

HANSER

RFID-Handbuch

Klaus Finkenzeller

Grundlagen und praktische Anwendungen induktiver
Funkanlagen, Transponder und kontaktloser Chipkarten

ISBN 3-446-40398-1

Leseprobe

Weitere Informationen oder Bestellungen unter
<http://www.hanser.de/3-446-40398-1> sowie im Buchhandel

8 Sicherheit von RFID-Systemen

Wie jedes andere System der Nachrichten- und Informationstechnik, so sind auch RFID-Systeme potentiell gefährdet, von einem Angreifer ausgespäht oder manipuliert zu werden. Um die möglichen Risiken des Einsatzes von RFID-Systemen etwas besser einschätzen zu können, werden wir daher in Kapitel 8.1 einige der gängigen Angriffsarten auf RFID-Systeme etwas genauer betrachten. Im Anschluß daran werden in Kapitel 8.2 kryptographische Verfahren zum Schutz gegen gängige Angriffe vorgestellt.

Ein RFID-System ist darauf angewiesen, dass die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle mit anderen Datenbeständen verknüpft werden. Die Sicherheitsaspekte in diesem so genannten Backend des RFID-Systems sind jedoch nicht spezifisch für RFID [rikcha-04]. Um den Rahmen dieses Buchs nicht zu sprengen, beschränken wir uns daher im Wesentlichen auf Angriffe auf die Luftschnittstelle zwischen dem Lesegerät und den Transpondern, sowie Angriffe auf den Transponder selbst. Angriffe auf das Hintergrundsystem, also zum Beispiel auf eine Datenbank, werden an dieser Stelle nicht weiter untersucht.

Betrachten wir den *Verwendungskontext* in einem offenen RFID-System, so fällt auf, dass es in der Regel zwei beteiligte Parteien mit unterschiedlichen Interessen gibt. Der *Systembetreiber* bildet die aktive Partei und stellt die Infrastruktur, also die Lesegeräte und das Hintergrundsystem, zur Verfügung. Die aktive Partei gibt auch die Transponder aus, und verwaltet und verwertet die mit den Transpondern assoziierten oder abgespeicherten Daten. Damit hat sie alle vom RFID-System erfassten Daten sowie deren Verwendung unter Kontrolle [rikcha-04]

Auf der anderen Seite stehen die Nutzer des RFID-Systems, in der Regel ein Kunde oder Angestellter des Systembetreibers. Die Nutzer bilden die passive Partei. Zwar ist die passive Partei im Besitz der Transponder (z. B. einem kontaktlosen Ticket oder Fahrschein, einem Ausweisdokument oder dem Warenetikett auf einem eben gekauften Produkt), sie hat aber nicht immer Einfluß auf deren Verwendung, bzw. auf die Verwendung der erfassten Daten [rikcha-04].

In einem *geschlossenen System*, z. B. bei der Fertigungssteuerung mittels RFID in einem Betrieb, existiert die Trennung zwischen aktiver und passiver Partei nicht. Hier ist der Systembetreiber auch gleichzeitig der Nutzer des Systems.

Daneben kann es auch noch eine dritte Partei geben, zum Beispiel einen Hacker oder Konkurrenten, der versucht, unberechtigterweise an die im Transponder oder System gespeicherten Daten zu gelangen, oder diese sogar zu seinem Vorteil zu verändern.

Die breite Einführung von RFID-Systemen bei Warenetiketten, Reisepässen und anderen Ausweisdokumenten, kontaktlosen Tickets und Eintrittskarten konfrontiert die breite Öffentlichkeit mit einer neuen und ungewohnten Technologie, deren Funktionsweise, und damit auch deren Grenzen oder Risiken nicht im Detail verstanden werden. Die Vielzahl an verschiedenen RFID-Systemen unterschiedlichster Performance trägt dabei nicht unwesentlich zu einer Verwirrung bei. Wie jeder neuen Technologie wird daher auch der RFID nicht nur mit Neugier, sondern auch mit Ängsten und sogar Ablehnung begegnet. Eine vergleich-

bare Reaktion war auch Ende der 70er Jahre bei der Einführung von Barcodes zur Produktkennzeichnung, dem *EAN-Code* oder dem amerikanischen *UPC*, zu beobachten.

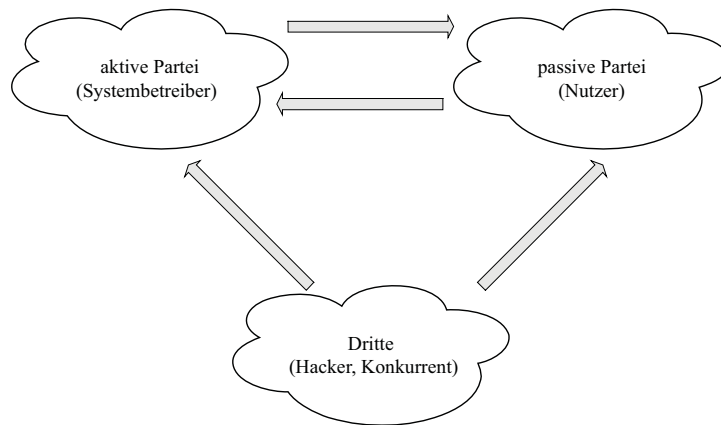


Abb. 8.1 Verwendungskontext in einem typischen RFID-System mit Parteien mit unterschiedlichen Interessen.

Ein wichtiger Diskussionspunkt war damals, und ist auch heute wieder der Schutz der *Privatsphäre* des Einzelnen. Im Vordergrund steht dabei die Angst, die neue Technologie RFID könnte zum unbemerkten und unerwünschten Sammeln von Daten des Einzelnen, also zum Ausspionieren der Privatsphäre durch die aktive Partei, eingesetzt werden. In den letzten Jahren haben sich vermehrt *Bürgerverbände* und *Verbraucherschutzorganisationen* darum bemüht, die Öffentlichkeit über die möglichen Risiken eines breiten Einsatzes von RFID-Systemen zu informieren.

In einigen Ländern, insbesondere in den USA, wurde bereits mehrfach die Einführung von Gesetzen zur Regulierung des Einsatzes von RFID gefordert, so etwa im Januar 2004 im US-Bundesstaat Missouri der „RFID Right to Know Act of 2004 (SB 0867)“, der jedoch bisher nicht verabschiedet wurde [lahiri]. Der Entwurf für diese Verordnung fordert unter anderem die eindeutige und sichtbare *Kennzeichnung von Produkten*, die einen RFID-Chip beinhalten.

8.1 Angriffe auf RFID-Systeme

Ein Blick auf die Abbildung 8.2 zeigt uns verschiedene grundlegende Angriffsarten auf die verschiedenen Komponenten eines RFID-Systems. Grundsätzlich kann ein Angriff dabei auf den Transponder, das Lesegerät oder auch das HF-Interface zwischen Transponder und Lesegerät erfolgen.

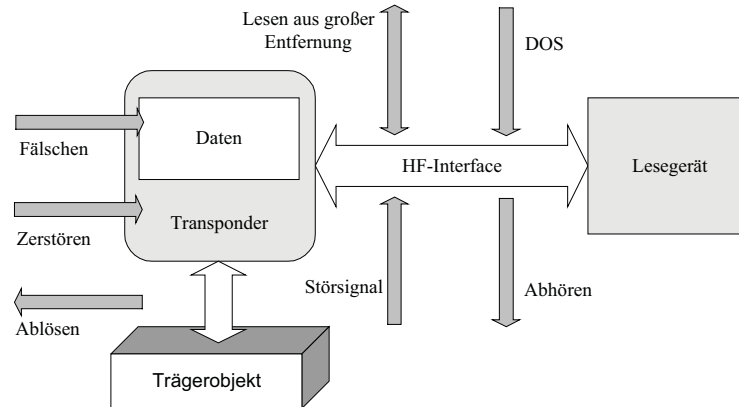


Abb. 8.2 Einige der grundlegenden Angriffsmöglichkeiten auf ein RFID-System (nach [rikcha-04]).

Die Angriffe können dabei völlig unterschiedlich motiviert sein. Je nach dem Zweck, der hierbei verfolgt wird, lassen sich für die nachfolgend beschriebenen Angriffe vier Angriffsarten klassifizieren [rikcha-04]:

- *Ausspähen*: Hier versucht der Angreifer, sich unberechtigten Zugang zu Informationen und Daten der aktiven oder passiven Datei zu verschaffen.
- *Täuschen*: Hierbei versucht der Angreifer, unzutreffende Informationen in das RFID-System einzuspeisen, um die aktive Partei, also den Betreiber eines RFID-Systems, oder die passive Partei, also den Benutzer eines RFID-Systems, zu täuschen.
- *Denial of Service*: Bei diesem Angriff wird die Verfügbarkeit von Funktionen eines RFID-Systems beeinträchtigt.
- *Schutz der Privatsphäre*: Der Angreifer sieht seine eigene Privatsphäre durch das RFID-System bedroht und versucht, diese durch einen entsprechenden Angriff auf das RFID-System zu schützen.

8.1.1 Angriffe auf den Transponder

Am leichtesten zugänglich ist in der Regel der Transponder, der auf Waren oder als Ticket für einen Angreifer jederzeit und in den meisten Fällen zeitlich unbegrenzt zur Verfügung steht. Gegenüber dem Transponder existiert daher eine Vielfalt an unterschiedlich wirksamen Angriffen.

8.1.1.1 Dauerhaftes Zerstören des Transponders

Die einfachste Möglichkeit eines Angriffes auf ein RFID-System besteht in der mechanischen oder chemischen *Zerstörung eines Transponders*. So kann die Antenne meist mit einfachen Hilfsmitteln durchtrennt oder abgeschnitten werden. Auch der Chip kann durch Knicken oder einen Hammerschlag leicht zerstört werden.

Eine weitere Möglichkeit ist die Zerstörung eines Transponders durch eine entsprechend starke *Feldeinwirkung*. So ist für induktiv gekoppelte Transponder nach ISO/IEC 14443

oder ISO/IEC 15693 eine maximale Feldstärke von 12 A/m bei einer Frequenz von 13,56 Mhz spezifiziert. Wird der Transponder bei dieser Frequenz in ein Feld mit deutlich höherer Feldstärke eingebracht, kann schließlich die am Shuntregler auftretende Verlustwärme nicht mehr ausreichend abgeführt werden, so dass der Transponder thermisch zerstört wird. Steht kein ausreichend starker Sender für diesen Frequenzbereich zur Verfügung, so kann der Transponder auch in einen Mikrowellenherd eingebracht werden.

