RFID-Sicherheit – Theorie und Praxis

Gerhard Klostermeier, Hochschule für Technik und Wirtschaft, Aalen

***Zusammenfassung*—Eine Ausarbeitung über RFID-Sicherheit mit Fokus auf Theorie und Praxis. Besonders beleuchtet werden dabei viele verschiedene logische, aber auch physikalische Angriffsmethoden und mögliche Gegenmaßnahmen.**

Keywords*—RFID, Sicherheit, Kryptographie, Angriffe, Gegenmaßnahmen

I. Einleitung

RFID (*Radio-frequency identification*) ist eine auf Radiowellen basierende Technik zur Identifikation von Objekten, die eine rasante Entwicklung durchmacht. Ihr Beginn reicht zurück bis in den Zweiten Weltkrieg, wo sie als Freund-Feind-Erkennung (engl. *identification friend or foe*, IFF) für Flugzeuge verwendet wurde. Der erste mit den heutigen RFID-Systemen vergleichbare Transponder wurde erst Jahre später, am 23. Januar 1973, von Mario Cardullo patentiert, welcher den passiven 16 Bit RFID-Tag zwei Jahre zuvor als Maut-Kontrollgerät potenziellen Käufern vorstellte. Der Name Radio-frequency identification ist jedoch auf Charles Walton zurückzuführen, der 1983 ein Patent mit dem Titel „Portable radio frequency emitting identifier“ einreichte. [1, vgl.][2, vgl.]

In den letzten Jahren wurden RFID-Tags immer billiger was dazu führte, dass sie an vielen Stellen (z.B. Lagersysteme) den Barcode ablösten. Aber auch die teureren, technisch komplexeren Transponder haben viele Anwendungsgebiete erobert, aus denen sie heute nicht mehr wegzudenken sind. Moderne Ausweise, Geldkarten, Zugangskontrollen und viele weitere Systeme nutzen RFID mit dem Ziel Funktionalität, Komfort und möglichst auch die Sicherheit zu erhöhen. [3, vgl.]

Der technische Aufbau eines Tags ist fast immer der gleiche: eine Antenne, welche mit einem Transponder-Chip verbunden ist. Die Antenne dient zur Kommunikation mit dem Lesegerät (RFID-Reader, auch *Proximity Coupling Device*, PCD) und induziert Strom aus dem elektromagnetischen Feld des RFID-Readers, mit dem der Chip betrieben wird. Der Chip beinhaltet alle Elemente, welche für einen RFID-Tag relevant sind: Modulator, Demodulator, Speicherverwaltung, Informationsverarbeitung, etc. [3, vgl.]

A. Transpondertypen

Im Wesentlichen werden zwei Transpondertypen unterschieden: *passive* und *aktive*.[4] Passive Tags besitzen keine zusätzliche Stromquelle, während aktive die Versorgung des Chips mit einer Batterie realisieren.

Andere Autoren sprechen von drei Typen, da sie sogenannte *short range radio devices* als aktiv bezeichnen. Transponder die ihren Chip mit einer Batterie betreiben werden, dann *semi-passiv* genannt (siehe Abbildung 1). [3]

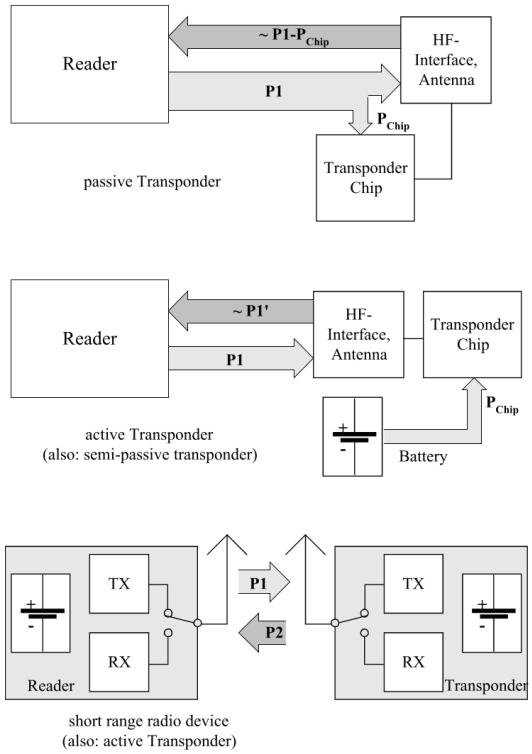

Abbildung 1. Transpondertypen [4]

B. Sicherheitseinbußen durch Kompromisse

Wie in vielen Gebieten der IT-Welt kämpft auch RFID mit Kürzungen beim Thema Sicherheit durch typische „Tradeoff“-Probleme. Größter Gegner sind dabei die Kosten aber auch Energieversorgung, Speichergröße und Bandbreitenengpässe machen es nicht leicht RFID mit „guter“ Kryptographie zu versehen. Besonders im “Low-end“ Bereich von RFID-Tags (z.B. *Smart Labes*, auch *Smart Tags*) ist es kaum möglich Kryptographie umzusetzen, was jedoch nicht an der Technik liegt, sondern lediglich daran, dass das Hauptkriterium in diesem Umfeld die Kosten sind. [3, vgl.]

II. RFID-Sicherheitstheorie

Die Theorie um die Sicherheit von RFID-Systemen ist geprägt von verschiedenen Ansätzen und Definitionen. Da RFID ein Sammelbegriff und keineswegs ein Standard ist, haben verschiedene Forscher, Kryptographen und Firmen eigene Vorstellungen davon, was für Sie Sicherheit im Bezug auf RFID-Systeme bedeutet.

A. Schutzziele

Für RFID-Tags, vor allem für sogenannte *kontaktlose Smartcards*, sind im Wesentlichen drei Schutzziele von besonderer Bedeutung:

- die Geheimhaltung von Daten,
- der Schutz vor unerlaubter Datenmanipulation
- und dem besonders für RFID-Anwendungen interessanten Schutzziel der Privatsphäre.

Nicht alle dieser Ziele sind für jede Anwendung einzuhalten. Für Tags die beispielsweise zur Warenidentifikation genutzt werden, ist es unnötig oder gar hinderlich die Privatsphäre zu schützen.[5, vgl.]

B. Definition von RFID-Sicherheit

Die folgenden Definitionen zielen hauptsächlich auf RFID-Tags ab, die mit *Lightweight-Kryptographie* auskommen müssen. Kontaktlose Smartcards, welche im Allgemeinen höhere Sicherheitsanforderungen haben, versuchen alle drei Schutzziele (siehe Abschnitt II-A) zu decken und bedienen sich dazu weiterer Sicherheitsmechanismen (siehe Abschnitt III-A und III-Q).

