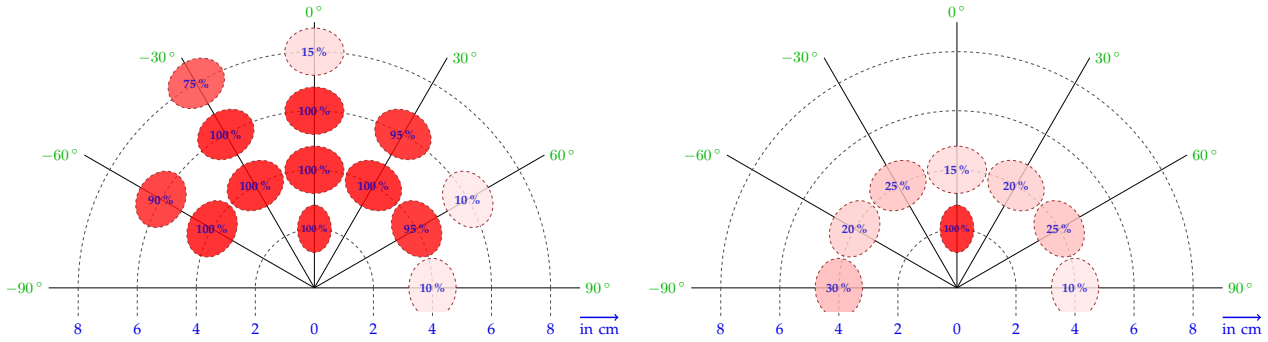


Abbildung 14: Kupferhülle, Transponder 1



(a) Transponder 1 (b) Transponder 2

Abbildung 15: Kupferfolie vor Transponder



(a) Transponder 1 (b) Transponder 2

Abbildung 16: Kupferfolie hinter Transponder

5.3.4 *Cryptalloy*

Eine Schutzhülle aus Cryptalloy dämpft, unter allen getesteten Folien, das Feld am besten (siehe Abbildung 17). Dieses Ergebnis ist nicht überraschend, da diese Folie genau für diesen Einsatzzweck entwickelt wurde. Überraschend ist eher, dass Aluminiumfolie ähnliche Ergebnisse wie Cryptalloy aufweist und dass Kupferfolie sogar zum Teil besser das Feld dämpft. Der Beschreibung zu Cryptalloy ist zu entnehmen [11], dass ein Hauptbestandteil von Cryptalloy Aluminium ist. Dadurch lassen sich die ähnlichen Ergebnisse zu den Tests mit Aluminiumfolie erklären.

