RFID-Sicherheit

Theorie und Praxis

Gerhard Klostermeier

Hochschule für Technik und Wirtschaft Aalen

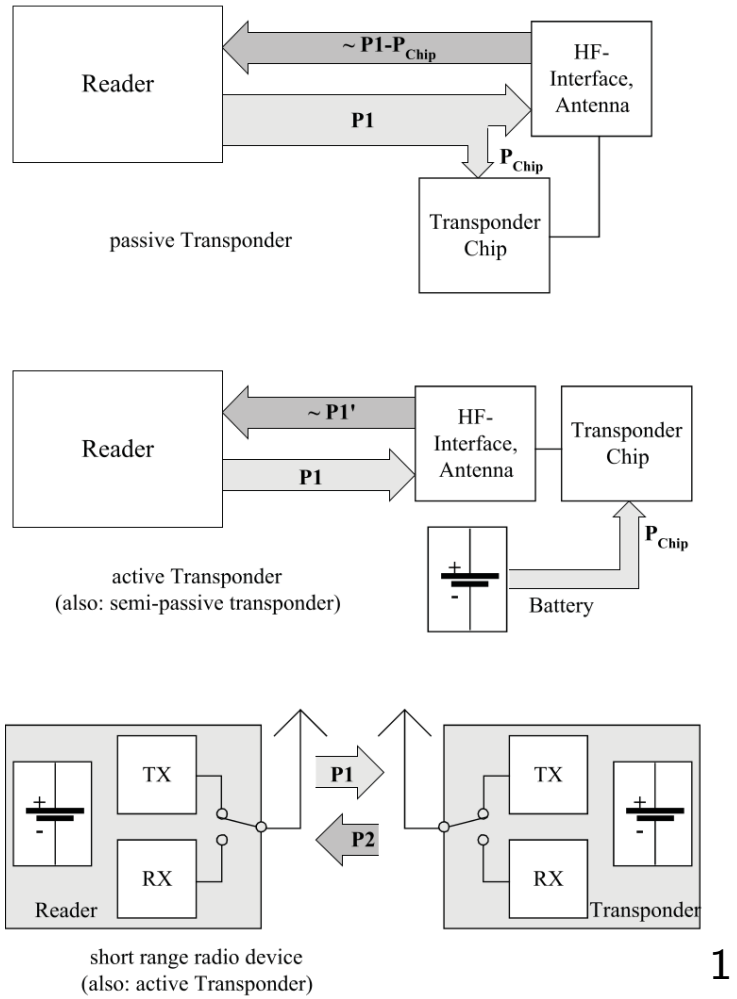
24. September 2013

Inhalt

- RFID: Radio-frequency identification
- Entstanden im Zweiten Weltkrieg
- 23. Januar 1973: Erster „moderner“ RFID-Transponder (von Mario Cardullo)
- Heute:
  - Günstige Tags ersetzten den Barcode (Warenidentifikation, Lagersysteme, etc.)
  - Komplexere Tags finden Anwendung in Ausweisen, Zugangskontrollen, etc.

Transpondertypen

Einleitung



[1]

[1] Quelle: Klaus Finkenzeller, RFID-Handbuch

Inhalt

Definition

Ein RFID-System ist 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. [a]

[a] Quelle: Serge Vaudenay, On privacy models for RFID

Definition

Ein RFID-Protokoll ist sicher unter der Voraussetzung, dass alle Interaktionen mit dem Transponder „zero-knowledge“ sind. [a]

[a] Quelle: Robert H. Deng et al., A zero-knowledge based framework for RFID privacy

Schutzziele

RFID-Sicherheitstheorie

Schutzziele:

- Geheimhaltung von Daten
- Schutz vor unerlaubter Datenmanipulation
- Schutz der Privatsphäre

Der Schutz der Privatsphäre fällt unterschiedlich aus:

- z.B. für Lagersysteme ist Privatsphäre hinderlich und unnötig
- z.B. für Personalausweise ist Privatsphäre unabdingbar

Problem

RFID-Kryptographie (besonders Lightweight-RFID-Kryptographie) muss billig, klein, schnell, energieeffizient und „bandbreitensparend“ sein.

Lösungsansätze:

- 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

Gate Equivalents (GE)

RFID-Sicherheitstheorie

- Größeneinheit für die Fläche von Hardware
- 1 GE entspricht der Fläche eines NAND-Gatters
- Low-end RFID-Chips haben typischerweise 10.000 GEs, davon stehen 2.000 GEs für Sicherheit zur Verfügung
- Beispiele: DES = 2309 GEs, AES = 3400 GEs

Vergelich von Lightweight-Kryptosystemen I

RFID-Sicherheitstheorie

Cipher	Key Size (Bit)	Block Size (Bit)	Area (GE)	Power Consumption (µW)	Throughput @100kHz (KBit/s)	Level of Security
Benchmark cipher						
AES-optimized	128	128	3400	4.5 @100kHz	12.4	Very High
Symmetric Key Primitives: Block Ciphers						
TEA	128	64	1984	39 @230kHz	22	Low
SEA (93 rounds)	96	96	1333	3.22 @100kHz	16	Low-Moderate
DESL	56	64	1848	1.6 @100kHz	44.44	Low-Moderate
DES	56	64	2309	2.14 @100kHz	44.44	Low
DESXL	184	64	2168	N/A	44.44	Moderate-High
mCRYPTON-64 (13 rounds)	64	64	2420	N/A	492	High
PRESENT-80 (4 Bits)	80	64	1650	3.86 @100kHz	200	High
KTANTAN-32	80	32	464	0.15 @100kHz	12.5	Low
PRINTcipher-48	80	48	402	2.6 @100kHz	6.25	Moderate-High