8.1.1.2 Abschirmen oder Verstimmen des Transponders

Ein sehr effektiver Angriff ist das *Abschirmen* eines Transponders gegenüber der magnetischen oder elektromagnetischen Strahlung des Lesegerätes durch Metallflächen. Im einfachsten Fall reicht es dabei, einen Transponder in eine metallische Folie, zum Beispiel *Alu-Haushaltsfolie*, einzuwickeln. Bei induktiv gekoppelten Transpondern wird der Antennenschwingkreis des Transponders durch eine Metalloberfläche in unmittelbarer Nähe stark verstimmt. Zusätzlich wird das magnetische Feld des Lesegerätes durch Wirbelstromverluste in der Metallfolie gedämpft. Häufig reicht es daher schon, einen Transponder auf einer Seite auf einer Metallfläche zu befestigen. Die elektromagnetischen Felder eines UHF-Backscatter-Systems (zum Beispiel auf 868 MHz) werden durch eine Metallfläche reflektiert, und so wirkungsvoll vom Transponder abgehalten. Ein passiver Transponder wird im günstigsten Fall gar nicht erst mit ausreichend Energie zum Betrieb des Chips versorgt.

Dieser Angriff ist vor allem dazu geeignet, einen Transponder nur zeitweise außer Betrieb zu setzen. Wird die Abschirmung entfernt, so ist der Transponder wieder uneingeschränkt funktionsfähig. Für den technisch weniger versierten Laien werden mittlerweile auch kommerzielle Produkte zur Abschirmung von Transponder angeboten [mcloak].

Antennen von UHF-Backscatter-Transpondern werden durch das Auf- oder Einbringen in ein *Dielektrikum*, zum Beispiel Glas oder Kunststoff, verstimmt. Die *Verstimmung* fällt um so stärker aus, je höher die Dielektrizitätskonstante ϵ_r und Dicke des umgebenden Dielektrikums sind. Durch die auftretende Verstimmung verschlechtert sich die Ansprechempfindlichkeit des Transponders auf der Sendefrequenz des Lesegerätes, so dass die Lesereichweite des derart angegriffenen Transponders verringert wird.

8.1.1.3 Emulieren und Klonen eines Transponders

Wie wir in den Kapiteln 10.1 “Transponder mit Speicherfunktion” und 10.2 “Mikroprozessoren” noch sehen werden, gibt es unterschiedlich komplexe Verfahren zur Informationsspeicherung in einem Transponder. Im einfachsten Fall, dem Read-only-Transponder, verfügt der Transponder lediglich über eine fest programmierte Kennung, die Seriennummer des Transponders. Das Blockschaltbild eines solchen einfachen Transponders ist in Abbildung 10.10 auf Seite 325 dargestellt.

Gelangt ein Read-only-Transponder in ein ausreichend starkes Feld eines Lesegerätes, beginnt er unmittelbar mit der periodischen Aussendung seiner Seriennummer, so dass diese von einem geeigneten Lesegerät problemlos gelesen werden kann. Ein Angreifer könnte nun aus diskreten Bauelementen selbst einen Read-only-Transponder (*Transponderklon*) aufbau-

en, und das PROM, das die Seriennummer des Transponders enthält, durch einen mehrfach programmierbaren Speicher (EEPROM) oder, im einfachsten Falle, durch eine Reihe von DIP-Schaltern ersetzen. Liest der Angreifer anschließend die Seriennummer eines beliebigen Transponders aus, kann er diese Seriennummer dann im Transponderklon einprogrammieren. Wird der Transponderklon in das Feld eines Lesegerätes gehalten, kann er nun die zuvor aus dem echten Transponder ausgelesene Seriennummer aussenden, und somit die Anwesenheit des echten Transponders gegenüber dem Lesegerät vortäuschen [westhues]. Für das Lesegerät besteht keine Möglichkeit festzustellen ob eine aktuell empfangene Seriennummer von einem echten Transponder oder einem Transponderklon gesendet wurde. Problematisch ist es dabei auch, dass der Angreifer keinen physischen Zugriff auf den Transponder benötigt, sondern sich lediglich mit einem geeigneten Lesegerät unbemerkt bis auf Lesereichweite an den zu klonenden Transponder annähern muss.

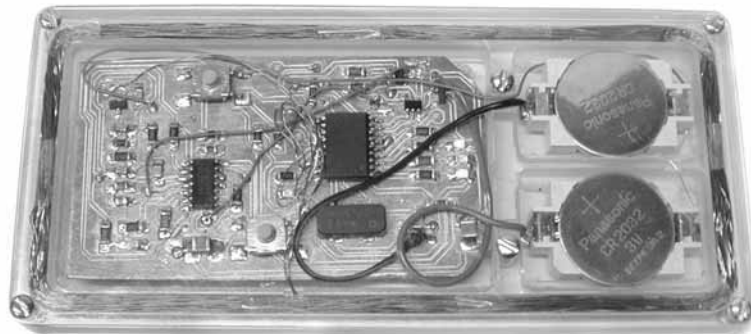


Abb. 8.3 Versuchsaufbau zum Auslesen und Klonen eines 125 kHz Read-only-Transponders.
(Quelle: Jonathan Westhues)

Nach dem Read-only-Transponder wird die nächste Stufe der Funktionalität durch Transponder mit beschreibbaren Speichern gebildet (siehe Kapitel 10.1.3.2 „Beschreibbare Transponder“, S. 326). Häufig können die *Speicherbereiche* völlig frei, d. h. ohne Kenntnis eines geheimen Passwortes oder Schlüssels, gelesen und beschrieben werden. Auch hierbei besteht die Möglichkeit, dass die gespeicherten Daten von einem Angreifer entweder einfach zu dessen Nutzen verändert werden, oder dass Kopien des angegriffenen Transponders hergestellt werden, indem die Daten ausgelesen und auf weitere Transponder kopiert werden. Durch den Einsatz von Authentifizierung und verschlüsselter Datenübertragung (siehe Kapitel 8.2.1 „Gegenseitige symmetrische Authentifizierung“, S. 253) kann das Klonen von Transpondern jedoch wirkungsvoll verhindert werden. RFID-Anwendungen, die für einen Angreifer leicht zugänglich sind, zum Beispiel Zutrittssysteme oder Ticketsysteme, sollten daher auf die Anwendung von Read-only-Transpondern oder den unverschlüsselten Zugriff auf Datenbereiche grundsätzlich verzichten.

8.1.2 Angriffe über das HF-Interface

RFID-Systeme sind Funksysteme und kommunizieren über elektromagnetische Wellen im Nah- und Fernfeld. Für einen Angreifer liegt es daher nahe zu versuchen, ein RFID-System über das HF-Interface anzugreifen. Der besondere Reiz liegt darin, dass bei einem Angriff über das HF-Interface kein physischer Zugriff auf ein Lesegerät oder einen Transponder nötig ist, sondern aus der Entfernung agiert werden kann.

Derzeit sind folgende Angriffe bekannt und untersucht:

- Abhören der Kommunikation zwischen Lesegerät und Transponder.
- Stören der Kommunikation zwischen Lesegerät und Transponder mittels *Störsender*.
- *Vergrößern der Lesereichweite* zum unbemerkten Auslesen entfernter Transponder.
- Blockieren eines Lesegerätes durch DOS-Attacken.
- Unbemerkte Verwendung eines entfernten Transponders mittels einer Relay-Attacke.

8.1.2.1 Abhören der Kommunikation

Da RFID-Systeme mittels elektromagnetischen Wellen miteinander kommunizieren, ist das *Abhören* der Systeme grundsätzlich mit einfachen Mitteln möglich. Das Abhören der Kommunikation zwischen einem Lesegerät und einem Transponder ist damit eine der spezifischsten Bedrohungen der RFID-Technologie. Die für RFID-Systeme angegebenen Reichweiten von wenigen Zentimetern (zum Beispiel ISO/IEC 14443, 13,56 MHz) bis hin zu mehreren Metern (ISO/IEC 18000-6, 868 MHz) gelten dabei für die aktive Kommunikation, bei der der Transponder ja noch mit Energie versorgt werden muss, und deshalb eine Spannung von mehreren Volt an der Antenne erzeugt werden muss.

Für Funkempfänger reicht eine um Zehnerpotenzen kleinere Ausgangsspannung der Antenne, um brauchbare Signale zu erhalten. Dies gibt Anlass zu der Vermutung, dass das passive Abhören einer Kommunikation auf eine weit größere Entfernung möglich ist.

Studien hierzu [Finke] zeigen, dass die Kommunikation induktiv gekoppelter Systeme bei 13,56 MHz über eine Entfernung von bis zu 3 m noch abhörbar ist. Das unmodulierte Trägersignal eines Lesegerätes kann bei einer *Empfängerbandbreite* von wenigen kHz sicher über mehrere 100 m detektiert werden. Problematisch für den erfolgreichen Empfang der vollständigen Kommunikation zwischen Lesegerät und Transponder ist jedoch die hierfür benötigte große Empfängerbandbreite, die je nach Bitrate von einigen 100 kHz bis zu mehreren MHz betragen kann. Zum einen erhöht sich die an einem Empfängereingang benötigte Eingangsspannung bei zunehmender Bandbreite um das Verhältnis $U_{in}[dB] = \sqrt{B_1/B_2}$ [ben-sky], zum anderen nehmen in gleichem Maße Störungen durch die teilweise sehr starken Sender in diesem Kurzwellenfrequenzbereich zu.

Weitaus günstiger sind die Verhältnisse im UHF-Frequenzbereich bei 868 MHz, 915 MHz oder auf 2,45 GHz, da hier die *Abhörreichweite* durch den Einsatz von *Richtantennen* deutlich verbessert werden kann (siehe hierzu auch Kapitel 8.1.2.3 “Lesen mit vergrößerter Lesereichweite”). Das *Downlinksignal* eines Lesegerätes sollte bei guten Bedingungen über mehrere hundert Meter empfangbar sein. Das relativ schwache *Backscatter-Signal* der

Transponder sollte dabei wenigstens noch über einige zehn Meter detektierbar bleiben. Störend machen sich jedoch metallische Flächen, also Zäune, Aluminiumverkleidungen an Wänden, aber auch große Gebäude im Ausbreitungsweg der Wellen bemerkbar, da hierdurch die Signale abgeschattet werden.