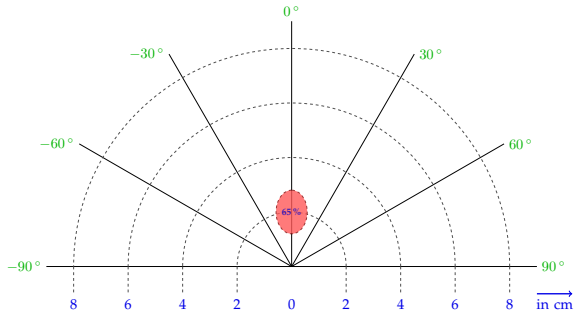
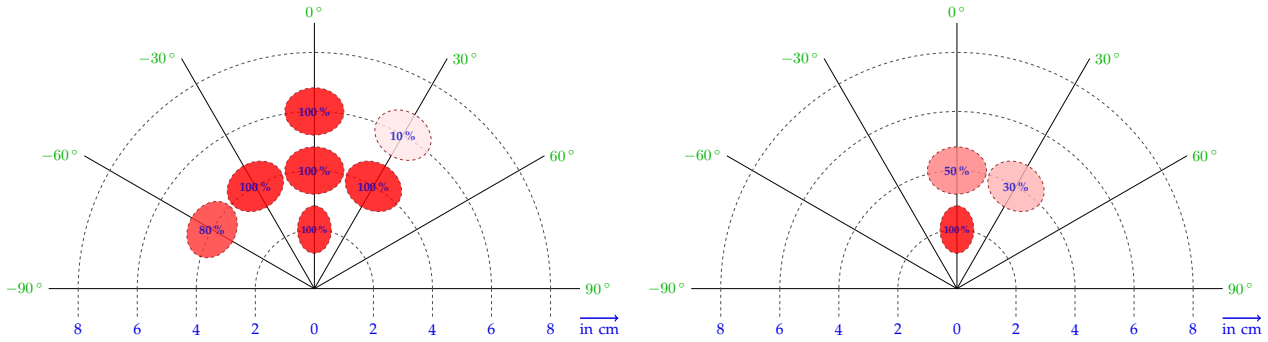
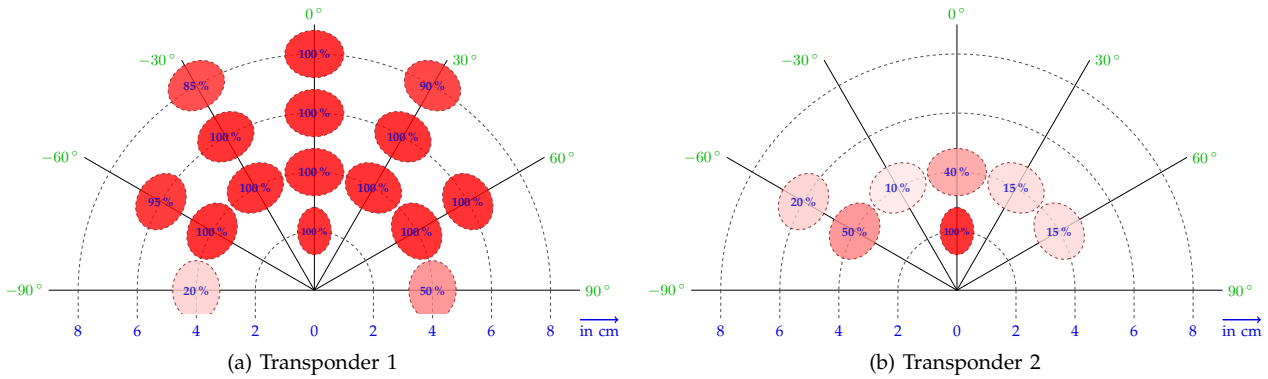


Abbildung 17: Cryptalloy-Hülle, Transponder 1



(a) Transponder 1 (b) Transponder 2

Abbildung 18: Cryptalloy-Folie vor Transponder



(a) Transponder 1 (b) Transponder 2

Abbildung 19: Cryptalloy-Folie hinter Transponder

6 FAZIT

6.1 Abschirmung

Die Abschirmungstests zeigen, dass mit metallischen Folien Signale vom RFID-Transpondern gedämpft werden können. Bereits die Aluminiumfolie hat erstaunlich gute Ergebnisse geliefert. Soll ein Signal noch besser gedämpft werden, empfiehlt sich der Einsatz von Kupferfolie. Etwas besser als Aluminiumfolie hat die speziell für RFID-Zwecke entwickelte Cryptalloy-Folie abgeschnitten. Cryptalloy-Folien und Hüllen sind jedoch teuer. Die kostengünstigere Alternative ist in diesem Fall die einfache Aluminiumfolie, die in fast jedem Haushalt zu finden ist.

Die Ergebnisse in 5.3.2 zeigen im Vergleich von 13a und 13b deutlich, dass Aluminiumfolie in der großen Tasche eines Geldbeutels die Auslesereichweite eines Transponders halbieren kann.

Für einen sicherheitsbewussten Benutzer, der sich vor ungewolltem Auslesen Dritter schützen will, ist es empfehlenswert, RFID-Transponder mit Hilfe von metallischen Folien zu verschleiern. Die Testergebnisse zeigen, dass bereits eine einfache Aluminiumfolie guten Ausleseschutz bietet. Soll der Schutz effektiver werden, empfiehlt es sich, Kupferfolie oder ein kommerzielles Produkt wie z.B. Cryptalloy zu verwenden.

6.2 Antennenverbesserung

Der Versuch die Auslesereichweite des RFID-Systems mit Hilfe eines handelsüblichen Küchensiebs zu steigern, hat nicht das gewünschte Ergebnis erbracht. Das Küchensieb hatte eher eine dämpfende Wirkung und hat die Auslesereichweite reduziert.