- *Definition nach Serge Vaudenay:* Einem Vorschlag von Serge Vaudenay zufolge ist ein RFID-System dann sicher, wenn es einem Angreifer nicht gelingen kann Rückschlüsse auf Informationen zu ziehen, obwohl dieser alle Interaktionen im System sehen kann. Des Weiteren muss ein Identitätsdiebstahl durch den Angreifer ausgeschlossen werden können. [3, vgl.][6]
- *Definition nach Robert H. Deng et al.:* Robert H. Deng und seine Kollegen Yingjiu Li, Moti Yung und Yunlei Zhao definieren ein RFID-Protokoll als sicher, unter der Voraussetzung dass alle Interaktionen mit dem Transponder „zero-knowledge“ sind. [3, vgl.][7]

C. RFID und Kryptographie

Ein naheliegender Gedanke für RFID ist, bekannte und bewährte Kryptographie einzusetzen. Bei „modernen“, komplexeren, kontaktlosen Smartcards ist dies durchaus auch der Fall (siehe Abschnitt III-A). Jedoch bedarf es bei günstigen Low-end RFID-Tags neuer Lösungen, die unter dem Titel *Lightweight-* oder *Ultra-Lightweight-Kryptographie* zusammengefasst werden. Die Bezeichnung „Lightweight“ soll keinesfalls vermitteln, dass es sich um „schlechte“ Kryptographie handelt, sondern um Kryptographie die angemessen ist für Low-end RFID-Tags.

Um Verfahren zu finden die für Lightweight-Kryptographie passend sind, werden viele Lösungsansätze parallel verfolgt:

- Effektive Implementierung bewährter kryptographischer Verfahren
- Einsatz bewährter Kryptographie mit kürzeren Parametern
- Entwicklung neuer Kryptographieverfahren
- Entwicklung von Kryptographieverfahren, die speziell die Probleme von Lightweight-Kryptographie für RFID angehen

[3, vgl.]

D. Lösungsansätze für RFID-Kryptographie

In den letzten Jahren wurde vermehrt auf Kryptographie gesetzt deren Grundlage ein Problem ist, von dem nicht die NP-Vollständigkeit bewiesen ist (z.B. Faktorisierung oder diskreter Logarithmus). Ursache dafür war, dass die große Mehrheit der Kryptosysteme die auf NP-vollständigen Problemen basieren, gebrochen wurden.

Rund um RFID-Kryptographie und besonders um Lightweight-Kryptographie entstand eine Vielzahl von neuen und optimierten Kryptosystemen. Beispiele sind DESL (*Data Encryption Standard - Lightweight*) und DESXL (*Data Encryption Standard - Extra Lightweight*), die im Wesentlichen mit weniger Durchgängen und einfacherer Blockbildung arbeiten als der etablierte DES-Algorithmus. Ein weiteres vielversprechendes Verfahren ist NTRU (*nth-degree truncated polynomial ring*)[9], welches ein asymmetrisches, auf mathematischen Gittern (Gruppentheorie) basierendes Kryptosystem ist.

Ebenfalls interessant ist, dass auch wieder auf Algorithmen gesetzt wird, deren Grundlage ein NP-vollständiges Problem ist. Lösungsansätze wie z.B. die HB-Protokollfamilie nutzen das LPN-Problem (*Learning Parity with Noise*).

Bei weitem nicht alle der Kryptographieverfahren konnten sich durchsetzten. Algorithmen wie *Hight*, *Clefia*, *Squash*, *Katan* und *LED* eigneten sich für die Praxis nicht. Weitere Verfahren die für die Praxis erprobt wurden, sind in der Vergleichstabelle I zu finden. [3, vgl.]

E. Gate Equivalents

Eine Möglichkeit die Hardware-Größe von kryptographischen Algorithmen zu messen, sind sogenannte *Gate Equivalents* (GEs). In der heutigen CMOS-Technologie beansprucht ein GE die Fläche eines NAND-Gatters mit zwei Eingängen und einem Ausgang.

Chips von Low-end RFID-Tags sind typischerweise beschränkt auf 10.000 GEs, wovon 2.000 GEs für Sicherheitsmechanismen genutzt werden und die verbleibenden 8.000 GEs für Signalverarbeitung und Speicher.

Den ersten Ansatz verfolgend, bewährte Kryptographie effektiv zu implementieren (siehe Abschnitt II-C), gelang es Kryptographen eine seriell arbeitende Version des DES-Algorithmus zu entwickeln, welcher eine Fläche von 2.310 GEs benötigt und mit 144 Taktzyklen einen Klartext verschlüsseln kann. Ein weiteres Beispiel ist eine Version von AES (*Advanced Encryption Standard*), welche in einer Architektur die nur das Verschlüsseln von Daten ermöglicht, 3.100 GEs an Fläche beansprucht. [3, vlg.]

III. RFID-Sicherheit in der Praxis

In der Praxis ist RFID-Sicherheit stark anwendungsabhängig. Tags die ausschließlich zur Waren Identifikation genutzt werden, besitzen meistens keine Sicherheitsmechanismen. RFID-Chips, wie sie beispielsweise in Skipässen zum Einsatz kommen, bieten Möglichkeiten etwas Sicherheit zu gewährleisten, die jedoch darunter leiden, dass diese Tags in hoher Stückzahl und so günstig wie möglich produziert

Tabelle I. VERGLEICH VON LIGHTWEIGHT-KRYPTOSYSTEMEN [8]

Cipher	Key Size (Bit)	Block Size (Bit)	Area (GE)	Power Consumption (µW)	Throughput @100kHz (KBit/s)	Tech. (µm)	Level of Security
Benchmark cipher							
AES-optimized	128	128	3400	4.5 @100kHz	12.4	0.35	Very High
Symmetric Key Primitives: Block Ciphers							
TEA	128	64	1984	39 @230kHz	22	0.35	Low
SEA (93 rounds)	96	96	1333	3.22 @100kHz	16	0.13	Low-Moderate
DESL	56	64	1848	1.6 @100kHz	44.44	0.18	Low-Moderate
DES	56	64	2309	2.14 @100kHz	44.44	0.18	Low
DESXL	184	64	2168	N/A	44.44	0.18	Moderate-High
mCRYPTON-64 (13 rounds)	64	64	2420	N/A	492	0.13	High
PRESENT-80 (4 Bits)	80	64	1650	3.86 @100kHz	200	0.18	High
KTANTAN-32	80	32	464	0.15 @100kHz	12.5	0.13	Low
PRINTcipher-48	80	48	402	2.6 @100kHz	6.25	0.18	Moderate-High
Symmetric Key Primitives: Stream Ciphers							
GRAIN (16 Bit word size)	80	-	3360 (Low power), 1294 (Min area)	1.2 @100kHz (Low power), 3.3 @100kHz (Min area)	123 (Low power), 100 (Min area)	0.35 (Low Power), 0.13 (Min area)	Moderate-High (High Risk)
TRIVIUM (16 Bit word size)	80	-	3090 (Low power), 2599 (Min area)	1.02 @100kHz (Low power), 5.6 @100kHz (Min area)	72 (Low power), 100 (Min area)	0.35 (Low Power), 0.13 (Min area)	Moderate-High (High Risk)
A2U2	56 + 5	-	226	0.135 @100kHz	50	0.13	Low
Physical Primitives: Physical One Way Functions							
PUF-64 (Using 128 CRPs)	-	$128 \cdot 0.4 = 52$ Bits	856	N/A	2.048	0.18	Low-Moderate
PUF+LFSR-64	-	$128 \cdot 0.4 = 52$ Bits	2392	N/A	15.488	0.18	Low-Moderate

werden. Als Letztes bleiben noch Anwendungen in denen die Sicherheit des RFID-Tags maßgeblich ist. Typische Beispiele für solche Modelle sind Zugangskontrollen oder Bezahlsysteme. Hier darf die Produktion eines Tags mehr kosten, was es möglich macht bekannte und bewährte Kryptographieverfahren wie AES oder 3DES zu implementieren.