8.1.2.2 Störsender

Eine sehr einfache, aber wirkungsvolle Methode, die Datenübertragung zwischen einem Transponder und einem Lesegerät zu unterbrechen, ist die Aussendung eines Störsignals mit Hilfe eines *Störsenders*. Erinnern wir uns noch einmal an das Frequenzspektrum eines RFID-Systems (zum Beispiel Abbildung 3.17 auf Seite 48), so sehen wir, dass neben dem sehr starken Trägersignal des Lesegerätes, das bei passiven RFID-Systemen auch zur Energieversorgung des Transponders eingesetzt wird, zwei sehr schwache *Modulationsseitenbänder* in Erscheinung treten, welche durch die Lastmodulation des Transponders (bei induktiver Kopplung) oder durch einen modulierten Rückstrahlquerschnitt (bei Backscatter-Systemen) entstehen. Um das starke Trägersignal eines Lesegerätes zu überdecken, und damit die Datenübertragung vom Lesegerät zu einem Transponder (Downlink) stören zu können, müssen Abstand, Sendeleistung und Antennengewinn bzw. Antennendurchmesser (bei induktiver Kopplung) mindestens dem eingesetzten Lesegerät entsprechen. Das schwache Antwortsignal des Transponders, und damit die Datenübertragung vom Transponder zum Lesegerät (Uplink), ist hingegen mit deutlich geringerem Aufwand zu stören.

Betrachten wir ein Backscatter-System bei 915 MHz, so ergibt sich, unter der Annahme eines Antennengewinns der Leserantenne von $G=1$ sowie der Transponderantenne von $G=1,64$ (Dipol) bei einer Entfernung von etwas über 3 m, eine Freiraumdämpfung von etwa 40 dB (vergleiche Tabelle 3.7 auf Seite 51). Bei einer Strahlungsleistung von 4 W EIRP sieht der Transponder damit noch eine Empfangsleistung $P_e = 0,4$ mW. Die vom Transponder reflektierte Leistung P_s liegt damit theoretisch in einem Bereich von $0 < P_s < 4P_e$, also maximal 1,6 mW (siehe Abbildung 4.89 auf Seite 152). Ein Störsender auf den Frequenzen der Modulationsseitenbänder des Transponders kann bei einer Entfernung zum Lesegerät gleich der des Transponders, also bereits mit einer Sendeleistung von wenigen mW, erheblich Schaden anrichten.

Ähnlich sind auch die Verhältnisse bei induktiv gekoppelten Systemen, allerdings ist hierbei zu beachten, dass auch für einen Störsender der in Kapitel 4.1.1.1 beschriebene Feldstärkeverlauf gültig ist, so dass ein Störsender entweder entsprechend nahe am Lesegerät positioniert werden muss, oder mit entsprechend großen Antennen und Sendeleistungen gearbeitet werden muss.

An dieser Stelle sei darauf hingewiesen, dass auch ein Störsender eine Funkanlage darstellt, und daher in den meisten Ländern der Betrieb eines solchen Gerätes illegal sein dürfte.

8.1.2.3 Lesen mit vergrößerter Lesereichweite

Eine für den Angreifer interessante Möglichkeit bestünde in der *Vergrößerung der Lesereichweite* eines Lesegerätes. Hierdurch könnte es einem Angreifer möglich werden, einen

Transponder aus sicherer Entfernung unentdeckt auszulesen. Gerade zum Thema Lesereichweite werden jedoch die technischen Möglichkeiten sowie die physikalischen Grenzen von RFID-Systemen häufig weit überschätzt. Wegen der großen Unterschiede zwischen induktiver Kopplung und Backscatter-Verfahren werden wir diese im Folgenden getrennt behandeln.

8.1.2.3.1 Induktive Kopplung

Das Ersatzschaltbild eines induktiv gekoppelten RFID-Systems ist in Abbildung 4.29 auf Seite 95 dargestellt. Durch den Strom i_1 in der Antennenspule des Lesegerätes L_1 wird ein magnetisches Feld erzeugt, welches über die Gegeninduktivität M mit der Transponderspule L_2 verkoppelt ist, und dort die Versorgungsspannung des Transponders U_{Q2} induziert. Umgekehrt wirkt der in der Transponderspule fließende Strom i_2 über die magnetische Gegeninduktivität M auf seine Ursache, den Strom i_1 , zurück. Diese Rückwirkung wird dazu eingesetzt, um vom Transponder Daten an das Lesegerät mittels Lastmodulation zu übertragen (siehe hierzu auch Kapitel 4.1.10.3 „Lastmodulation“, S. 103).

Bewegt man einen Transponder über die normale Lesereichweite eines solchen RFID-Systems hinaus, so kann das Abreißen der Kommunikation auf zwei unterschiedliche Ursachen zurückzuführen sein. Ein Ursache kann darin bestehen, dass der Transponder schlicht und einfach nicht mehr genügend Energie zu seinem Betrieb über die Antenne erhält. Genauso ist es jedoch möglich, dass der Transponder noch ausreichend Energie zu seinem Betrieb empfängt, die Amplitude der erzeugten Lastmodulation aber nicht mehr ausreicht, um vom Lesegerät noch detektiert werden zu können. Wir bezeichnen die maximale Reichweite der Energieübertragung als *Energereichweite* des Systems, im Gegensatz zur *Lastmodulationsreichweite*, also des maximalen Abstands zwischen Transponder und Leserantenne, bei dem das Lesegerät gerade noch in der Lage ist, die Lastmodulation des Transponders zu detektieren.

Soll der Leseabstand des Lesegerätes vergrößert werden, muss zunächst die Energereichweite des Lesegerätes vergrößert werden. Hierzu werden zweckmäßigerweise der Durchmesser der Leserantenne sowie der Strom in der Sendeantenne (d. h. die Sendeleistung des Lesegerätes) vergrößert (siehe auch Kapitel 4.1.1.2 „Optimierter Antennendurchmesser“, S. 69). Problematisch ist hierbei jedoch, dass bei zunehmendem Antennendurchmesser der Leserantenne, selbst bei konstantem Abstand zwischen Transponder und Leserantenne, die magnetische Gegeninduktivität und damit auch der Pegel des Lastmodulationssignals am Lesegerät abnimmt. Hinzu kommt noch, dass mit zunehmender Sendeleistung des Lesegerätes das durch den Sender erzeugte (parasitäre) *Rauschen* auch im Frequenzbereich der Lastmodulationsseitenbänder ansteigt. Dies führt dazu, dass sehr schnell eine Grenze erreicht wird, bei der ein zunehmender technischer Aufwand getrieben werden muss, um das Lastmodulationssignal des Transponders noch empfangen zu können. Ein für ISO/IEC 14443 ausgelegter Transponder, der von handelsüblichen Lesegeräten problemlos über eine Entfernung von 10 cm ausgelesen wird, kann laut [kvir-wool] daher selbst unter Optimierung aller Parameter nicht über mehr als 40 cm ausgelesen werden.

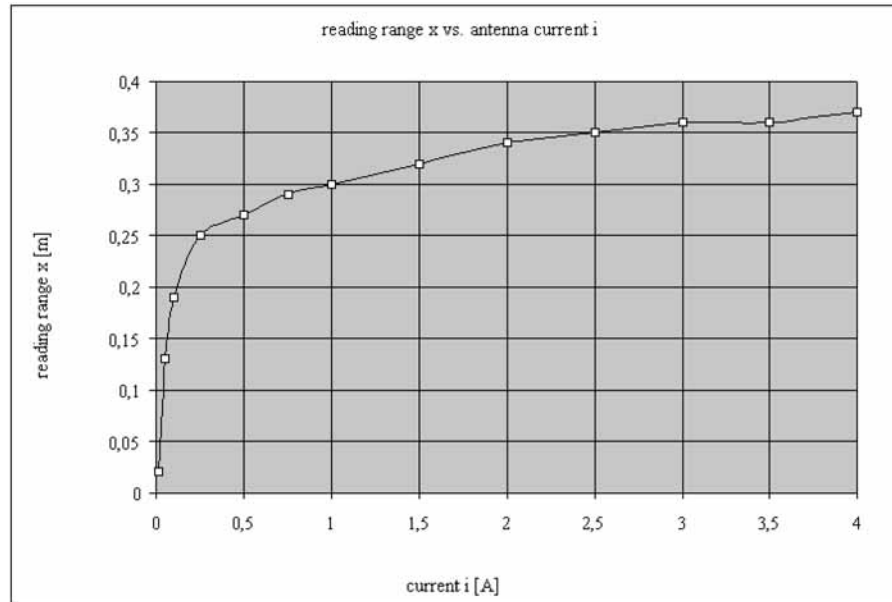


Abb. 8.4 Auch bei zunehmendem Antennenstrom (x-Achse) und optimiertem Antennendurchmesser erreicht die Lesereichweite eines ISO/IEC 14443-Systems eine Grenze bei 40 cm Abstand.

8.1.2.3.2 Backscatter-Kopplung

Das Modell eines passiven Backscatter-Systems ist in Abbildung 4.76 auf Seite 140 dargestellt. Wir erinnern uns, dass ein Teil der von der Antenne des Lesegerätes abgestrahlten Leistung P_1 an der Antenne des Transponders angelangt. Zum Betrieb des Transponders wird davon die Leistung P_e benötigt. Ein anderer Teil der Energie wird von der Antenne des Transponders als Leistung P_s wieder abgestrahlt oder reflektiert. Von der reflektierten Leistung gelangt schließlich ein kleiner Teil P_3 zurück zum Lesegerät, und kann dort detektiert und demoduliert werden.

Bewegt man einen Transponder über die Lesereichweite eines Backscatter-Systems hinaus, kann das Abreißen der Kommunikation auf zwei unterschiedliche Ursachen zurückzuführen sein. Eine sehr nahe liegende Ursache kann darin bestehen, dass der Transponder schlicht und einfach nicht mehr genügend Energie P_e zu seinem Betrieb über die Antenne erhält. Genauso ist es jedoch möglich, dass der Transponder noch ausreichend Energie zu seinem Betrieb empfängt, die reflektierte Leistung P_s aber nicht mehr ausreicht, um vom Lesegerät detektiert werden zu können. Bei den heute verbreiteten Backscatter-Systemen dürfte die Energieaufnahme des Transponderchips²³, also die zum Betrieb des Transponders benötigte Energie P_e , für die Reichweite eines Systems ausschlaggebend sein. Wir bezeichnen diese Reichweite als *Energierreichweite* des Systems, im Gegensatz zur Backscatter-Reichweite, also der theoretischen Reichweite des von der Antenne des Transponders reflektierten Signals.

²³ bei einem passiven Transponder.

Eine nahe liegende Möglichkeit zur Erhöhung der Reichweite ist daher die *Erhöhung der Sendeleistung* des Lesegerätes. Ein Blick auf Formel [4.61] auf Seite 123 zeigt uns, dass wir zur Verdopplung der Energiereichweite die Sendeleistung des Lesegerätes vervierfachen müssen. Um bei doppelter Reichweite die vom Transponder zurück kommende Leistung P_3 konstant zu halten, ist es hingegen notwendig, die Sendeleistung des Lesegerätes zu versechzehnfachen, wie uns ein Blick auf Formel [4.67] auf Seite 126 bestätigt. Stellt man die benötigte Sendeleistung als Funktion der Energiereichweite sowie der Backscatter-Reichweite grafisch dar (siehe Abbildung 8.5), so erkennt man, dass es einen Schnittpunkt der beiden Graphen gibt.