Magnetische Felder werden im Nahfeld ($Abstand < \lambda$) gedämpft und erst im Fernfeld ($Abstand > \lambda$) von einer metallischen Oberfläche reflektiert. Im Fernfeld wird beim Auftreffen der elektromagnetischen Welle auf eine metallische Oberfläche die elektrische Komponente kurzgeschlossen und dadurch die magnetische von der Oberfläche reflektiert. Im Nahfeld wird das Aussenden eines Feldes bei Anwesenheit eines metallischen Objekts bereits erschwert, da im Objekt ein elektrischer Kurzschluss entsteht.

Das eingesetzte metallische Sieb hat einen Radius von 8 cm. In einem Niederfrequenz (LF) RFID-System beträgt bei einer Sendefrequenz von 125 kHz die Wellenlänge $\lambda \approx$ 2,4 km. Das metallische Sieb befindet sich somit im Nahfeld der Antenne ($Abstand < \lambda$), wodurch aufgrund des Induktionseffekts Spannung in das Objekt induziert wird. Da das metallische Sieb jedoch ein geschlossener Leiter ist und dadurch einen „Kurzschluss“ verursacht, baut sich im Sieb ein gegenphasiges Magnetfeld auf. Dieses gegenphasige Feld stört das Feld des Lesegeräts und ist der Grund für die reduzierte Auslesereichweite.

Das Verfahren funktioniert bei Mikrowellen-Systemen (UMTS, WLAN, ...) nur, da z.B. bei einer Frequenz von 2,4 GHz die Wellenlänge $\lambda = 12{,}5$ cm ist.

Das Küchensieb ist für die Reichweitensteigerung bei Niederfrequenz (LF) RFID-Systemen ungeeignet und bewirkt vermutlich nur bei Mikrowellen- oder SUHF-Systemen eine Steigerung.

6.3 Verbesserungsvorschläge für Transponder

In den nächsten Jahren werden vermehrt RFID-Transponder in Chipkartenform in Umlauf kommen. Das bekannteste Beispiel hierfür ist der neue ePerso in Deutschland. Ist der kryptografische Schutz eines Transponders unzureichend oder ist gar keiner vorhanden, können theoretisch die Daten des Transponders „beim Vorbeigehen“ ausgelesen werden. Deutsche Forscher haben erst vor kurzem unzureichend geschützte RFID-Transponder gehackt [8]. In großen Menschenansammlungen, z.B. in öffentlich Verkehrsmitteln, können dadurch eine große Menge an Daten per RFID erfasst werden.

Die Transponder eines RFID-Systems haben einen großen Nachteil: Der Ein- und Ausschalter fehlt. Deshalb ist an dieser Stelle der Aufbau eines Transponders mit Ein- und Ausschalter beschrieben, der das ungewollte Auslesen eines Transponders vermeiden soll.

Ein vom `ISO 7816` Standard abgeleiteter Gehäusevorschlag ist in Abbildung 20 zu sehen. Der Schalter ist so dick wie die Chipkarte selbst und sollte deshalb nicht weiter stören. Bei Bedarf kann die Karte mit diesem Schalter einfach ein- und ausgeschaltet werden. Dadurch können sicherheitsbewusste Personen z.B. den ePerso im alltäglichen Leben deaktiviert lassen und diesen immer bei Gebrauch durch Umlegen des Schalters aktivieren.

Anstelle eines Schalters kann jedoch auch ein Taster eingesetzt werden. Dadurch wird der Transponder nur dann aktiviert, wenn der Taster durch eine Person aktiviert wird. Ein Schalter wiederum hat den Vorteil, dass der Transponder dauerhaft in einem Zustand (an oder aus) bleiben kann. Handelt es sich z.B. um einen Transponder für ein Zugangssystem, kann dieser beim Betreten des Gebäudes durch umlegen des Schalters aktiviert werden und müsste nicht, wie beim Taster, jedes mal aktiviert werden.

Abbildung 21 enthält zwei Schaltungserweiterungen für einen passiven Transponder. Schalter S_1 sorgt dafür, dass die Antenne (de-) aktiviert wird. S_2 hingegen schließt die komplette Schaltung kurz, wodurch der Transponder nicht funktionieren wird.