Durch die hohen Kosten sind die Gegenmaßnahmen der folgenden Abschnitte oft nur in Tags der letzten Kategorie zu finden.

In der Praxis wird versucht die Schutzziele (siehe Abschnitt II-A) so methodisch wie möglich umzusetzen. Ein Beispiel bietet die Tabelle II.

Tabelle II. SCHUTZZIELE, BEDROHUNGEN, SCHUTZMECHANISMEN [5]

		Beispiel
Was ist zu schützen?	Schutzziel	Geheimhaltung
Was kann alles passieren?	Bedrohung	Verlust der Geheimhaltung
Mit welchem Mechanismus kann die Bedrohung abgewandt werden?	Schutzmechanismus	Verschlüsselung
Welches Verfahren soll angewandt werden?	Algorithmus	AES

A. *Logische Angriffe*

UNTER „logischen“ Angriffen sind Angriffsmethoden gesammelt, die keine physikalische Eigenschaft des RFID-Transponders oder des Lesegeräts ausnutzen.

B. *Unerlaubtes Auslesen*

Ein Angreifer kann mit einem Lesegerät einen RFID-Tag aktivieren und versuchen ihn auszulesen. Die Aktivierungsreichweite als physikalische Begrenzung macht es dem Angreifer im Normalfall schwieriger aber nicht unmöglich. Durch geschickte Antennen und passende RFID-Rreader-Hardware lassen sich für passive LF-Tags (*Low Frequency*, 120 kHz - 140 kHz) Reichweiten von bis zu einem Meter bewerkstelligen. Für HF-Transponder (*High Frequency*, 13,56 MHz) sind Reichweiten zwischen einem und drei Metern möglich. [10, vgl.]

Um vor unerlaubtem Auslesen geschützt zu sein, sollte sich das Lesegerät gegenüber dem RFID-Transponder authentifizieren und umgekehrt (*Mutual Authentication*). In der Praxis hat sich für kontaktlose Smartcards *3-Pass Mutual Authentication* als Authentifizierungsmethode durchgesetzt. [5, vgl.]
Die Abbildung 2 zeigt konkret wie im Falle der *Mifare Classic*-Technik von NXP eine Authentisierung abläuft. Hierbei ist zu beachten, dass nur die nonce (*number used only once*) des Tags im Klartext übertragen wird (Pass 1). [12]
Die Abbildung 3 zeigt wie einige andere Tags 3-Pass Mutual Authentication durchführen. Das typische Challenge-Response-System ist nicht mehr so leicht zu erkennen und gegenüber dem vorigen Verfahren (siehe Abbildung 2), wird hier

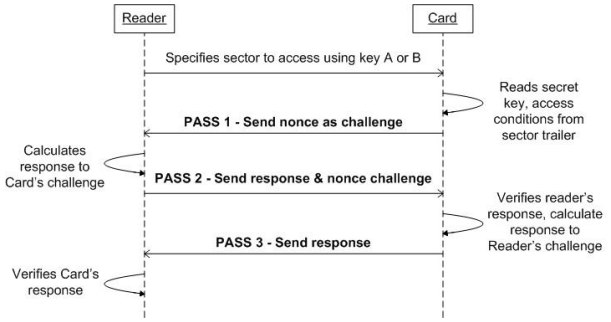

Abbildung 2. Challenge-Response basierte 3-Pass Mutual Authentication von Mifare Classic [11]

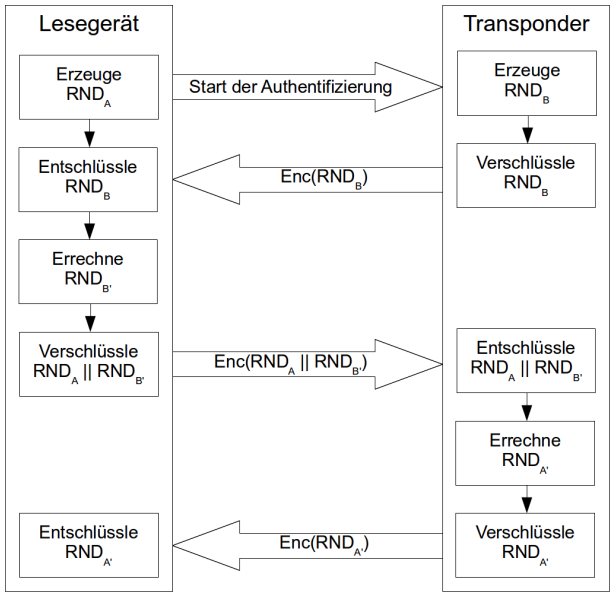

Abbildung 3. 3-Pass Mutual Authentication [5]

auch der erste Durchlauf verschlüsselt. Die dabei verwendeten Verschlüsselungsmethoden können sich je nach Transpondertyp oder Konfiguration des Tags unterscheiden.
Der genaue Ablauf ist dabei wie folgt:

- Das Lesegerät erstellt eine Zufallszahl RND_A und der RFID-Transponder eine Zufallszahl RND_B.
- Der Tag verschlüsselt RND_B und schickt die Challenge an den RFID-Reader (Pass 1).
- Das Lesegerät entschlüsselt RND_B mit dem gleichen Schlüssel (symmetrische Kryptographie), mit dem es zuvor der RFID-Tag verschlüsselt hat.
- Nun erzeugt das Lesegerät $RND_{B'}$ mit Hilfe einer beider Seiten bekannten Rechenvorschrift (z.B. eine einfache Byte-Rotation).
- RND_A und $RND_{B'}$ werden mit dem gemeinsamen, geheimen Schlüssel verschlüsselt und an den Transponder übertragen (Pass 2).
- Nach der Entschlüsselung des Paars rechnet der Tag $RND_{B'}$ zu RND_B zurück und vergleicht dies mit dem ursprünglich von ihm generierten RND_B. Gleichen sich diese nicht, so bricht der Transponder den Authentifizierungsvorgang ab.
- Falls RND_B korrekt war, errechnet der RFID-Tag aus RND_A unter Zuhilfenahme der selben Rechenoperation wie auch schon zuvor $RND_{A'}$.
- Der Transponder verschlüsselt $RND_{A'}$ und sendet es an den RFID-Reader (Pass 3).
- Auch das Lesegerät ist, nach dem Entschlüsseln der Nachricht und dem Zurückrechnen von $RND_{A'}$ zu RND_A, in der Lage zu überprüfen, ob der RFID-Tag die Authentifizierungskriterien erfüllt.

[5, vgl.]

C. Lauschangriff (Eavesdropping)

Durch Authentifizierung kann sichergestellt werden, dass ein Angreifer nicht aktiv einen Tag ausliest, aber ein passives Mitlauschen einer Kommunikation kann dadurch nicht verhindert werden.

Um dieses Problem zu lösen wird die Funkstrecke zwischen Smartcards und Lesegerät verschlüsselt. Die dafür eingesetzten Verschlüsselungsverfahren sind oftmals proprietär, wobei sich in den letzten Jahren vermehrt offene Verfahren wie DES, 3DES und AES durchsetzten konnten. Die konkrete Implementierung in Hardware bleibt allerdings immer noch unter Verschluss (siehe Abschnitt III-J).