Vergelich von Lightweight-Kryptosystemen II

RFID-Sicherheitstheorie

Cipher	Key Size (Bit)	Block Size (Bit)	Area (GE)	Power Consumption (µW)	Throughput @100kHz (KBit/s)	Level of Security
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)	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)	Moderate-High (High Risk)
A2U2	56 + 5	-	226	0.135 @100kHz	50	Low
Physical Primitives: Physical One Way Functions						
PUF-64 (Using 128 CRPs)	-	$128 \cdot 0.4 = 52$ Bits	856	N/A	2.048	Low-Moderate
PUF+LFSR-64	-	$128 \cdot 0.4 = 52$ Bits	2392	N/A	15.488	Low-Moderate

[2]

[2] Quelle: Mathieu David, Lightweight Cryptography for Passive RFID Tags

Inhalt

Definition

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

Unerlaubtes Auslesen I

Logische Angriffe

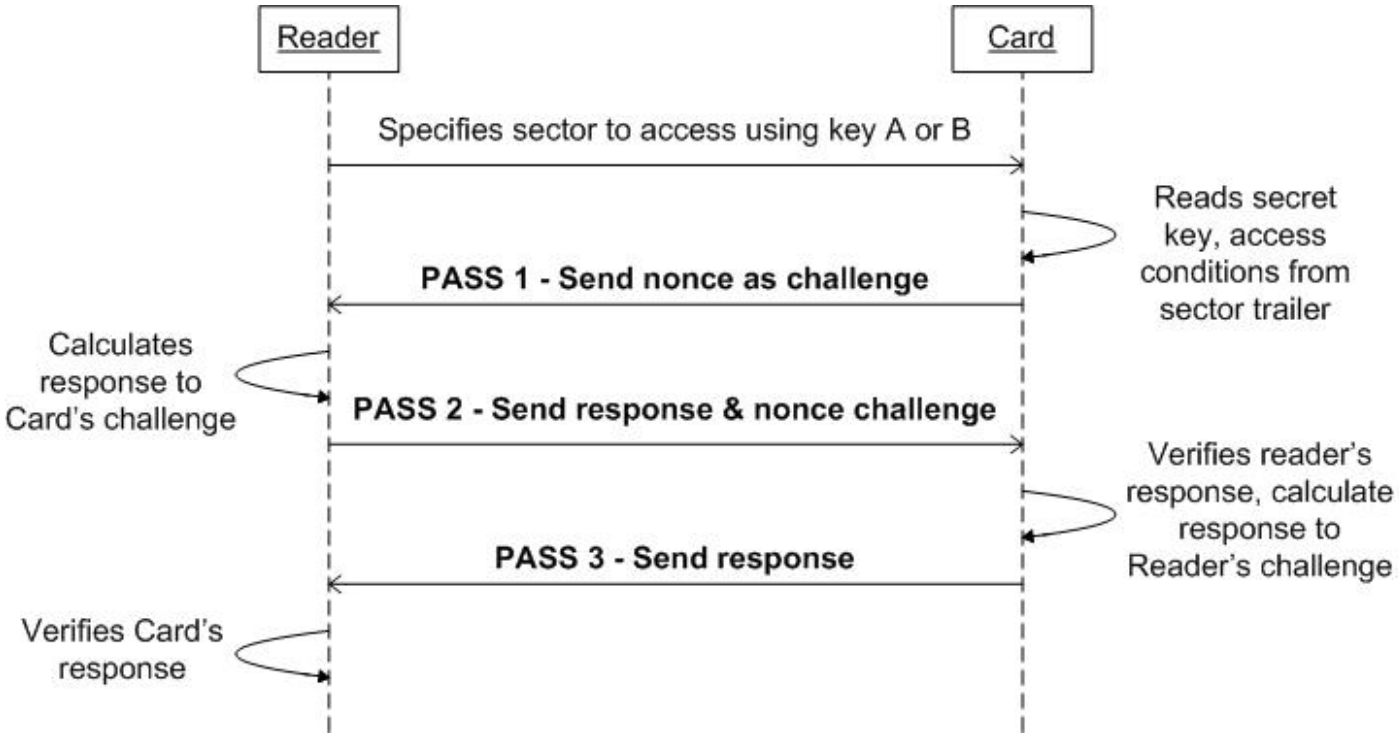
Angriff:

- Angreifer aktiviert Transponder zum Auslesen
- Reichweite für LF-Tags (*Low Frequency*, 120 kHz - 140 kHz): bis zu 1 Meter
- Reichweite für HF-Tags (*High Frequency*, 13,56 MHz): bis zu 3 Metern

Gegenmaßnahme:

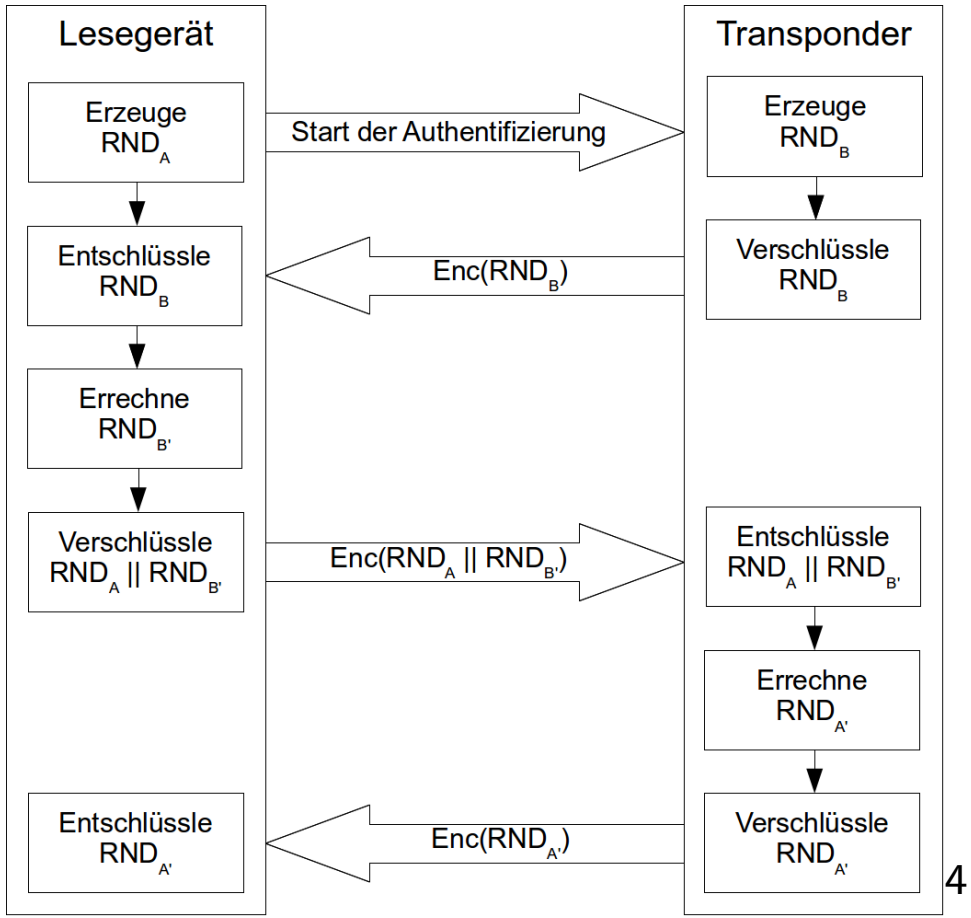
- (Gegenseitige) Authentifizierung

Challenge-Response basierte 3-Pass Mutual Authentication von Mifare Classic



[3]

3-Pass Mutual Authentication



[4]

[3] Quelle: Wee Hon Tan, Practical Attacks on the MIFARE Classic

[4] Quelle: Gerhard H. Schalk und Renke Bienert, RFID - MIFARE und kontaktlose Smartcards angewandt

Lauschangriff (Eavesdropping) I

Logische Angriffe

Angriff:

- Angreifer belauscht (passiv) eine Kommunikation zwischen Transponder und Lesegerät

Gegenmaßnahme:

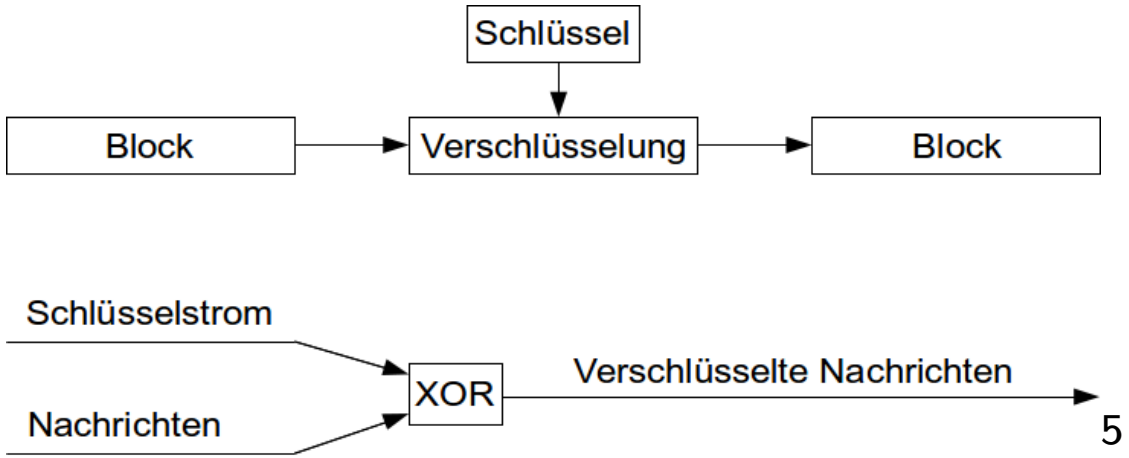
- Verschlüsselung

Lauschangriff (Eavesdropping) II

Logische Angriffe

Wahl der Chiffre:

- In der Vergangenheit oftmals proprietär
- Heute vermehrt bewährte Verfahren (z.B. DES oder AES)
- Vom Einsatz einer Stromchiffre abgeraten, da mit vertretbarem Aufwand kaum ein sicheres Schlüsselmanagement zu realisieren ist