Theoretisch sollten diese Erweiterungen funktionieren. In der Praxis können jedoch unsaubere Verarbeitung im und am Schalter, sowie etwaige Kapazitäten im Schalter beeinträchtigend auf die Funktionsweise des Transponders wirken.

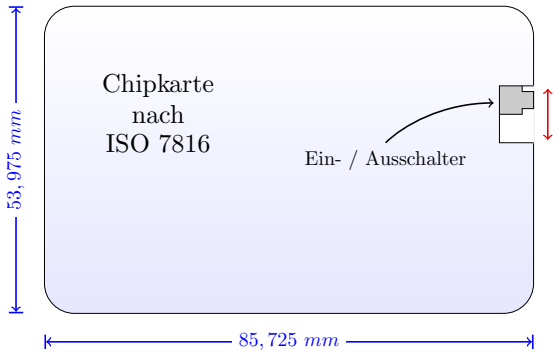


Abbildung 20: Gehäuse für eine verbesserte Chipkarte mit einem Ein- / Ausschalter

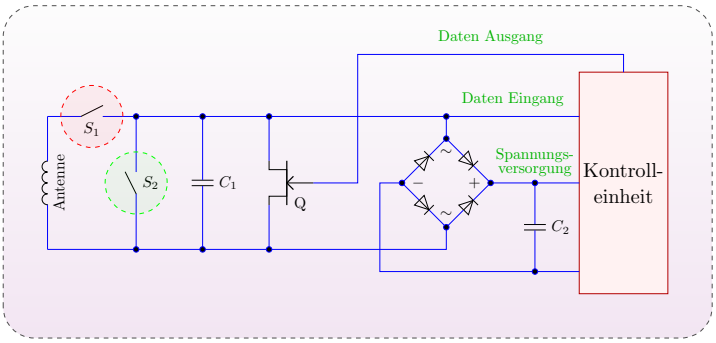


Abbildung 21: Schaltungserweiterung um den Ein- / Ausschalter S_1 oder S_2

LITERATUR

[1] Harry Sockmann, "Communication by Means of Reflected Power," Proceedings of the Institute of Radio Engineers, Tech. Rep., Oktober 1948.

[2] RFID-Ready, "RFID-Frequenzen," 2011, [Zugriff am 30-August-2011] , online verfügbar: http://www.rfid-ready.de/rfid-frequenzen.html

[3] Wikibooks, "RFID-Technologie," 2011, [Zugriff am 30-August-2011] , online verfügbar: http://de.wikibooks.org/wiki/RFID-Technologie

[4] K. Finkenzeller, *RFID Handbuch*. Carl Hanser Verlag München, 2008.

[5] Spiegel, "Das geht unter die Haut," Januar 2006, [Zugriff am 30-August-2011], online verfügbar: http://www.spiegel.de/netzwelt/tech/0,1518,394217,00.html

[6] "The RFID Tag and Reader," Januar 2011, [Zugriff am 20-Dezember-2011], online verfügbar: http://rfid-managerialviewpoint.blogspot.com/2011/01/rfid-tag-and-reader.html

[7] Bundesministerium des Innern, "Schutzmechanismen gegen unberechtigtes auslesen der daten im epass-chip," [Zugriff am 31-August-2011], online verfügbar: http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/ohneMarginalspalte/Sicherheit_ePassChip.html?nn=106768

[8] H. Security, "Deutsche Forscher knacken RFID-Karten," Oktober 2011, [Zugriff am 16-Oktober-2011], online verfügbar: http://heise.de/-1358760

[9] H. K. Thomas Finke, "Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems," Bundesamt für Sicherheit in der Informationstechnik – BSI, Tech. Rep., 2004.

[10] "RFID-Zapper," [Zugriff am 20-Dezember-2011], online verfügbar: http://runningserver.com/?page=runningserver.content.thelab.rfidzapper

[11] K. Technologies, "Abschirmmaterial und Produkte für elektronische RFID-Ausweise," 2011, [Zugriff am 13-September-2011], online verfügbar: http://www.cryptalloy.de