Ein Grund warum Hersteller wie NXP möglicherweise inzwischen fast ausschließlich Smartcards mit DES, 3DES oder AES anbieten, ist vermutlich auch der *Mifare Classic-Hack*. Die Mifare Classic-Technik, die mit der proprietären Stromchiffre „CRYPTO-1“ verschlüsselt, wurde 2007 von einem Forscherteam um Karsten Nohl und Henryk Plötz „reverse-engineert“ (siehe Abschnitt III-J).[13] Dabei wurden signifikante Sicherheitsprobleme im Verschlüsselungsalgorithmus gefunden, sowie Schwachstellen im Pseudo–Zufallszahlengenerator die dazu führten, dass in den folgenden Jahren eine Vielzahl von Angriffen für diese Schwachstellen perfektioniert und veröffentlicht wurden.

Grundproblem war vermutlich, dass *Kerckhoffs-Prinzip* nicht eingehalten wurde, welches in etwa besagt, dass der Verschlüsselungsalgorithmus nicht geheim sein sollte, sondern nur der Schlüssel. Erfahrene Kryptographen hätten beim Kontrollieren des Verfahrens vermutlich gleich vom Einsatz einer Stromchiffre abgeraten, da mit vertretbarem Aufwand kaum ein sicheres Schlüsselmanagement zu realisieren ist.

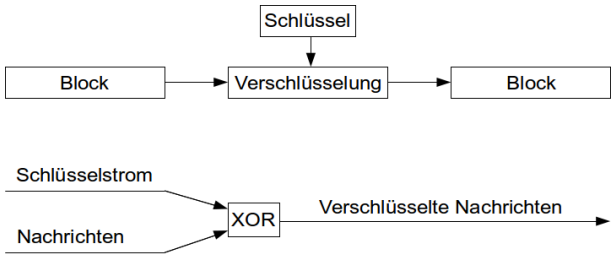

Abbildung 4. Block- und Stromchiffre [5]

Modernere Mifare-Produkte, aber auch die meisten anderen Smartcards, verwenden ausschließlich Blockchiffren. [5, vgl.]

Bei Blockchiffren ist der Operationsmodus ein wesentliches Merkmal, welches über mehr oder weniger Sicherheit entscheidet. Grundgesetzlich sind zwei Modi zu unterscheiden:

- *Electronic Codebook* (ECB)
- *Cipher Block Chaining* (CBC)

Bockchiffren (z.B. DES) im Electronic Codebook Modus haben ein entscheidendes Problem. Würde beispielsweise ein Bild in 8-Byte-Blöcke zerstückelt, welche anschließen verschlüsselt und danach wieder zusammengesetzt werden, so sind die Konturen des Bildes immer noch deutlich zu erkennen (siehe Abbildung 5). Das hat zur Folge, dass der ECB Modus bei Smartcards kaum verwendet wird.

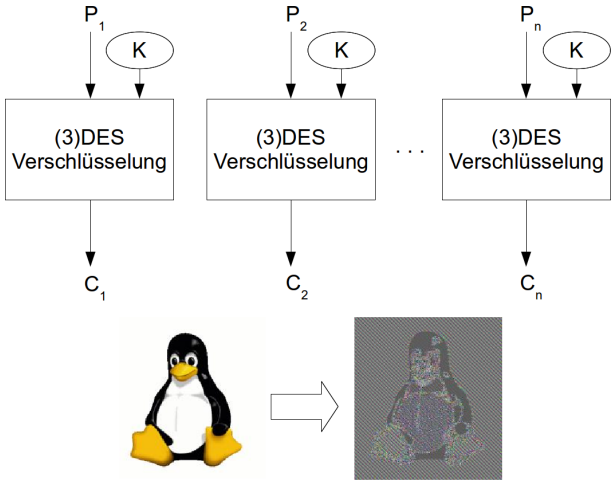

Abbildung 5. (3)DES Verschlüsselung im Electronic Codebook Modus [5, vgl. & Tux by Larry Ewing]

Der Cipher Block Chaining Modus löst die Probleme des ECB Modus, in dem jeder Folgeblock von seinem Vorgänger abhängig gemacht wird (siehe Abbildung 6). Für den Ersten Block ist dafür ein IV (*Initialization Vector*) nötig, welcher typischerweise den Wert „0“ hat.

D. Unerlaubte Manipulation

Eine unerlaubte Datenmanipulation kann schnell auftreten. Der Angreifer muss unter Umständen nicht einmal in der Lage sein die Daten zu interpretieren, wenn es ihm um eine Manipulation geht, die beispielsweise falsche Vorgänge oder Zustände hervorrufen sollen.

Um sicher zu gehen, dass es sich um eine legitime Kommunikation handelt, muss der rechtmäßige Empfänger drei Dinge ausmachen können:

- Die empfangene Nachricht kommt vom „echten“ Sender.
- Die empfangene Nachricht wurde nicht manipuliert.
- Die empfangene Nachricht ist keine Wiederholung einer alten, gültigen Nachricht, die bereits früher empfangen wurde.

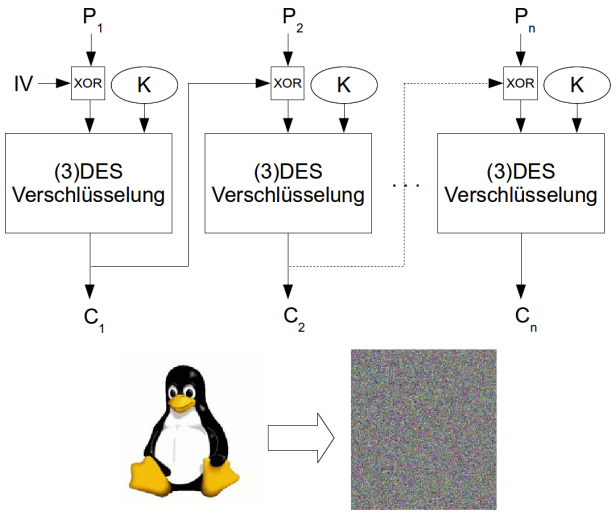

Abbildung 6. (3)DES Verschlüsselung im Cipher Block Chaining Modus [5, vgl. & Tux by Larry Ewing]

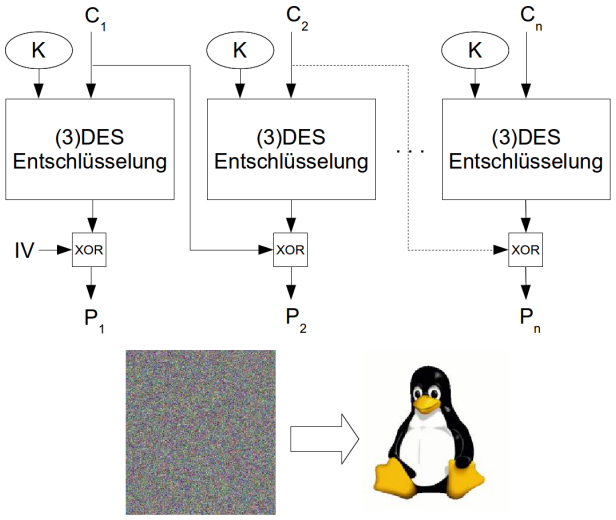

Abbildung 7. (3)DES Entschlüsselung im Cipher Block Chaining Modus [5, vgl. & Tux by Larry Ewing]

Der erste Punkt wird mit gegenseitiger Authentifizierung gelöst (siehe Abschnitt III-B). Der dritte Punkt kann mit Hilfe eines Session-Keys und eines Zählers realisiert werden (siehe Abschnitt III-E). Um die eigentliche Manipulation zu verhindern (zweiter Punkt), wird ein MAC (*Message Authentication Code*) verwendet. Im Prinzip ist ein MAC eine Prüfsumme die über jede Nachricht generiert und mit übertragen wird. Dabei spielt es keine Rolle, ob die Nachricht verschlüsselt oder unverschlüsselt ist, da lediglich die Datenintegrität gewährleistet werden soll.