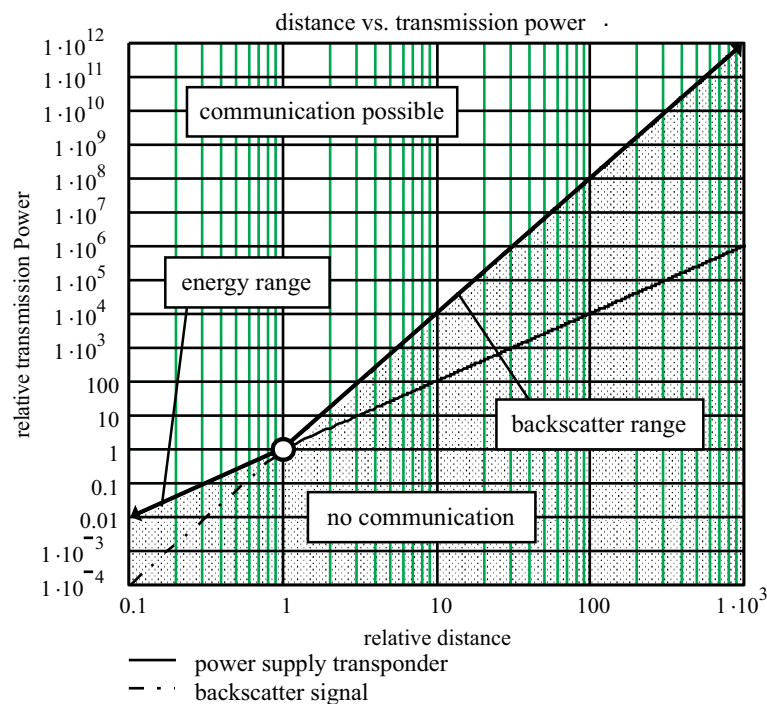


Abb. 8.5 Die benötigte Sendeleistung als Funktion der Energiereichweite (power supply transponder) und der Backscatter-Reichweite (backscatter signal).

Wie bereits erwähnt können wir davon ausgehen, dass die Reichweite der meisten Transpondersysteme durch die Energiereichweite des Systems bestimmt ist. Bei einer bestimmten Sendeleistung befinden wir uns daher auf einem Punkt der Geraden der Energiereichweite (energy range) links vom Schnittpunkt. Solange wir uns links vom Schnittpunkt befinden, ist die Reichweite also proportional der Quadratwurzel der Sendeleistung. Mit einer Verzehnfachung der Sendeleistung ließe sich so die Reichweite eines Systems verdreifachen. Dies gilt jedoch nur solange, bis wir den Schnittpunkt der beiden Geraden erreichen. Rechts vom Schnittpunkt hat der Transponder zwar immer ausreichend Energie zum Betrieb zur Verfügung, das vom Transponder reflektierte Signal wird aber schnell zu schwach, um vom Lesegerät noch detektiert werden zu können. Sobald der Schnittpunkt der beiden Geraden

erreicht ist, müssen wir die Sendeleistung verhundertfachen, um die Lesereichweite noch einmal zu verdreifachen. Um die Reichweite ausgehend vom Schnittpunkt der beiden Geraden zu verzehnfachen, müssten wir die Sendeleistung sogar um den Faktor 10.000 erhöhen. Dies führt jedoch zu anderen Effekten, wie ein zunehmendes Seitenbandrauschen um das Trägersignal des Lesegerätes, sowie zu *Intermodulationsprodukten* durch Unlinearitäten im parallel betriebenen Empfänger des Lesegerätes, welche die theoretisch mögliche Reichweite noch einmal stark reduzieren können.

Gehen wir noch einmal zurück zu Abbildung 4.76 auf Seite 140, so sehen wir, dass der Antennengewinn der Leserantenne zweifach in den Ausbreitungsweg der Signale eingeht. Zunächst wird die in der Entfernung r am Transponder ankommende Leistung P_2 um den Antennengewinn verstärkt. Im gleichen Maße erhöht sich die vom Transponder reflektierte Leistung P_s . Der vom Lesegerät empfangene Anteil der reflektierten Leistung P_3 wird von der Antenne des Lesegerätes ein weiteres Mal um den *Antennengewinn* der Leserantenne verstärkt. In der Gesamtwirkung entspricht dies einer Verschiebung des Schnittpunktes unserer beiden Graphen aus Abbildung 8.5 nach rechts.

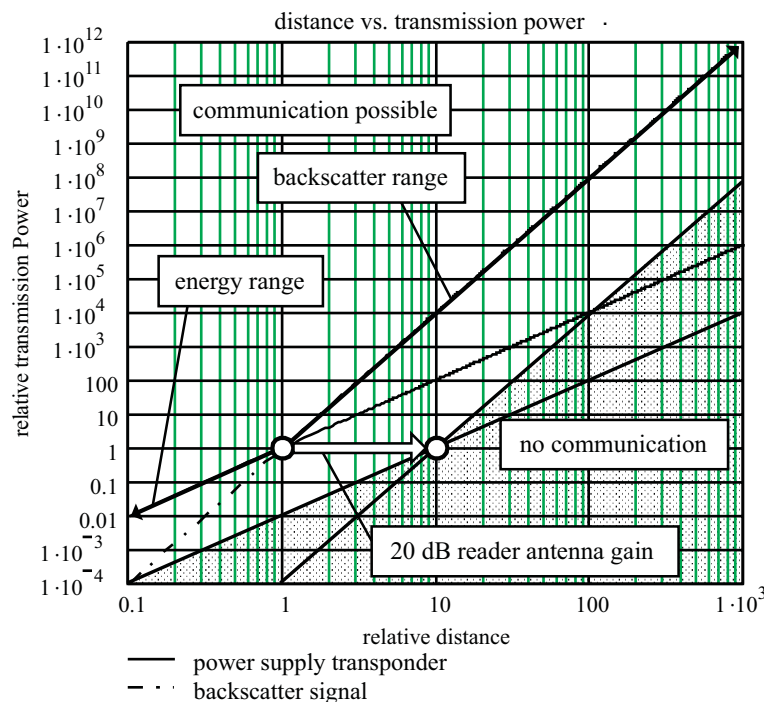


Abb. 8.6 Durch zusätzlichen Antennengewinn kann die Reichweite des Systems einfach erhöht werden.

Der Reichweitengewinn durch die Erhöhung des Antennengewinns kann sehr einfach anhand von Formel [4.114] auf Seite 156 berechnet werden, und ist in Abbildung 8.7 noch einmal grafisch dargestellt.

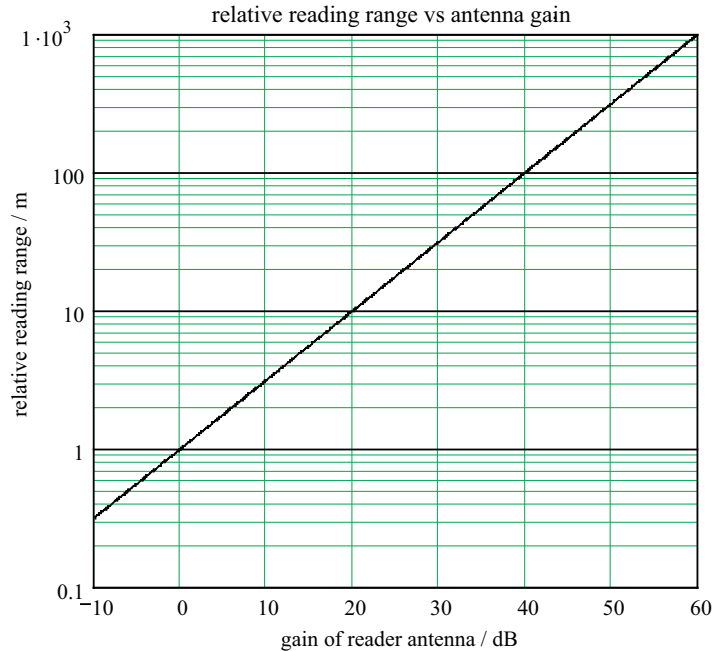


Abb. 8.7 Durch das Vergrößern des Antennengewinns kann die Reichweite eines UHF-Systems effektiv vergrößert werden.

Gewinne bis etwa 17 dB können dabei noch relativ einfach unter Verwendung einer Langyagi-Antenne erreicht werden [rothammel]. Bei 17 dB Antennengewinn erreicht die Länge des Trägerrohres dabei allerdings schon eine Länge von knapp dem 10-fachen der Wellenlänge λ , also etwa 3,4 m für 868 MHz, 3,3 m für 915 MHz oder 1,2 m bei 2,45 GHz. Immerhin kann damit schon etwa die 7- bis 8-fache Lesereichweite gegenüber der Verwendung einer Dipolantenne erreicht werden. Die Theorie besagt, dass bei Verdoppelung der Antennenlänge und Elementenzahl der Gewinn um maximal 3 dB ansteigen kann [rothammel]. Um einen Antennengewinn von 20 dB, und damit die 10-fache Lesereichweite zu erreichen, benötigt man daher mindestens eine Antenne doppelter Länge, also das 20-fache der Wellenlänge λ . Für 868 MHz ergibt sich daraus eine Länge des Trägerrohres von ganzen 7 m. Eine Größe also, bei der die Antenne schon reichlich unhandlich wird. Um die 20-fache Lesereichweite zu erreichen, wird ein Antennengewinn von etwa 26 dB benötigt. Dies kann nur noch durch das Zusammenschalten mehrerer *Langyagi-Antennen* zu einer *Antennengruppe* erreicht werden, was bereits zu Antennenungetümen mit Abmessungen von mehreren Metern führt. Aus der Praxis sind Angriffe mit Langyagi-Antennen schon bekannt. So hat Mitte 2005 der erfolgreiche Versuch, einen Transponder über einen Abstand von 21 m (69 feet) auszulesen, zu einigem Aufsehen in der Fachpresse geführt [defcon-69] [cheung].

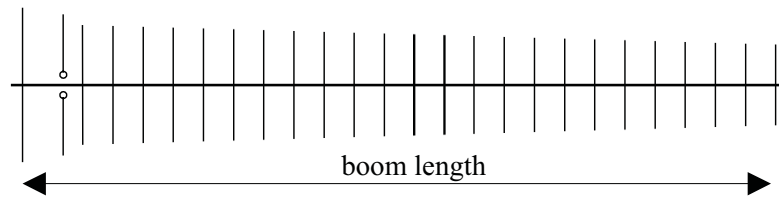


Abb. 8.8 Schematische Darstellung einer Langyagi-Antenne mit 26 Elementen.