Lauschangriff (Eavesdropping) III

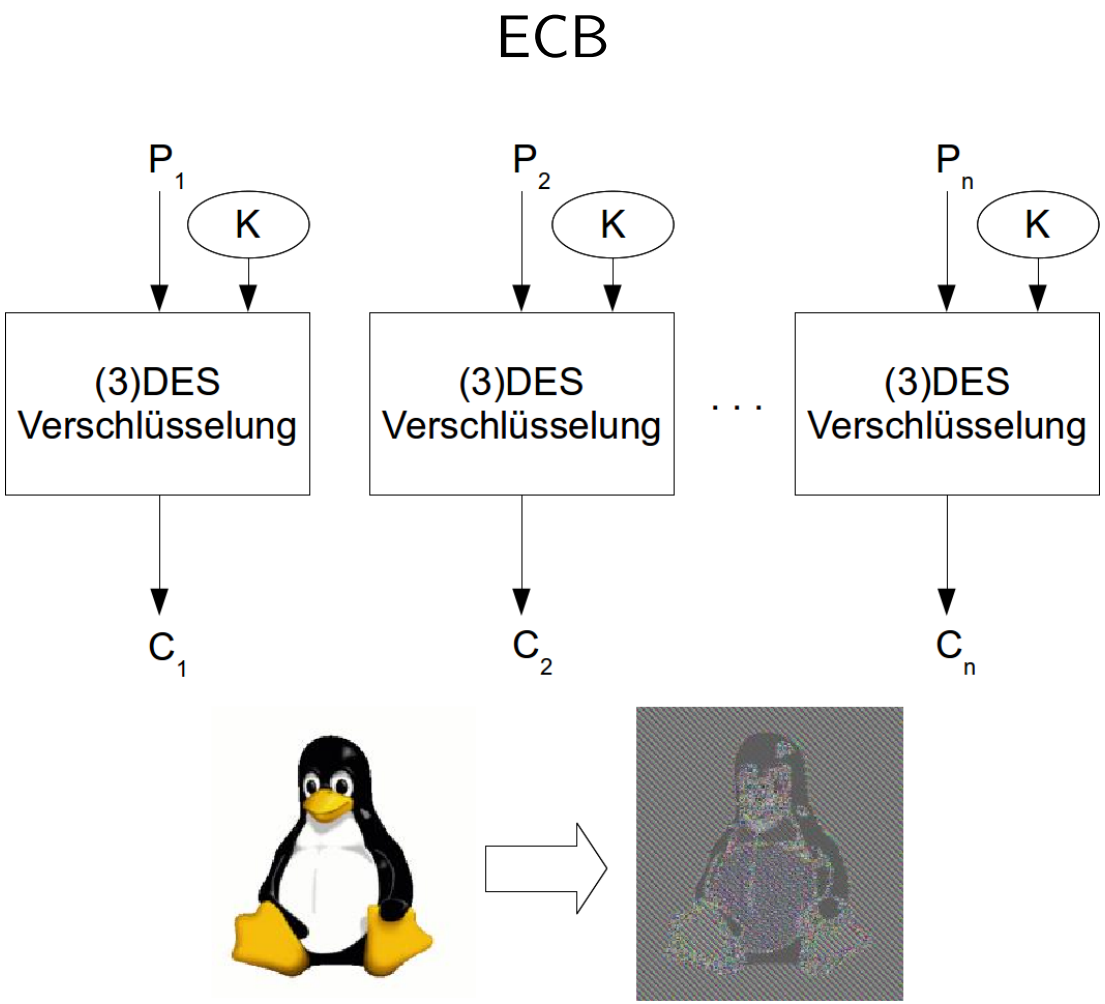
Logische Angriffe

Wahl des Operationsmodus (für Blockchiffren):

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- PCBC, CFB, ...