Ein Beispiel für ein MAC ist in Abbildung 8 dargestellt. Zur Erstellung der MAC wird die zu übertragende Nachricht $(P_1, P_2, ..., P_n)$ mit (3)DES im CBC Modus verschlüsselt. Der letzte Block (C_n) wird an die Nachricht angehängt und

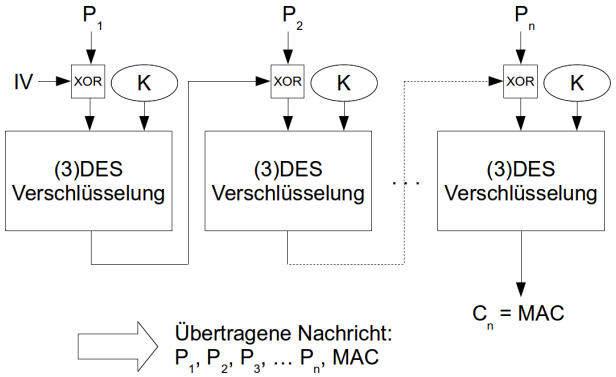

Abbildung 8. MAC auf Basis von (3)DES [5, vgl.]

repräsentiert den MAC. Wie bereits erwähnt, müssen für die Übertragung $P_1, P_2, ..., P_n, MAC$ nicht verschlüsselt sein.

Dadurch, dass sich Sender und Empfänger ein gemeinsames Geheimnis teilen, dass als Schlüssel für den (3)DES-Algorithmus genutzt wird, muss auf Empfangsseite der selbe MAC herauskommen, wenn identisch vorgegangen wird. Hat ein Angreifer einen Teil der Nachricht P_x zu P_y verfälscht, ist der MAC nicht mehr gültig und müsste neu berechnet werden. Da dem Angreifer jedoch nicht der geheime Schlüssel bekannt ist, kann er dem Empfänger nicht vortäuschen, dass die Nachricht gültig wäre.

E. Reply-Angriff

Bei einem Reply-Angriff (auch Replay-Angriff) wiederholt der Angreifer bereits übertragene Nachrichten. Das Problem kann mit dem folgenden Szenario einfach verdeutlicht werden: Einem Angreifer gelingt es eine Kommunikation mit zuschneiden, die das Öffnen einer Tür zur Folge hat. Mit Hilfe eines geeigneten Geräts kann er die Nachrichten des Transponders für den RFID-Reader exakt wiederholen, ohne sie verstehen zu müssen. Das Lesegerät wird die Tür für den Angreifer aufsperren, da es nicht merken kann, dass es sich nicht um einen echten Tag handelt.

Um sich vor diesen Angriffen zu schützen werden zwei Mechanismen eingesetzt. Als Erstes wird aus den Zufallszahlen die bei der Authentifizierung ausgetauscht wurden (siehe Abschnitt III-B, Abbildung 3), ein *Session Key* generiert. Wenn mit diesem die Kommunikation verschlüsselt wird, kann ein Angreifer die Nachrichten nicht vorhersagen oder in einer anderen *Session* wiederholen.

Zweiter Mechanismus welcher verhindert, dass innerhalb der selben Session zwei identische Nachrichten den gleichen MAC haben, ist ein Zähler, der von beiden Seiten für jede Übertragung hochgezählt wird. Aus seinem Wert wird der Initialisierungsvektor (IV) abgeleitet, der für die Generierung des MACs im CBC Modus nötig ist (siehe Abbildung 8). [5, vgl.]

F. Relay-Angriff

Bei einem Relay-Angriff täuscht der Angreifer das physikalische Vorhandensein des Transponders über eine große Entfernung vor, indem er die Nachrichten auf einem anderen Kommunikationskanal weiterreicht.

Für ein realistisches Szenario sind typischerweise zwei Angreifer und spezielle Hardware nötig. Angreifer 2 aktiviert mit einem Lesegerät die Karte des Opfers, ohne dass dieser es merkt. Der modifizierte RFID-Reader hält, z.B. über Funk, eine Verbindung zu dem Gerät des Angreifers 1. Dieser befindet sich direkt beim Lesegerät und täuscht dem Reader ein RFID-Tag vor, welcher die Daten jedoch aus der Verbindung zu Angreifer 2 bezieht. Da die Karte des Opfers berechtigt ist, beispielsweise eine Tür zu öffnen, wird sich diese aufsperren auch wenn der gültige Transponder Kilometer entfernt ist. Abbildung 9 verdeutlicht den Aufbau dieses Angriffes. [5, vgl.]

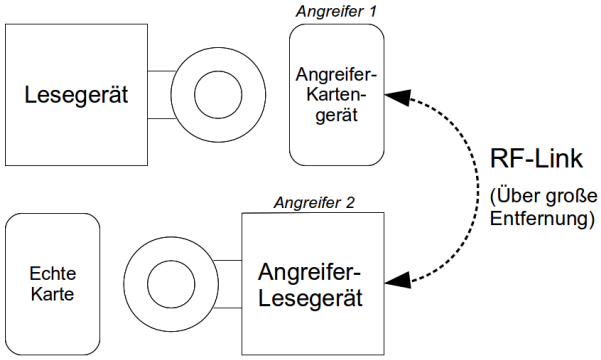

Abbildung 9. Relay-Angriff [5, vgl.]

Dass es sich nur um einen rein theoretischen Angriff handelt bewies Gerhard Hancke bereits 2005.[14] Mit der raschen Entwicklung von Handys in Richtung Smartphones, gelang es 2011 einem Team um Lishoy Francis und Gerhard Hancke einen Relay-Angriff mit Mobiltelefonen durchzuführen.[15] Diese Telefone besitzen NFC-Hardware (*Near Field Communication*) welche kompatibel zu vielen RFID-Anwendungen ist. Besonderheit ist, dass einige NFC-fähige Smartphones auch in der Lage sind einen RFID-Transponder zu emulieren. [16]

Gegen Relay-Angriffe gibt es nur wenig Schutz. Momentan bietet die Mifare Plus-Technik von NXP eine Kommandofolge an, mit der ein solcher Angriff möglicherweise erkannt und abgewehrt werden kann. Dazu müssen Transponder und Lesegerät die Kommandofolge zum einen schnell und zum anderen verschlüsselt abarbeiten, damit sich keine Möglichkeit bietet eine Manipulation durch zu führen. Wenn es zu Verzögerungen im Ablauf kommt, ist es wahrscheinlich, dass das System einer Relay-Attacke ausgesetzt ist.[5, vgl.]