Sollen noch höhere Antennengewinne erreicht werden, um die Reichweite noch weiter zu steigern, so müssen Parabolspiegel zum Einsatz kommen. Die 100-fache Lesereichweite kann dann mit einem Gewinn von 40 dB erreicht werden. Der erforderliche Spiegeldurchmesser beträgt für 868 MHz knappe 15 m (5,1 m bei 2,45 GHz). Für die 1000-fache Lesereichweite schließlich ist ein Gewinn von 60 dB erforderlich, für dessen Realisierung wir einen *Parabolspiegel* mit ganzen 145 m Durchmesser (52 m bei 2,45 GHz) benötigen.

Aus diesen Berechnungen ist leicht abzusehen, bis zu welchen Entfernungen ein Angriff noch mit vernünftigem Aufwand zu realisieren ist. Ab günstigsten erscheint dabei eine Kombination aus einer Langyagi-Antenne mit einer moderat angehobenen Sendeleistung des Lesegerätes. Sinnvoll wäre es hier, den Schnittpunkt der beiden Geraden aus Abbildung 8.6 zu treffen. Viel mehr als die 20-fache Reichweite scheint aber mit vertretbarem Aufwand aus heutiger Sicht nicht realisierbar zu sein.

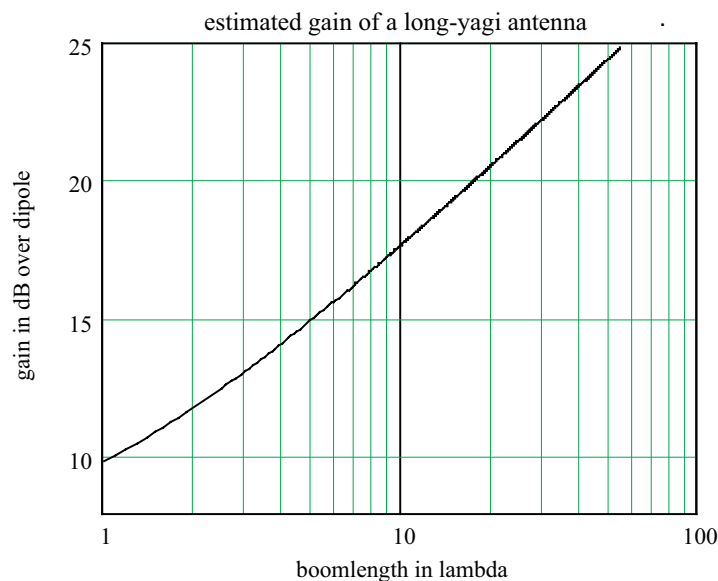


Abb. 8.9 Der theoretische Gewinn einer Langyagi-Antenne, gemessen in dB über Dipol, in Abhängigkeit der Länge des Trägerrohres (boom) in Vielfachen der Wellenlänge λ (nach [rothammel]).

8.1.2.4 Denial of Service-Angriff durch Blocker Tags

Moderne RFID-Lesegeräte sind problemlos in der Lage, auch mit einer größeren Anzahl von Transpondern im Ansprechfeld zu kommunizieren. Hierzu verwendet das Lesegerät einen *Antikollisionsalgorithmus*, mit dem ein einzelner Transponder selektiert werden kann, um anschließend eine Kommunikation mit diesem Transponder durchzuführen. Für einige Anwendungen ist es auch ausreichend, ausschließlich die *Seriennummern* der in Lesereichweite befindlichen Transponder zu ermitteln, da die dazugehörigen Daten in einer Datenbank geführt werden (z. B. Produktdaten zu einem EPC).

In der Praxis haben sich vor allem zwei Antikollisionsalgorithmen durchgesetzt, der binäre Suchbaum (*Binary-Search-Tree-Algorithmus*) sowie das *Slotted-ALOHA-Verfahren*. Zum tieferen Verständnis der Blocker Tags sei daher auch auf das vorhergehende Kapitel 7.2.4.2 „Slotted-ALOHA-Verfahren“, S. 222, sowie auf das Kapitel 7.2.4.3 „Binary-Search-Algorithmus“, S. 226 verwiesen.

Bei Verwendung des binären Suchbaums wird also, wie in Kapitel 7 gezeigt, ein rekursiver Algorithmus eingesetzt, bei dem bei jeder auftretenden Kollision an einer Bitstelle der empfangenen Seriennummern eine Verzweigung im binären Baum gewählt wird, indem das entsprechende Bit in der nachfolgenden Iteration auf „0“ oder „1“ gesetzt wird. Genau hier setzt das *Blocker Tag* an, das an jeder Bitposition der Seriennummer eine Kollision simuliert, indem es gleichzeitig eine „0“ und eine „1“ sendet (vergleiche Abbildung 7.20 auf Seite 227). Dem so getäuschten Lesegerät bleibt nichts anderes übrig, als den gesamten binären Suchbaum zu durchlaufen [juels].

Das Blocker Tag täuscht einem angegriffenen Lesegerät vor, es würden sich 2^k Transponder in dessen Ansprechfeld befinden, wobei k die Anzahl der Bits der Seriennummer darstellt. Das Abfragen einer derart großen Anzahl von Seriennummern blockiert das betroffene Lesegerät im wahrsten Sinn des Wortes. Benötigt ein Lesegerät zum Ermitteln einer einzelnen Seriennummer eine Zeit t_1 , so wird zum Durchlaufen des vollständigen Suchbaums die Zeit $t_g = t_1 \cdot 2^n$ benötigt, wobei n die Anzahl der Bits einer einzelnen Seriennummer darstellt. Nehmen wir an, die Zeit t_1 beträgt 1 ms und die Länge n einer Seriennummer unseres Systems beträgt 48 Bit, so benötigt ein Lesegerät zum Durchlaufen des gesamten Suchbaums $t_g = 2,8 \cdot 10^{11}$ Sekunden, oder in Jahren: 8925! Es ist klar, dass es einem Lesegerät damit unmöglich gemacht wird, einen echten Transponder in seinem Ansprechfeld auszumachen, zumal eine Unterscheidung zwischen echter und vorgetäuschter Seriennummer in der Regel nicht möglich ist. Ein Blocker Tag, das den vollständigen Suchbaum eines Lesegerätes blockiert (*Denial of Service, DOS*), wird auch als *Full-Blocker* oder als *Universal-Blocker* bezeichnet [juels].

Auch das weit verbreitete Slotted-ALOHA-Verfahren kann von einem Blocker-Tag leicht blockiert werden. Bei diesem Verfahren folgt dem Antikollisionskommando eines Lesegerätes eine vorher definierte Anzahl von Zeitschlitz (Slots), in denen die im Ansprechfeld des Lesers befindlichen Transponder ihre Seriennummer an das Lesegerät senden. Die Transponder wählen dabei den von ihnen verwendeten Schlitz zufällig aus. Versuchen zwei oder mehr Transponder, ihre Seriennummer im selben Zeitschlitz zu übertragen, so kann wegen der auf-

tretenden Kollision keine der Seriennummern mehr richtig gelesen werden. Um das Slotted-ALOHA-Verfahren zu stören, muss ein Blocker Tag einfach nur in jedem der zur Verfügung stehenden Zeitschlitz eine Seriennummer, oder noch einfacher, ein ungültiges Datenpaket (z. B. ein Datenpaket mit absichtlich falscher Prüfsumme) senden. Für das Lesegerät wird es damit unmöglich, einen weiteren Transponder im Ansprechfeld zu detektieren.

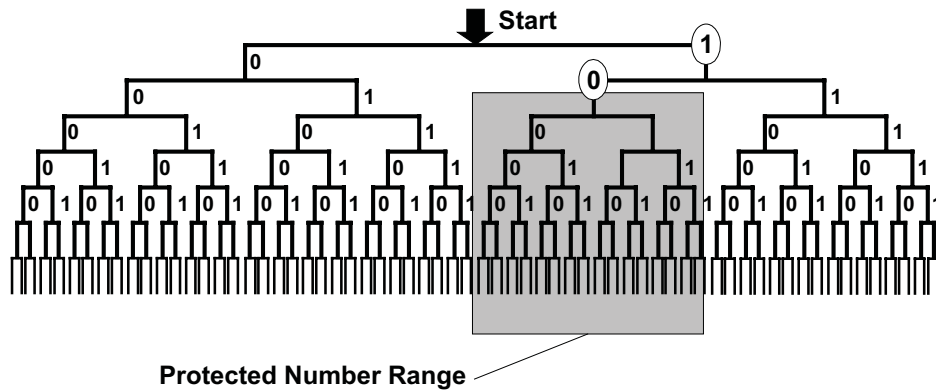


Abb. 8.10 Bestimmte Nummernbereiche können von der Blockierung ausgenommen werden.

Nicht immer ist es erwünscht, den Suchbaum und damit den Nummernkreis eines RFID-Systems vollständig zu blockieren. So kann es sein, dass bestimmte Nummernkreise der Seriennummern bestimmten Anwendungen zugeordnet sind. So besteht z. B. eine EPC-Seriennummer aus einem 8 Bit Header, 28 Bit EPC Manager code (Organisation, die den Transponder herausgegeben hat), 24 Bit Object manager code (Bezeichnung des Objekts laut Angabe des vorhergehenden EPC Managers) sowie einer 36 Bit langen individuellen Nummer. Ein Blocker Tag könnte daher so ausgelegt sein, dass bestimmte Teile des binären Suchbaums von der Blockierung ausgeschlossen werden. So werden im Beispiel in Abbildung 8.10 alle Seriennummern eines RFID-Systems, die mit den Bits „01“ beginnen, von der Blockierung ausgenommen.

8.1.2.5 Relay-Attack

Hierbei handelt es sich um eine besondere Art eines Angriffes, bei der der Angreifer die Reichweite zwischen Lesegerät und Transponder durch eine zwischengeschaltete Übertragungseinrichtung (Relais) fast beliebig erweitern kann. Der Angreifer leiht sich dabei den Transponder kurzzeitig aus und täuscht dem Lesegerät mit Hilfe des Relais vor, der Transponder befände sich selbst im Ansprechbereich des Lesegerätes. Hierzu benötigt der Angreifer noch nicht einmal physischen Zugriff auf den Transponder, sondern muss sich lediglich in Lesereichweite des Transponders befinden. Der Inhaber des Transponders bemerkt den Angriff in der Regel nicht, oder erst zu einem späteren Zeitpunkt lange nach dem Angriff, etwa wenn unter Verwendung des angegriffenen Transponders kostenpflichtige Aktionen (z. B. Einkäufe oder Bahnfahrten) ausgelöst wurden.