Lauschangriff (Eavesdropping) IV

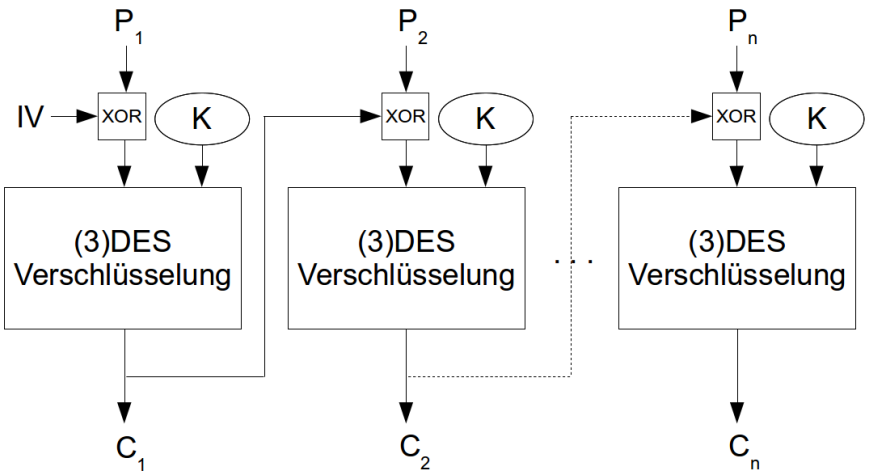
Logische Angriffe

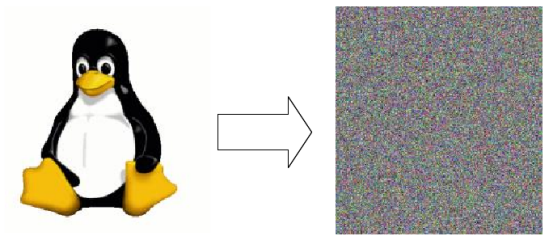


Lauschangriff (Eavesdropping) V

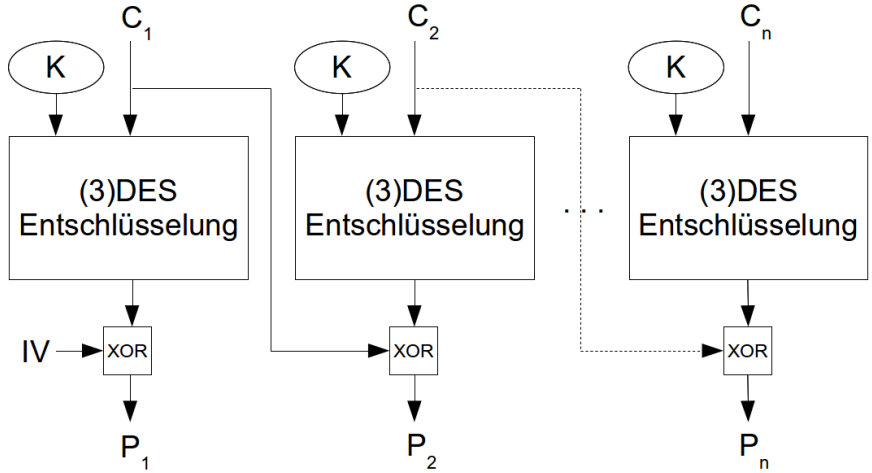
Logische Angriffe

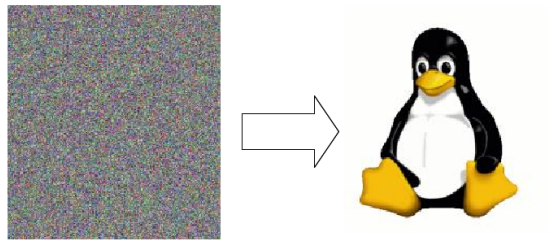
CBC (Verschlüsselung)





CBC (Entschlüsselung)





[5] Quelle: Gerhard H. Schalk und Renke Bienert, RFID - MIFARE und kontaktlose Smartcards angewandt

Unerlaubte Manipulation I

Logische Angriffe

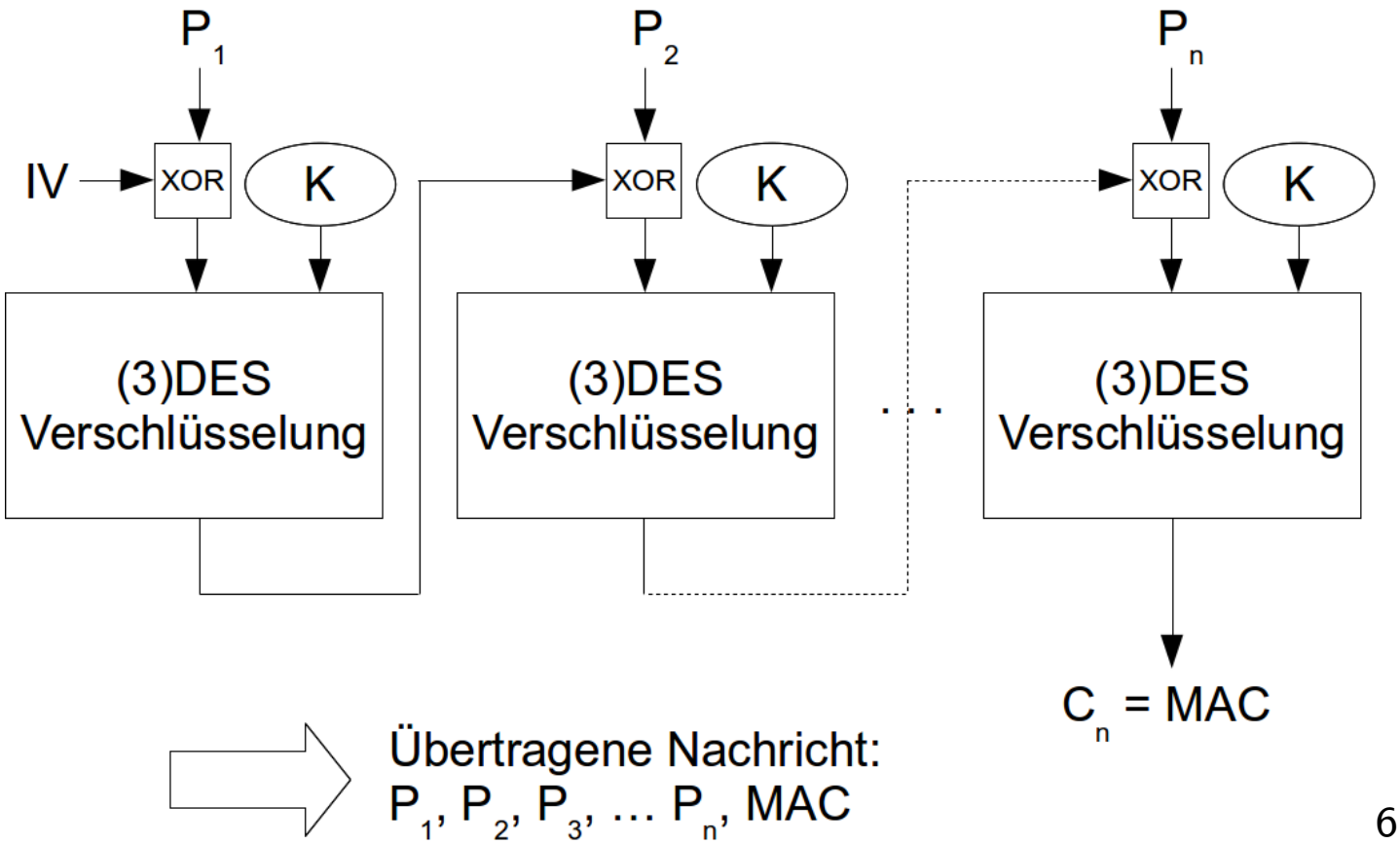
Angriff:

- Angreifer verändert, wiederholt, etc. eine Kommunikation zwischen Transponder und Lesegerät

Probleme und Gegenmaßnahmen:

- Die empfangene Nachricht kommt vom „echten“ Sender
  $\rightarrow$ Authentifizierung
- Die empfangene Nachricht wurde nicht manipuliert
  $\rightarrow$ MAC (Message Authentication Code)
- Die empfangene Nachricht ist keine Wiederholung einer alten, gültigen Nachricht, die bereits früher empfangen wurde
  $\rightarrow$?