G. Denail of Service-Angriff durch Blocker Tags

Damit ein RFID-Reader einen von mehreren Transpondern im seinem Lesefeld dediziert ansprechen kann, kommt ein Antikollisionsalgorithmus zum Einsatz. Dieser Mechanismus verhindert auch, dass ein Leser blockiert ist, wenn mehr als ein Tag in seiner Reichweite liegt.

In der Praxis haben sich zwei Antikollisionsalgorithmen durchgesetzt: der *Binary-Search-Tree-Algorithmus* und das

Slotted-ALOHA-Verfahren. Ein Blocker Tag macht sich Eingenschaften der beiden Verfahren zu Nutze, die einen RFID-Reader sehr lange beschäftigen oder sogar das Erkennen eines weiteren Tags unmöglich machen.

Um beispielsweise ein Lesegerät, dass den Binary-Search-Tree-Algorithmus nutzt lahm zu legen, wird von dem Blocker Tag für jede Bitstelle der Seriennummer (auch *Unique Identifier*, UID) eine „0“ und eine „1“ gleichzeitig ausgesandt. Dem rekursiven Algorithmus bleibt durch diese Kollisionen nichts anderes übrig, als den kompletten Binärbaum zu durchlaufen.

Angenommen die Zeit zur Ermittlung einer einzigen Seriennummer sei t_1, so bemisst sich der Durchlauf durch den Baum als $t_g = t_1 \cdot 2^n$, wobei n die Länge der Seriennummern in Bit ist. Wenn von einer Zeit $t_1 = 1ms$ und einer typischen Seriennummernlänge von $48Bit$ ausgegangen wird, so beträgt $t_g = 2,8 \cdot 10^{11}$ Sekunden. Das sind 8925 Jahre![4, vgl.]

H. Physikalische Angriffe

DIE folgenden physikalischen Angriffe haben oft wenig mit der RFID-Technik an sich zu tun. Transponder und Lesegeräte die sicher sein sollen, haben jedoch die selben Probleme wie andere sicherheitskritische Hardware auch.

I. Seitenkanalangriff: Power Analysis

Bei einem Seitenkanalangriff werden Systemkomponenten bei ihrer Arbeit beobachtet, um Korrelationen zwischen dem was ermittelt wurde und dem was im Inneren passiert herzustellen.

Ein verdeutlichendes Beispiel: Ein Safeknacker möchte einen klassischen, mechanischen Safe öffnen. Er nutzt den Seiteneffekt des Schlosses aus, welches beim bedienen leise „klick“-Geräusche macht, indem er mit einem Stethoskop den Safe abhört. Durch die „klick“-Geräusche kann er Rückschlüsse auf die richtige Zahlenkombination ziehen.

Als weiteres beliebtes Beispiel dient oft die „Differential Pizza Analysis“. Ein Reporter zählt die Pizzen, die jeden Abend ins Pentagon geliefert werden. Diese Zahl ist über einen relativ großen Zeitraum konstant. Wenn sich dann die Anzahl eines Abends stark erhöht, kann der Reporter den Rückschluss ziehen, dass eine größere geheime Operation geplant wird, da viele Mitarbeiter Überstunden machen.

Bei Smartcards ist der übliche Seitenkanal die Messung des Stromverbrauchs. Dadurch kann beispielsweise feststellt werden, wann der Krypto-Coprozessor startet, wann ein Speicherbereich aktiviert wird, oder sogar ob Nullen oder Einsen aus den einzelnen EEPROM-Zellen geladen werden. Im einfachsten Fall könnte so direkt der geheime Schlüssel ausgelesen werden, wenn bekannt ist, wann dieser geladen wird. Diese Angriffe werden SPA (*Simple Power Analysis*) oder DPA (*Differential Power Analysis*) genannt.

In der Praxis sind solche Angriffe nicht so einfach. Allein für die Messung des Stromverbrauchs einer Smartcard, muss ein Angreifer sich einen geschickten Messaufbau einfallen lassen. Auch haben moderne Transponder Mechanismen implementiert, die kritische Operationen im Stromverbrauch kaschieren. [5, vgl.]

J. Reverse Engineering

„Reverse Engineering bezeichnet das rückwärtige Herausfinden einer Schaltung aus dem fertigen Aufbau.“[5] In der Praxis bedeutet das den RFID-Transponder zu öffnen, die Module abzuschleifen und die Halbleiterschichten darin unter einem hochauflösenden Mikroskop zu analysieren (siehe Abbildung 10).

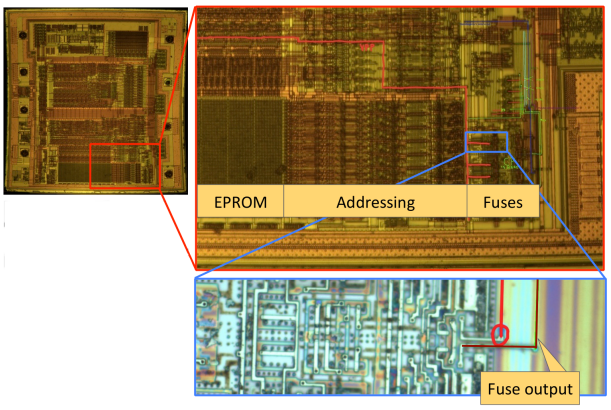

Abbildung 10. Reverse Engineering eines Chips (auf der Suche nach „Fuses“) [17]

Mit dieser Technik wurde um 2008 auch der Mifare Classic Chip von NXP untersucht. Laut Aussagen der Forscher war es nicht schwer Schwachstellen im Chip aufzudecken. Das liegt unter anderem daran, dass die Mifare Classic-Technik Mitte der 90er Jahre entworfen wurde. Die mittlerweile gut bekannte Methode des Reverse Engineerings wird bei modernen Chips schon in der Designphase mit berücksichtigt. Schutzmechanismen gegen das Öffnen der Chips bleiben jedoch, wie so oft, ein ständiger Wettlauf mit den Techniken der Angreifer. [5, vgl.]

K. Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- und Spannungsangriffe

All diese Angriffstechniken wurden in einem Abschnitt zusammengefasst, da sie immer das selbe Ziel haben: die Manipulation des internen Programmablaufs.

- *Microprobing:* Beim Microprobing werden am geöffneten Chip mit sehr feinen Nadeln Manipulationen und Messungen durchgeführt, um beispielsweise den kompletten internen Speicher direkt am Bus auszulesen. Um Angreifer davon abzubringen, wird die oberste Schicht häufig durch ein sehr feines Gitter geschützt (siehe Abbildung 12), welches, wenn es verletzt wird, den Chip abschaltet. Aber auch für Verteidigungsmaßnahmen wie das Gitter gibt es passende Angriffe wie z.B. FBI (*Focused Ion Beams*). [17]
- *Licht- und Laserangriffe:* Mit einfachem, optisch sichtbarem Licht, aber auch mit Laser oder Röntgenstrahlung lässt sich beispielsweise der Programmzähler eines geöffneten Chips beeinflussen (bei hoher Auflösung sogar einzelne Speicherzellen). Mit einem Angriff dieser

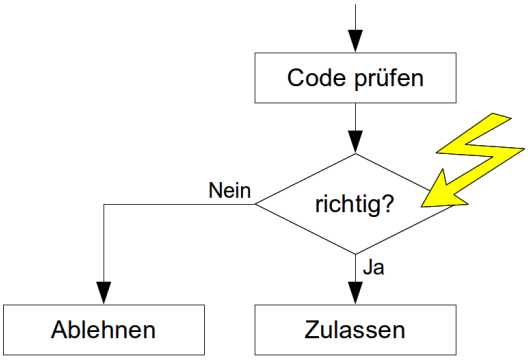

Abbildung 11. Manipulation des Programmablaufs durch Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- oder Spannungsangriffe [5, vgl.]