Zur praktischen Durchführung einer *Relay-Attack* werden zwei unterschiedliche Komponenten benötigt, die über eine Funkverbindung miteinander verbunden werden [kvir-wool] [hancke]. In die Nähe des Lesegerätes wird eine Komponente (*Ghost, Proxy*) gebracht, die in der Lage ist, die Signale des Lesegerätes zu empfangen und eine Lastmodulation zu erzeugen, um mit dem Lesegerät zu kommunizieren und somit einen Transponder zu *simulieren*. Die zweite Komponente (*Leech, Mole*) besteht aus einem Sender, der einen Transponder mit Energie zu dessen Betrieb versorgen kann, sowie eine Lastmodulation des Transponders demodulieren kann und somit in der Lage ist, ein Lesegerät zu simulieren (Abbildung 8.11).

Die einfachste Möglichkeit besteht nun darin, die vom Lesegerät oder dem Transponder empfangenen Daten im Ghost zu demodulieren, und den empfangenen Datenstrom eins zu eins über die Funkverbindung an den Leech zu übertragen, welcher den Datenstrom schließlich an den Transponder sendet [hancke]. Umgekehrt werden die vom Transponder gesendeten Antwortdaten im Leech demoduliert, und der so empfangene Datenstrom eins zu eins über die Funkverbindung an den Ghost gesendet, der wiederum die Daten per Lastmodulation an das Lesegerät weiter überträgt (Abbildung 8.12). Für das Lesegerät erscheint dies so, als sei der Transponder wirklich in der Ansprechreichweite des Lesegerätes, so dass eine vollständige Transaktion zwischen dem Transponder und dem Lesegerät abgewickelt werden kann.

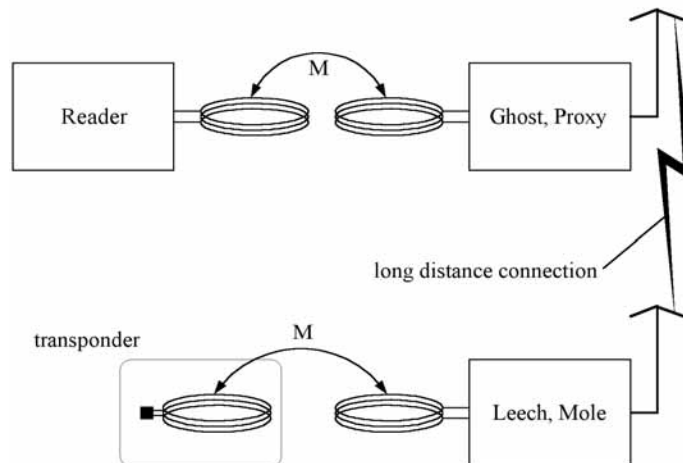


Abb. 8.11 Bei der Relay-Attacke wird einem Lesegerät vorgetäuscht, ein weit entfernter Transponder befände sich innerhalb der Lesereichweite des Lesegerätes. Dadurch kann der Angreifer Aktionen auslösen, zu denen sonst die physikalische Anwesenheit des Transponders am Lesegerät benötigt wird (z. B. Zutrittsysteme, Zahlungsverkehr, etc.)

Bei der Übertragung des Datenstroms zwischen Ghost und Leech treten jedoch *Laufzeiten* auf, welche mit zunehmendem Abstand größer werden. Beim Einsatz einer Funkstrecke werden die Signale zwar mit Lichtgeschwindigkeit übertragen, aber auch dies bedeutet eine Laufzeit von etwa $3 \mu\text{s}$ pro Kilometer Entfernung, in eine Richtung. Für ein zeitkritisches Protokoll, wie z. B. ISO/IEC 14443 Typ A, kann dies schnell zu einem Problem werden. Ist das letzte Bit eines vom Lesegerät gesendeten Request- oder Antikollisionskommandos eine

„1“, so muss das erste Bit der Antwort des Transponders nach einer Zeit von exakt $91,1 \mu\text{s}$ beim Lesegerät eintreffen. Die Dauer eines Bits beträgt dabei, bei der verwendeten Bitrate von 106 kBit/s , etwa $9,43 \mu\text{s}$. Bei der Übertragung der Modulationssignale über eine Entfernung von einem Kilometer kommt das Kommando des Lesegerätes dabei schon mit $3 \mu\text{s}$ Verzögerung an. Bei der Übertragung der Antwort vom Leech zum Ghost kommen noch einmal $3 \mu\text{s}$ Verzögerung hinzu, so dass die Antwort des Transponders $6 \mu\text{s}$ später als erwartet am Lesegerät eintrifft, was bereits mehr als der halben Dauer eines Bits entspricht und dazu führen kann, dass die Antwort vom Lesegerät nicht mehr akzeptiert wird.

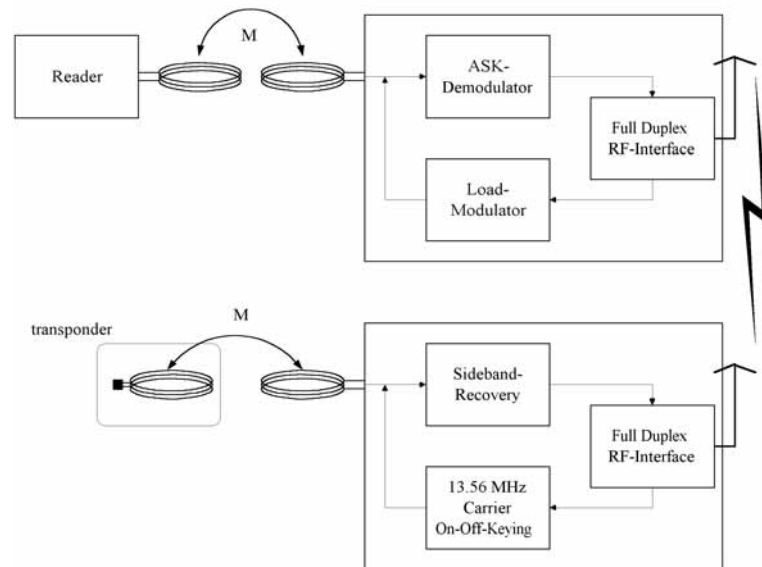


Abb. 8.12 Ein analoges Relais-System kann durch die Übertragung eines demodulierten Datenstroms zwischen Ghost und Leech sehr einfach realisiert werden.

Die bei der Aussendung eines Applikationskommandos geltenden Timeoutzeiten sind um ein Vielfaches größer als die von ISO/IEC 14443 Typ A tolerierten zeitlichen Abweichungen auf ein Request- oder Antikollisionskommando. Auf der anderen Seite ist das Protokoll für die Applikationsdaten vollkommen transparent, d. h. die Applikationsdaten (INF / APDU) werden in der Protokollschicht verpackt, aber niemals verändert, wie dies z. B. in Abbildung 9.28 auf Seite 286 dargestellt ist. Aus diesem Grunde kann im Ghost der vollständige *Protokollstack* eines Transponders implementiert werden. Zeitkritische Kommandos wie ein Request- oder Antikollisionskommando können dann vom Ghost selbständig abgearbeitet werden, und benötigen noch nicht einmal eine Interaktion mit dem Leech oder dem anzugreifenden Transponder. Auf die gleiche Weise kann auf Seiten des Leech eine Kommunikationsbeziehung mit einem Transponder aufgebaut werden, ohne zunächst mit dem Ghost kommunizieren zu müssen. Wird vom Ghost schließlich ein Datenblock empfangen, so werden nur die darin enthaltenen Applikationsdaten (APDU) an den Leech übertragen, welcher diese wieder in einen vollständigen Datenblock (Abbildung 9.28) verpackt und an den Transponder weitersendet. In umgekehrter Übertragungsrichtung wird analog dazu verfahren.

ren. *Timeoutzeiten* für Applikationskommandos betragen in der Regel einige zehn bis hundert Millisekunden, so dass die Übertragungszeiten zwischen Ghost und Leech kaum noch ins Gewicht fallen. Auf diese Weise können durch den Angreifer sehr große Entfernungen überbrückt werden. Selbst eine streckenweise Datenübertragung im Internet ist denkbar.

Relais-Attacken unter Verwendung eines Protokollstacks in Ghost und Leech lassen sich wegen der üblicherweise strikten Trennung von Protokoll- und Anwendungsdaten (APDU) nicht erkennen. Dies wäre nur mit Verfahren möglich, welche diese strikte Trennung aufheben und beispielsweise auch Statusinformationen der Protokollschicht in eine *Authentifizierung* zwischen Transponder und Lesegerät (siehe Kapitel 8.2.1 “Gegenseitige symmetrische Authentifizierung”) einbeziehen [hancke-kuhn].

8.2 Abwehr durch kryptographische Maßnahmen

In zunehmendem Maße werden RFID-Systeme auch in sicherheitsrelevanten Anwendungen, wie Zutrittssystemen, oder als Zahlungsmittel und Tickets eingesetzt. Bei diesen Einsatzbereichen muss jedoch immer mit potenziellen *Angriffsversuchen* gerechnet werden, bei denen versucht wird, RFID-Systeme „auszutricksen“ und sich damit unberechtigten Zutritt zu Gebäuden oder einen unbezahlten Zugriff auf Dienstleistungen (Tickets) zu verschaffen. Die technischen Möglichkeiten hierzu haben wir bereits in Kapitel 8.1 “Angriffe auf RFID-Systeme” eingehend untersucht.

Schon in den Mythen und Märchen wurde versucht, *Sicherheitssysteme* zu überlisten. So gelang es zum Beispiel *Ali Baba*, durch das Ausspähen eines geheimen Passwortes, sich unberechtigten Zutritt in das vermeintlich sichere Warenlager der 40 Räuber zu verschaffen. Auch bei modernen *Authentifizierungsprotokollen* wird ausnahmslos die Kenntnis eines Geheimnisses (d. h. eines kryptographischen Schlüssels) überprüft. Durch geeignete Algorithmen kann jedoch das Ausspähen der geheimen Schlüssel verhindert werden. Im Einzelnen müssen folgende Angriffsversuche auf sicherheitsrelevante RFID-Systeme abgewehrt werden können:

- Unberechtigtes Auslesen eines Datenträgers, um Daten zu duplizieren und/oder zu verändern.
- Einbringen eines applikationsfremden Datenträgers in den Lesebereich eines Lesegerätes mit der Absicht, unberechtigten Zutritt oder Leistungen zu erlangen.
- Abhören der Funkverbindung und Wiedervorspielen der Daten, um so einen echten Datenträger vorzutäuschen („replay and fraud“).

Bei der Auswahl von geeigneten RFID-Systemen sollte den kryptologischen Funktionen der betrachteten Systeme besondere Aufmerksamkeit zukommen. Anwendungen, die keinerlei Sicherheitsfunktionen bedürfen (z. B. Industrieautomation, Werkzeugerkennung), werden durch kryptologische Verfahren nur unnötig verteuert. Im Gegensatz dazu kann sich bei sicherheitsrelevanten Anwendungen (z. B. Ticketing, Kleingeldbörse) der unüberlegte Verzicht auf kryptologische Verfahren durch unberechtigte Inanspruchnahme von Leistungen mittels manipulierter Transponder teuer rächen.