Art können z. B. Verzweigungen im Programm beeinflusst werden (siehe Abbildung 11).
Als Gegenmaßnahme kommen Lichtsensoren zum Einsatz. Diese können wie das Gitter gegen Microprobing aktiv eingreifen.

- *Temperatur-, Frequenz- und Spannungsangriffe:* Wenn bei einem Mikrocontroller Betriebsparameter wie Temperatur, Taktfrequenz oder Betriebsspannung verändert werden, können unkontrollierte Fehlfunktionen auftreten, die möglicherweise ein Angreifer ausnutzen kann. Aus diesem Grund haben moderne Smartcards Sensoren für die wichtigen Betriebsparameter. Wenn diese nicht im gewünschten Bereich liegen, kann sofort der Programmdurchlauf gestoppt werden.

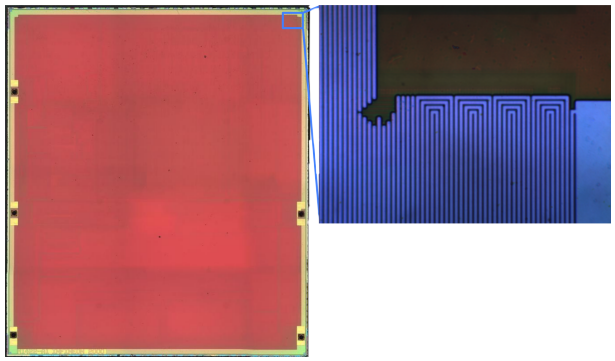

Abbildung 12. Schutzgitter in Chips gegen Microprobing [17]

L. Gegenmaßnahme: Secure Access Module

Als *Secure Access Module* (SAM) werden typischerweise Chips bezeichnet, deren Zweck es ist, Informationen sicher zu verwalten und zu verarbeiten. Dazu beinhalten sie möglichst viele Schutzmechanismen gegen physikalische Angriffe wie Power Analysis, Reverse Engineering, Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- und Spannungsangriffe.

Bei sicherheitskritischen RFID-Systemen ist die Smartcard selbst als SAM zu betrachten. Aber auch das „Backend"-System oder die Lesegeräte sollten über ein SAM verfügen, um Schlüssel sicher zu verwahren. In solchen Fällen kann das SAM auch eine sichere Software-Implementierung sein, was jedoch eine sichere Hardware-Umgebung voraussetzt. In der Praxis haben sich daher Kontakt-Smartcards (z.B. SIM-Karten) durchgesetzt. In vielen RFID-Lesegeräten für sichere Anwendungen ist ein Slot für SIM-Karten (oder andere Bauformen) vorhanden.

M. Störsender

Wie jede Funktechnik ist auch RFID von Störsendern betroffen. Da das Feld des Lesegeräts aus einem relativ starken Trägersignal besteht, ist es schwerer den „Downlink" (RFID-Reader zu Transponder) als den „Uplink" (Transponder zu RFID-Reader) zu stören. Jedoch ist beides mit relativ geringem technischen Aufwand möglich.

Einziges Hindernis, welches kriminelle Angreifer nicht aufhält ist, dass ein Störsender eine Funkanlage darstellt, deren Betrieb in den meisten Ländern illegal sein dürfte (zumindest ab einer gewissen Sendeleistung). [4, vgl.]

N. Dauerhaftes Zerstören

Dass Transponder dauerhaft zerstört werden können ist naheliegend. Allein durch physische Gewalt ist es einfach möglich einen Chip zu demolieren. Interessant wird es, wenn ein RFID-Tag zerstört werden soll, ohne äußerlich Spuren zu hinterlassen. Um das zu bewerkstelligen macht man sich die RFID-Technik passiver Transponder zu nutze, welche ihre Energie über die Antenne beziehen. Wenn ein Tag einem viel zu starken elektromagnetischen Feld ausgesetzt wird, induziert die Antenne so viel Energie das davon der Chip durchbrennt.

Ein Gerät zu bauen, dass ein für RFID-Tags zu starkes Feld aufbaut, ist mit einfachen „Hausmitteln" möglich. Das bewiesen zwei Studenten am 22ten Chaos Communication Congress (22C3), einer Konferenz des Chaos Computer Clubs (CCC).[18] Hierfür wurde die Elektronik einer Einwegkamera ausgebaut und anstatt der Blitzröhre eine Spule mit 4-5 Wickelungen angebracht. Wenn der mit ca. 300V geladene Kondensator sich über die Spule entlädt, wird dabei ein so starkes elektromagnetisches Feld erzeugt, dass in der Nähe befindliche RFID-Transponder zerstört werden können.

Die unter dem Namen *RFID-Zapper* bekannt gewordenen Geräte sind einfach selbst zu bauen. Es ist aber auch möglich, bereits fertige Geräte käuflich zu erwerben. [19, vgl.]

O. Weitere Sicherheitsmechanismen

In den folgenden Abschnitten werden weitere Sicherheitsmechanismen vorgestellt, die nicht eindeutig logischen Angriffen (siehe Abschnitt III-A) oder physikalischen Angriffen (siehe Abschnitt III-H) zuzuordnen sind.

P. Schlüsseldiversifizierung

Wenn der richtige Verschlüsselungsalgorithmus gewählt wurde, ist die Sicherheit abhängig von der Geheimhaltung der Schlüssel. Ein gutes Schlüsselmanagement ist daher entscheidend.

Bei vielen sicherheitskritischen RFID-Systemen (z.B. Zugangskontrolle), steckt einer der Gefahrenfaktoren in der symmetrischen Verschlüsselung und der Tatsache, dass häufig der selbe Schlüssel für alle Transponder verwendet wird. Gelingt es einem Angreifer den Schlüssel eines RFID-Tags zu „knacken“, ist nicht nur der eine Transponder kompromittiert, sondern gleich das ganze System.

Eine Lösung für dieses Problem ist die UID zur Schlüsseldiversifizierung zu verwenden. Die UID wird vom Hersteller vergeben und ist fest programmiert, d.h. kann nicht durch ein RFID-Reader geändert werden. (Ausnahmen sind Spezialtransponder die von anderen, nicht berechtigten Herstellern stammen und die Vorgabe der nur lesbaren UID ignorieren.[20]) Ein einfaches Beispiel wie eine solche Schlüsseldiversifizierung anhand der UID aussehen könnte zeigt Abbildung 13. [5, vgl.]

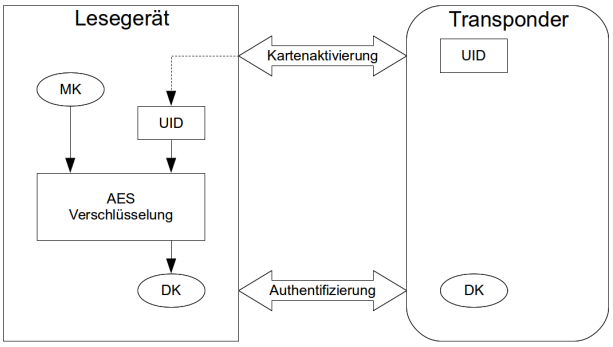

Abbildung 13. Beispiel für eine einfache Schlüsseldiversifizierung [5, vgl.]

Q. Random Identifier

Viel diskutiert wird seit einiger Zeit über das Thema Datenschutz im Zusammenhang mit RFID. Da die UID „öffentlich“ ist und von Jedermann ohne zusätzliche Berechtigungen ausgelesen werden kann, ist es möglich Rückschlüsse auf den Transponderbesitzer zu ziehen oder z.B. ein Bewegungsprofil zu erstellen.

Der Standard ISO/IEC 14443 beinhaltet die Option zunächst ein *Random Identifier* (RID) anstatt der UID zu verwenden, um den Datenschutzproblemen vorzubeugen.

Um dennoch Schlüsseldiversifizierung anhand der UID machen zu können (siehe Abschnitt III-P), muss es nach dem Selektieren (anhand der RID) möglich sein, die UID auszulesen. Diese muss natürlich verschlüsselt übertragen werden, damit nicht wieder der Datenschutz gefährdet wird.

Die Abbildung 14 zeigt wie eine Schlüsseldiversifizierung mit RID aussehen könnte. Um die UID zu erfragen wird eine Zufallszahl RND_Q an den Transponder gesandt. Diese ist mit dem nicht diversifizierten Schlüssel K verschlüsselt, den beide Seiten kennen müssen.

Der RFID-Tag entschlüsselt RND_Q und verwendet die Zufallszahl als Schlüssel für die Übertragung der UID. Der restliche Verlauf der Schlüsseldiversifizierung ist identisch mit dem im Abschnitt III-P.

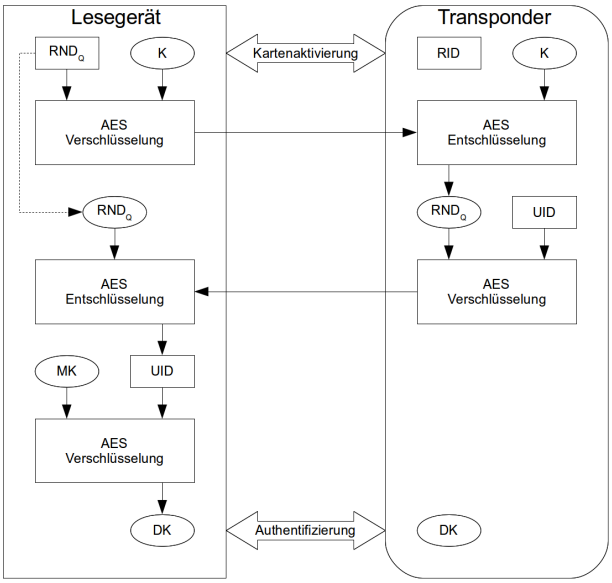

Abbildung 14. Beispiel für eine einfache Schlüsseldiversifizierung bei Verwendung von RID [5, vgl.]

IV. Fazit

WIE bei jedem anderen IT-System, so bleibt auch bei RFID die Sicherheit ein Ideal. Transponder und Lesegeräte zu schaffen die vor physikalischen und logischen Angriffen hundertprozentig Schutz bieten bleibt eine Utopie. Nichtsdestotrotz sollte versucht werden, die Technologie und vor allem die Kryptographie auszureizen. Dass dies nur in einem gewissen Rahmen stattfinden kann, ist durch den Preisdruck dem eine solche Technik ausgesetzt ist selbstverständlich.

REFERENZEN

[1] Wikipedia.org. (Aug. 2013). Radio-frequency identification, Adresse: https://en.wikipedia.org/w/index.php?title=Radio-frequency_identification&oldid=567861037.

[2] Bob Violino. (Apr. 2003). Genesis of the Versatile RFID Tag, Adresse: http://www.rfidjournal.com/articles/view?392/.

[3] Diana Maimut und Khaled Ouafi, "Lightweight Cryptography for RFID Tags", *IEEE Security & Privacy*, März 2012.

[4] Klaus Finkenzeller, *RFID-Handbuch - Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*, 6. aktualisierte und erweiterte Auflage. München: Hanser Fachbuchverlag, 2012, ISBN: 978-3-446-42992-5.

[5] Gerhard H. Schalk und Renke Bienert, *RFID - MIFARE und kontaktlose Smartcards angewandt*, 1. Aufl. Berlin: Elektor-Verlag, 2011, ISBN: 978-3-895-76219-2.

[6] Serge Vaudenay, "On privacy models for RFID", in *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, Ser. ASIACRYPT'07, Kuching, Malaysia: Springer-Verlag, 2007, S. 68–87, ISBN: 3-540-76899-8, 978-3-540-76899-9. Adresse: http://dl.acm.org/citation.cfm?id=1781454.1781461.

[7] Robert H. Deng und Yingjiu Li und Moti Yung und Yunlei Zhao, "A zero-knowledge based framework for RFID privacy", *Journal of Computer Security*, Bd. 19, Nr. 6, S. 1109–1146, 2011.

[8] Mathieu David. (Dez. 2011). Lightweight Cryptography for Passive RFID Tags, Adresse: http://vbn.aau.dk/files/61132753/Thesis_Mathieu_David.pdf.

[9] Wikipedia.org. (Aug. 2013). NTRU, Adresse: https://en.wikipedia.org/w/index.php?title=NTRU&oldid=543758650.

[10] Francis Brown. (Aug. 2013). RFID Hacking, Adresse: http://www.bishopfox.com/resources/tools/rfid-hacking/.

[11] Wee Hon Tan. (Sep. 2009). Practical Attacks on the MIFARE Classic, Adresse: http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf.

[12] Peter van Rossum. (Sep. 2008). Mifare Classic Troubles, Adresse: http://www.ict-forward.eu/media/workshop2/presentations/rossum-mifare.pdf.

[13] Henryk Plötz und Karsten Nohl. (Dez. 2007). Mifare – Little Security, Despite Obscurity, Adresse: http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html.

[14] Gerhard Hancke. (2005). A Practical Relay Attack on ISO 14443 Proximity Cards, Adresse: http://www.rfidblog.org.uk/hancke-rfidrelay.pdf.

[15] Lishoy Francis und Gerhard Hancke und Keith Mayes und Konstantinos Markantonakis. (Nov. 2011). Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones, Adresse: http://eprint.iacr.org/2011/618.

[16] Michael Roland. (Juni 2012). Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?, Adresse: http://www.medien.ifi.lmu.de/iwssi2012/papers/iwssi-spmu2012-roland.pdf.

[17] Philipp Maier und Karsten Nohl. (Dez. 2012). Low-Cost Chip Microprobing, Adresse: https://events.ccc.de/congress/2012/Fahrplan/events/5124.en.html.

[18] MiniMe und Mahajivana. (Jan. 2006). RFID-Zapper, Adresse: https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper%28EN%29_77f3.html.

[19] Jonathan Collins. (Jan. 2006). RFID-Zapper Shoots to Kill, Adresse: http://www.rfidjournal.com/articles/view?2098/.

[20] Proxmark Communitiy Forum. (Juli 2011). Changeable UID Mifare 1K (Mifare 1K cards Copy), Adresse: http://www.proxmark.org/forum/viewtopic.php?id=896&p=2.