8.2.1 Gegenseitige symmetrische Authentifizierung

Die *gegenseitige Authentifizierung* zwischen Lesegerät und Transponder beruht auf der „*Three Pass Mutual Authentication*“ nach ISO 9798-2, bei der beide Kommunikationsteilnehmer gegenseitig die Kenntnis eines Geheimnisses (geheimer kryptographischer Schlüssel) überprüfen.

Bei diesem Verfahren sind alle zu einer Applikation gehörenden Transponder und Lesegeräte im Besitz des **gleichen**, geheimen *kryptographischen Schlüssels* K (\rightarrow symmetrisches Verfahren). Beim Eintritt eines Transponders in den Lesebereich eines Lesegerätes ist zunächst nicht bekannt, ob beide Kommunikationsteilnehmer der gleichen Applikation angehören. Aus Sicht des Lesegerätes besteht das Bedürfnis, die Applikation vor einer *Manipulation* mit gefälschten Daten zu schützen. Ebenso besteht auf Seiten des Transponders das Bedürfnis, die gespeicherten Daten vor unberechtigtem Auslesen oder Überschreiben zu schützen.

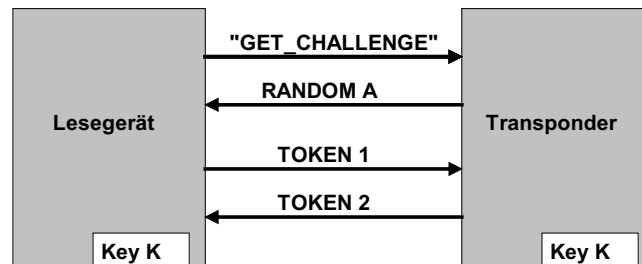


Abb. 8.13 Ablauf einer gegenseitigen Authentifizierung zwischen Transponder und Lesegerät.

Die gegenseitige Authentifizierung beginnt damit, dass das Lesegerät ein „GET_CHALLENGE“-Kommando an das TAG sendet. Im Transponder wird daraufhin eine *Zufallszahl* (random number) R_A erzeugt und an das Lesegerät zurückgesendet (response \rightarrow challenge-response-Verfahren). Das Lesegerät erzeugt nun seinerseits eine Zufallszahl R_B . Unter Verwendung des gemeinsamen geheimen Schlüssels K und eines gemeinsamen Schlüsselalgorithmus e_K berechnet das Lesegerät einen verschlüsselten Datenblock (Token 1), welcher beide Zufallszahlen sowie zusätzliche Steuerdaten enthält, und sendet diesen Datenblock an den Transponder.

$$\text{Token 1} = e_K(R_B || R_A || \text{ID}_A || \text{Text1}) \quad [8.1]$$

Im Transponder wird das empfangene Token 1 entschlüsselt und die dadurch im Klartext erhaltene Zufallszahl R_A' auf Übereinstimmung mit der zuvor ausgesendeten R_A verglichen. Stimmen beide Zahlen überein, ist aus Sicht des Transponders somit auch die Übereinstimmung der beiden gemeinsamen Schlüssel bewiesen. Im Transponder wird nun erneut eine Zufallszahl R_{A2} erzeugt und daraus ein verschlüsselter Datenblock (Token 2) errechnet, der zusätzlich R_B und Steuerdaten enthält. Token 2 wird vom Transponder an das Lesegerät gesendet.

$$\text{Token 2} = e_K(R_{A2} || R_B || \text{Text2}) \quad [8.2]$$

Das Lesegerät überprüft nun, nach der Entschlüsselung von Token 2, seinerseits die Übereinstimmung der zuvor ausgesendeten R_B mit der eben empfangenen R_B' . Stimmen beide Zahlen überein, so ist nun auch aus Sicht des Lesegeräts die Übereinstimmung der gemeinsamen Schlüssel bewiesen. Transponder und Lesegerät haben sich somit als einem gemeinsamen System zugehörig identifiziert, die weitere Kommunikation zwischen beiden Kommunikationsteilnehmern ist somit legitimiert.

Zusammenfassend weist das Verfahren der gegenseitigen Authentifizierung folgende Vorteile auf:

- Die geheimen Schlüssel werden nie über die Funkstrecke übertragen, es werden lediglich verschlüsselte Zufallszahlen übertragen.
- Es werden immer zwei Zufallszahlen gleichzeitig verschlüsselt. Eine Rücktransformation von Token 1 über R_A , mit dem Ziel, den geheimen Schlüssel zu errechnen, scheidet damit aus.
- Es können beliebige Algorithmen zur Verschlüsselung der Token verwendet werden.
- Durch die strikte Verwendung von Zufallszahlen aus zwei unabhängigen Quellen (Transponder, Lesegerät) bleibt das Aufzeichnen und spätere Wiedervorspielen einer Authentifizierungssequenz (replay attack) ohne Erfolg.
- Aus den erzeugten Zufallszahlen kann ein zufälliger Schlüssel (session key) berechnet werden, um damit die nachfolgende Datenübertragung kryptologisch zu sichern.

8.2.2 Authentifizierung mit abgeleiteten Schlüsseln

Ein Nachteil des in 8.1 beschriebenen Authentifizierungsverfahren besteht darin, dass alle zu einer Applikation gehörenden Transponder mit einem identischen kryptographischen Schlüssel K gesichert sind. Dies stellt für Anwendungen, bei denen sehr große Mengen von Transpondern im Einsatz sind (z. B. Ticketing im ÖPNV mit einigen Millionen Transponder), eine potenzielle Gefahr dar. Da solche Transponder für jedermann in unkontrollierbarer Anzahl zugänglich sind, muss mit einer geringen Wahrscheinlichkeit damit gerechnet werden, dass der Schlüssel eines Transponders aufgedeckt wird. Das oben beschriebene Verfahren wäre damit Manipulationen ungeschützt ausgeliefert.

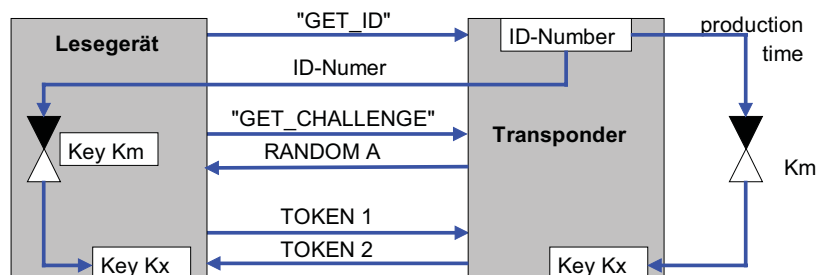


Abb. 8.14 Bei einer Authentifizierung mit abgeleiteten Schlüsseln wird zunächst aus der Seriennummer (ID-Number) des Transponders ein transpondereigener Schlüssel im Lesegerät berechnet. Dieser Schlüssel muss dann zur Authentifizierung eingesetzt werden.

Eine wesentliche Verbesserung des beschriebenen Authentifizierungsverfahrens besteht darin, jeden Transponder mit einem anderen kryptographischen Schlüssel zu sichern. Hierzu wird während der Produktion des Transponders dessen Seriennummer ausgelesen. Mittels eines kryptologischen Algorithmus und eines *Masterschlüssels* K_M wird daraus ein Schlüssel K_X berechnet (= abgeleitet) und damit der Transponder initialisiert. Jeder Transponder erhält dadurch einen mit der eigenen ID-Nummer und dem Masterschlüssel K_M verknüpften Schlüssel.

Die gegenseitige Authentifizierung beginnt damit, dass das Lesegerät die ID-Nummer des Transponders anfordert. In einem besonderen Sicherheitsmodul des Lesegerätes, dem *SAM* (security authentication module), wird daraus unter Verwendung des Masterschlüssels K_M der spezifische Schlüssel des Transponders berechnet, um mit diesem das Authentifizierungsverfahren einzuleiten. Als SAM werden üblicherweise kontaktbehaftete Chipkarten mit Kryptoprozessoren verwendet, der gespeicherte Masterschlüssel kann damit niemals ausgelesen werden.

8.2.3 Verschlüsselte Datenübertragung

In Kapitel 7.1 „Prüfsummenverfahren“, S. 209, wurde die Behandlung von Störungen dargestellt, wie sie bei der Übertragung von Daten durch physikalische Einflüsse auftreten. Wir erweitern nun dieses Modell um einen potenziellen Angreifer. Grundsätzlich kann zwischen zwei Arten eines Angriffs unterschieden werden: Angreifer 1 verhält sich passiv und versucht, durch Abhören der Übertragungsstrecke vertrauliche Daten zur missbräuchlichen Verwendung auszuspähen. Angreifer 2 hingegen versucht aktiv, die übertragenen Daten zu manipulieren und zu seinen Gunsten zu verändern.

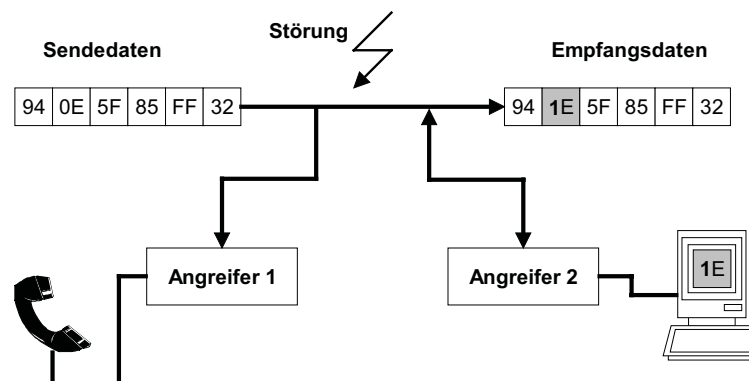


Abb. 8.15 Angriffsversuche auf eine Datenübertragungsstrecke. Angreifer 1 versucht, die übertragenen Daten abzu hören, während Angreifer 2 die Daten mutwillig verändert.

Im Empfänger werden die Chiffredaten durch Verwendung eines geheimen Schlüssels K' sowie eines geheimen Algorithmus wieder in die ursprüngliche Form zurücktransformiert (= *Entschlüsseln*, *Dechiffrieren*).

Um sowohl passive als auch aktive Angriffsversuche wirkungsvoll zu unterbinden, werden kryptographische Verfahren eingesetzt. Hiermit können die Sendedaten (Klartext) vor der

Übertragung so verändert (= verschlüsselt) werden, dass einem potenziellen Angreifer kein Rückschluss mehr auf den wirklichen Inhalt der Nachricht (Klartext) möglich ist.

Eine *verschlüsselte Datenübertragung* erfolgt immer nach dem gleichen Schema: Unter Verwendung eines geheimen *Schlüssels K* sowie eines geheimen Algorithmus werden die Sendedaten (Klartext) in Chiffredaten (Chiffretext) transformiert (= *Verschlüsseln, Chiffrieren*). Für einen potenziellen Angreifer sind die abgehörten Daten ohne Kenntnis des angewendeten Verschlüsselungsalgorithmus sowie des geheimen Schlüssels *K* nicht interpretierbar. Ein Rückschluss von den Chiffredaten auf die Sendedaten ist nicht möglich.

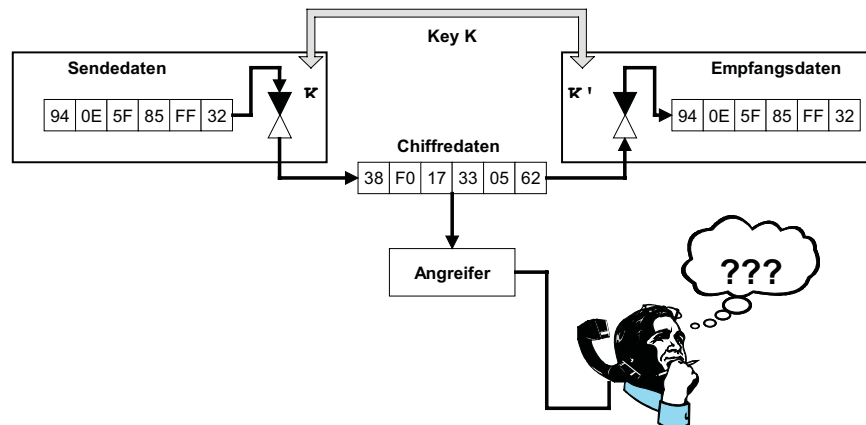


Abb. 8.16 Durch die Verschlüsselung der zu übertragenden Daten ist ein wirkungsvoller Schutz der Daten vor dem Abhören oder Verändern möglich.

Falls die Schlüssel *K* zum Chiffrieren und *K'* zum Dechiffrieren identisch sind ($K=K'$) oder in einem direkten Zusammenhang stehen, spricht man von einem *symmetrischen Schlüssel-Verfahren*. Ist die Kenntnis des Schlüssels *K* für die Dechiffrierung irrelevant, so handelt es sich um ein *asymmetrisches Schlüssel-Verfahren*. Bei RFID-Systemen werden bislang ausschließlich symmetrische Verfahren eingesetzt, auf andere Verfahren wird deshalb hier nicht weiter eingegangen.

Wird jedes Zeichen vor der Übertragung einzeln verschlüsselt, so handelt es sich um *sequentielle Chiffren* (auch *Stromverschlüsselung, streamcipher*). Werden hingegen mehrere Zeichen zu einem Block zusammengefasst, so spricht man von einem Blockchiffre. Da Blockchiffren in der Regel sehr rechenintensiv sind, spielen sie bei RFID-Systemen eine untergeordnete Rolle. Im Folgenden wird der Schwerpunkt deshalb auf sequentielle Chiffren gelegt.

Ein grundsätzliches Problem aller kryptographischen Verfahren ist die sichere Verteilung des geheimen Schlüssels *K*, der ja den berechtigten Kommunikationsteilnehmern vor Beginn der Datenübertragung bekannt sein muss.

8.2.3.1 Streamcipher

Als sequentielle Chiffren oder Stromchiffren werden Verschlüsselungsalgorithmen bezeichnet, bei denen die Folge von Klartextzeichen nacheinander in jedem Schritt mit einer variie-

renden Funktion verschlüsselt wird [fury]. Die Ideallösung einer Stromchiffre ist das so genannte „one-time-pad“, nach seinem Erfinder auch „Vernam Chiffre“ genannt [longo].

Hierzu wird vor der verschlüsselten Datenübertragung, zum Beispiel durch Würfeln, ein zufälliger Schlüssel K erzeugt und beiden Kommunikationsteilnehmern zur Verfügung gestellt. Die Verknüpfung der Schlüsselreihe mit der Klartextreihe geschieht durch zeichenweise Addition oder XOR-Verknüpfung. Die Länge der als Schlüssel verwendeten Zufallsreihe muss mindestens der Länge der zu verschlüsselnden Nachricht entsprechen, da periodische Wiederholungen eines im Verhältnis zum Klartext typischerweise kurzen Schlüssels die Kryptoanalyse und damit einen Angriff auf die Übertragungsstrecke ermöglichen würde. Außerdem darf der Schlüssel nur ein einziges Mal verwendet werden, sodass für die sichere Schlüsselverteilung ein extrem hoher Aufwand erforderlich ist. Für RFID-Systeme ist eine Stromverschlüsselung in dieser Form jedoch völlig unpraktikabel.

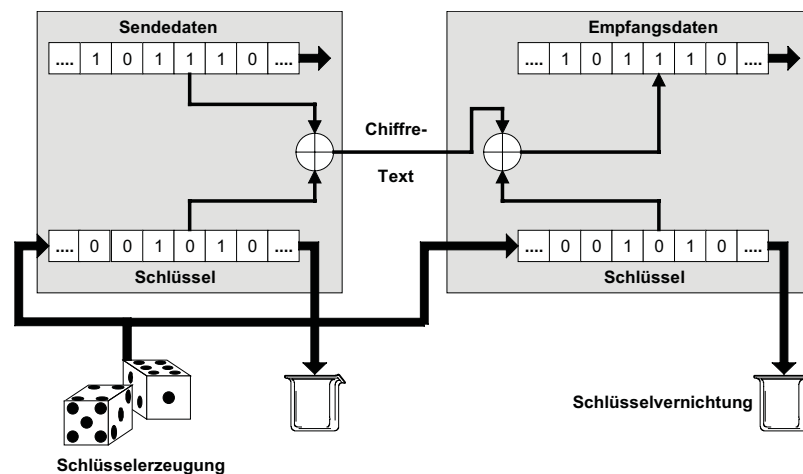


Abb. 8.17 Beim „one-time-pad“ wird der aus Zufallszahlen (Würfel) erzeugte Schlüssel nur ein einziges Mal verwendet und anschließend vernichtet (Papierkorb). Ein Problem stellt hierbei die sichere Übertragung des Schlüssels zwischen Sender und Empfänger dar.

Um die Probleme der Schlüsselerzeugung und Schlüsselverteilung zu vermeiden, werden nach dem Vorbild des „one-time-pad“ Stromchiffren konstruiert, die statt einer wirklichen Zufallsreihe so genannte *Pseudozufallsfolgen* verwenden. Zur Erzeugung von Pseudozufallsfolgen werden so genannte Pseudozufallsgeneratoren (pseudo-random-generator) verwendet.

Abbildung 8.18 zeigt das Grundprinzip einer sequentiellen Chiffre mit Pseudozufallsgeneratoren: Damit sich die Verschlüsselungsfunktion einer sequentiellen Chiffre mit jedem Zeichen (zufällig) ändern kann, muss die Funktion außer von dem augenblicklichen Eingabezeichen auch noch von einem weiteren Merkmal, dem inneren Zustand M abhängen. Dieser innere Zustand M wird nach jedem Verschlüsselungsschritt durch die Zustandsüberföhrungsfunktion $g(K)$ verändert. Der Pseudozufallsgenerator wird aus den Komponenten M und $g(K)$ gebildet. Die Sicherheit der Chiffre hängt im Wesentlichen von der Anzahl der inneren Zustände M und der Komplexität der Überföhrungsfunktion $g(K)$ statt. Das Studium

sequentieller Chiffren besteht somit zur Hauptsache aus der Untersuchung von Pseudozufalls-generatoren.

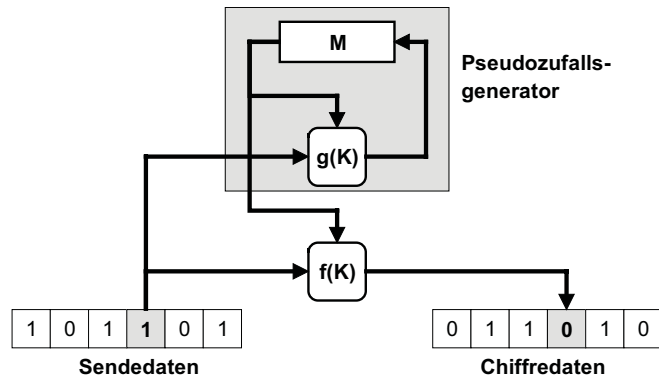


Abb. 8.18 Prinzip der Erzeugung eines sicheren Schlüssels durch einen Pseudozufalls-generator.

Die *Verschlüsselungsfunktion* $f(K)$ selbst ist dagegen in der Regel sehr einfach und kann auch nur aus einer Addition oder XOR-Verknüpfung bestehen [fumy] [glogau].

Schaltungstechnisch werden Pseudozufalls-generatoren durch Zustandsautomaten (state-machine) realisiert. Diese bestehen aus binären Speicherzellen, so genannten Flip-Flops. Verfügt ein Zustandsautomat über n Speicherzellen, so kann er 2^n verschiedene innere Zustände M annehmen. Die Zustandsüberföhrungsfunktion $g(K)$ wird durch Boolesche Schaltwerke (combinatorial logic; Coder) dargestellt (eine tiefere Erklärung der Funktionsweise von Zustandsautomaten ist im Kap. 10.1.2.1 „State-Machine“, S. 323 zu finden). Eine wesentliche Vereinfachung bei der Implementierung und Entwicklung von Pseudozufalls-generatoren ergibt sich durch die Beschränkung auf rückgekoppelte Schieberegister.

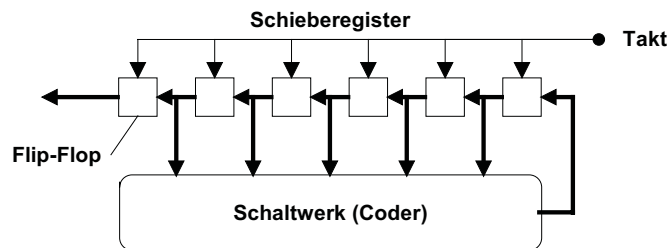


Abb. 8.19 Grundschaltung eines Pseudozufalls-generators aus einer Anordnung rückgekoppelter Schieberegister.

Ein Schieberegister entsteht aus der Reihenschaltung von Flip-Flops (Ausgang $_n$ wird mit Eingang $_{n+1}$ verbunden) und Parallelschaltung aller Takteingänge. Bei jedem Takt wird der Inhalt der Flip-Flop-Zellen um eine Stelle weitergeschoben. Der Inhalt des letzten Flip-Flop wird ausgegeben [rueffel] [golomb].