Beispeil für ein MAC (Message Authentication Code)



6

[6] Quelle: Gerhard H. Schalk und Renke Bienert, RFID - MIFARE und kontaktlose Smartcards angewandt

Reply-Angriff I

Logische Angriffe

Angriff:

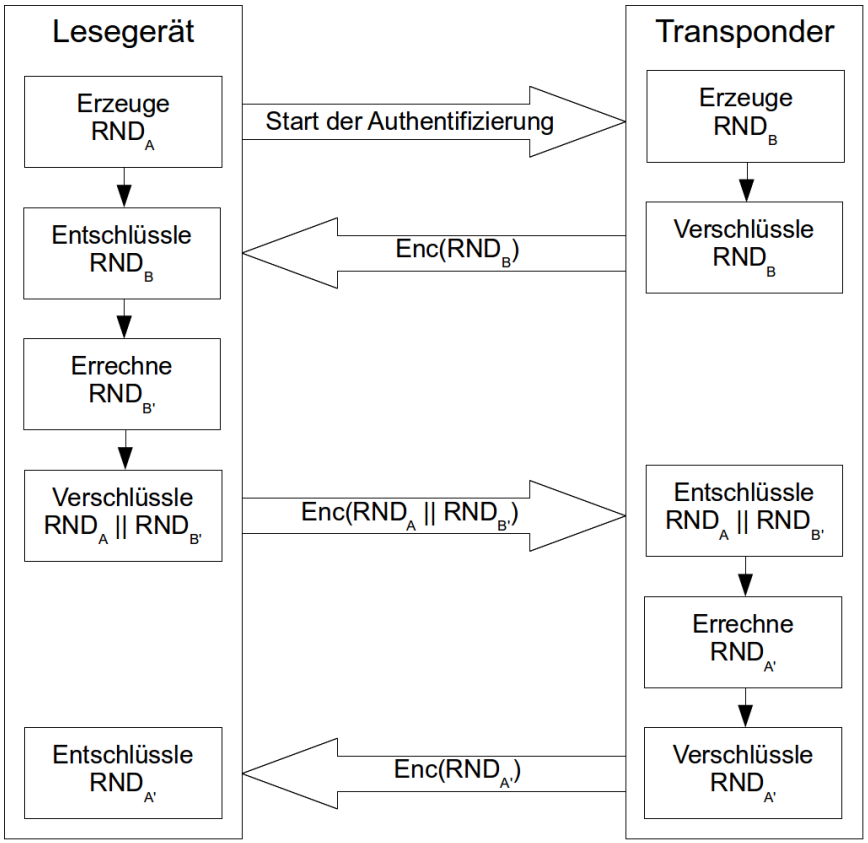
- Angreifer wiederholt eine Kommunikation zwischen Transponder und Lesegerät

Gegenmaßnahmen:

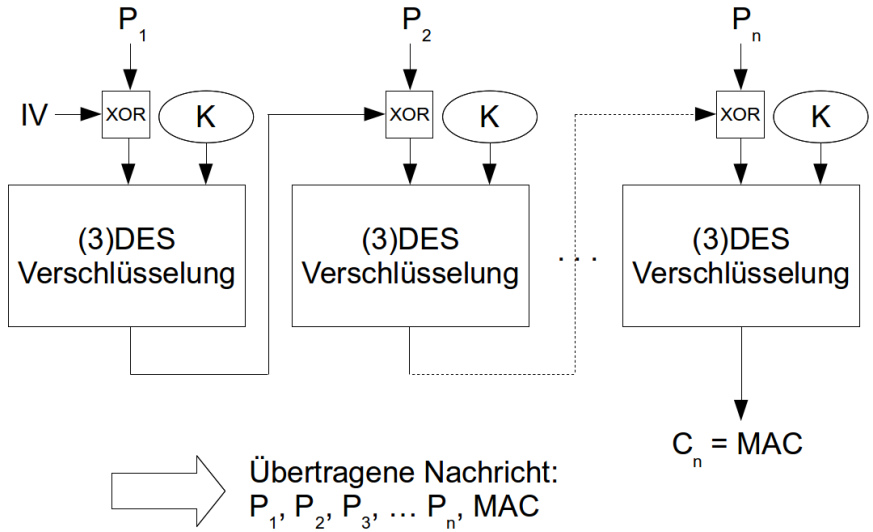
- Session Keys
- Zähler

Reply-Angriff II

Session Key $= F_1(RND_A)$



IV $= F_2(Zähler)$



Relay-Angriff I

Logische Angriffe

Angriff:

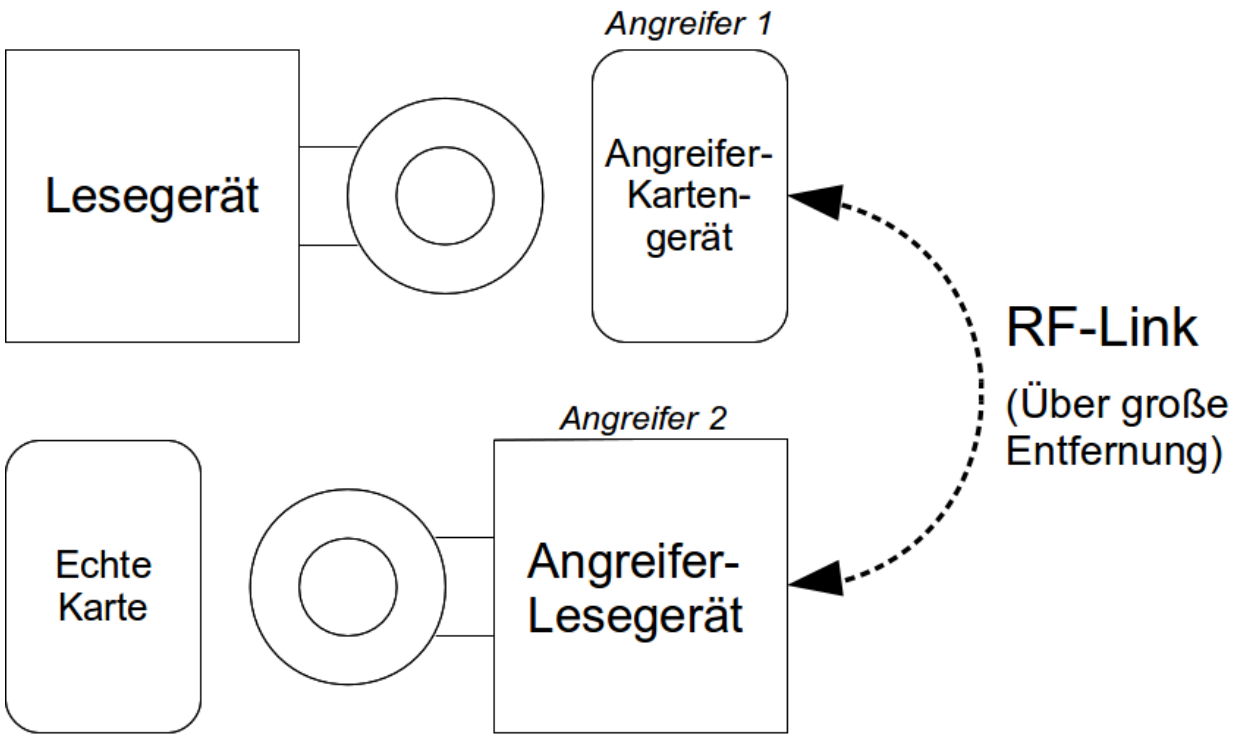
- Physikalisches Vorhandensein des Transponders wird über eine große Entfernung vorgetäuscht

Gegenmaßnahme:

- Zeitkritische Kommandofolge
- (Es gibt keine wirklich gute Lösung)

Relay-Angriff II

Logische Angriffe



Blocker Tags

Logische Angriffe

Angriff:

- Angreifer platziert Blocker Tag im Feld des RFID-Readers und löst damit ein „Denail of Service“ aus
- Blocker Tags nutzt Eigenschaften der gängigen Antikollisionsalgorithmen aus (Binary-Search und/oder Slotted-ALOHA-Verfahren)

Gegenmaßnahme:

- Keine?!

Definition

Unter „physikalischen“ Angriffen sind Angriffsmethoden gesammelt, die hardwarebedingte Eigenschaft des RFID-Transponders oder des Lesegeräts ausnutzen.

Physikalische 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.

Seitenkanalangriff: Power Analysis

Physikalische Angriffe

Angriff:

- Seitenkanalangriff: Angreifer beobachtet Systemkomponenten bei ihrer Arbeit, um Korrelationen zwischen dem was ermittelt wurde und dem was im Inneren passiert herzustellen.
- Beispiel Power Analysis: Angreifer misst Stromverbrauch eines Transponders um den geheimen Schlüssel herauszufinden

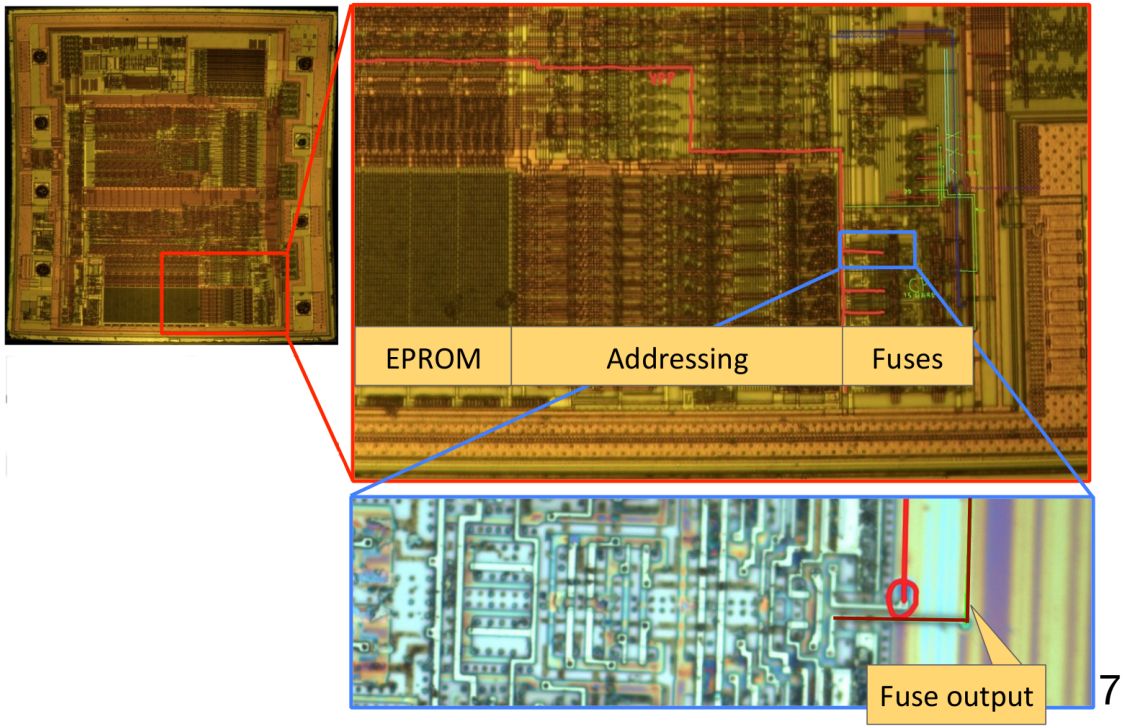
Gegenmaßname:

- Kritische Operationen im Stromverbrauch kaschieren

Reverse Engineering

Physikalische Angriffe

- Rückwärtiges Herausfinden einer Schaltung aus dem fertigen Aufbau
- Erfolgreich angewandt beim Mifare Classic Hack:
  Die proprietäre Chiffre „CRYPTO-1“ konnte komplett rekonstruiert werden



[7]

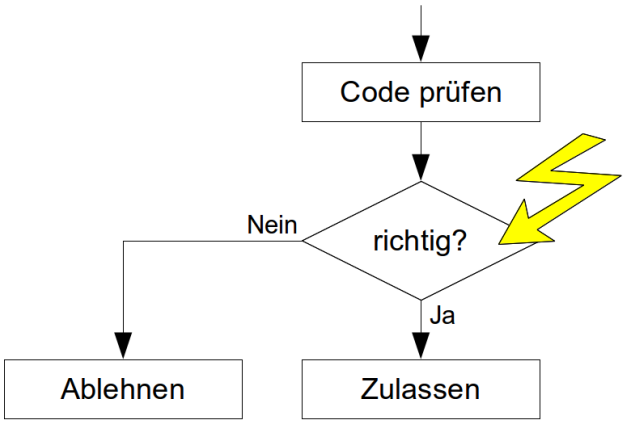
[7] Quelle: Philipp Maier und Karsten Nohl, Low-Cost Chip Microprobing

Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- und Spannungsangriffe I

Physikalische Angriffe

Angriff:

- Angreifer will Programmablauf zu seinen Gunsten manipulieren



8

Gegenmaßnahmen:

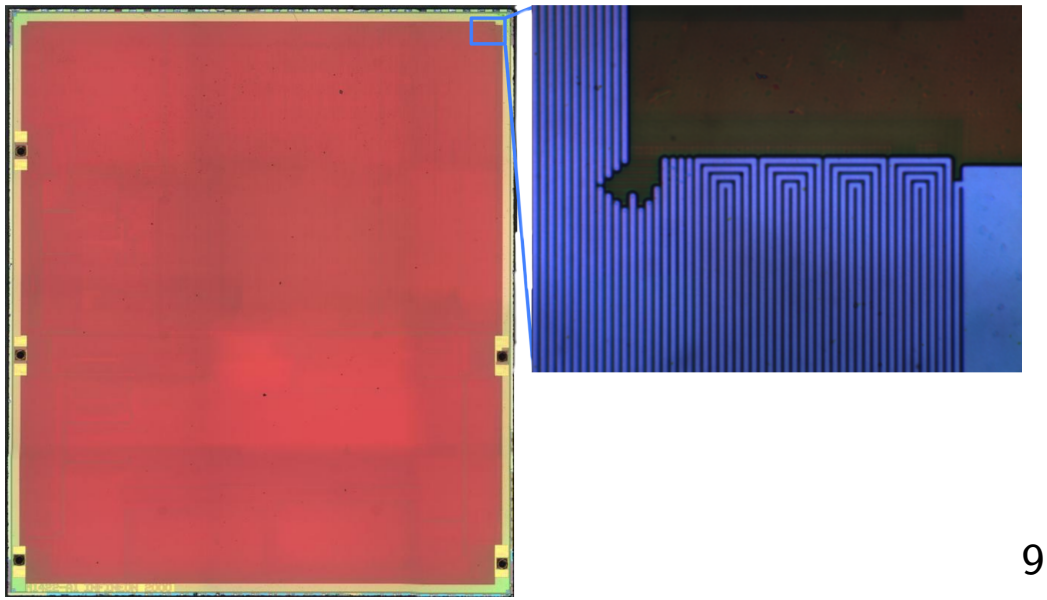
- Je nach Angriff unterschiedlich

Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- und Spannungsangriffe II

Physikalische Angriffe

Microprobing:

- Angriff: Am geöffneten Chip Daten direkt mit Nadeln von den Leiterbahnen abgreifen/manipulieren
- Gegenmaßnahme: Schutzgitter (Bei einem Angriff wird der Chip abgeschaltet)



9

Micoprobing, Licht-, Laser-, Temperatur-, Frequenz- und Spannungsangriffe III

Licht- und Laserangriffe:

- Angriff: Am geöffneten Chip Daten durch optisch sichtbares Licht, durch Laser oder durch Röntgenstrahlung manipulieren
- Gegenmaßnahme: Lichtsensoren (Bei einem Angriff wird der Chip abgeschaltet)

Temperatur-, Frequenz- und Spannungsangriffe:

- Angriff: Angreifer verändert Betriebsparameter um unkontrollierte Fehlfunktionen hervorzurufen
- Gegenmaßnahmen: Sensoren welche die wichtigsten Parameter überwachen (Bei einem Angriff wird der Chip abgeschaltet)

[8] Quelle: Gerhard H. Schalk und Renke Bienert, RFID - MIFARE und kontaktlose Smartcards angewandt

[9] Quelle: Philipp Maier und Karsten Nohl, Low-Cost Chip Microprobing

Dauerhaftes Zerstören I

Physikalische Angriffe

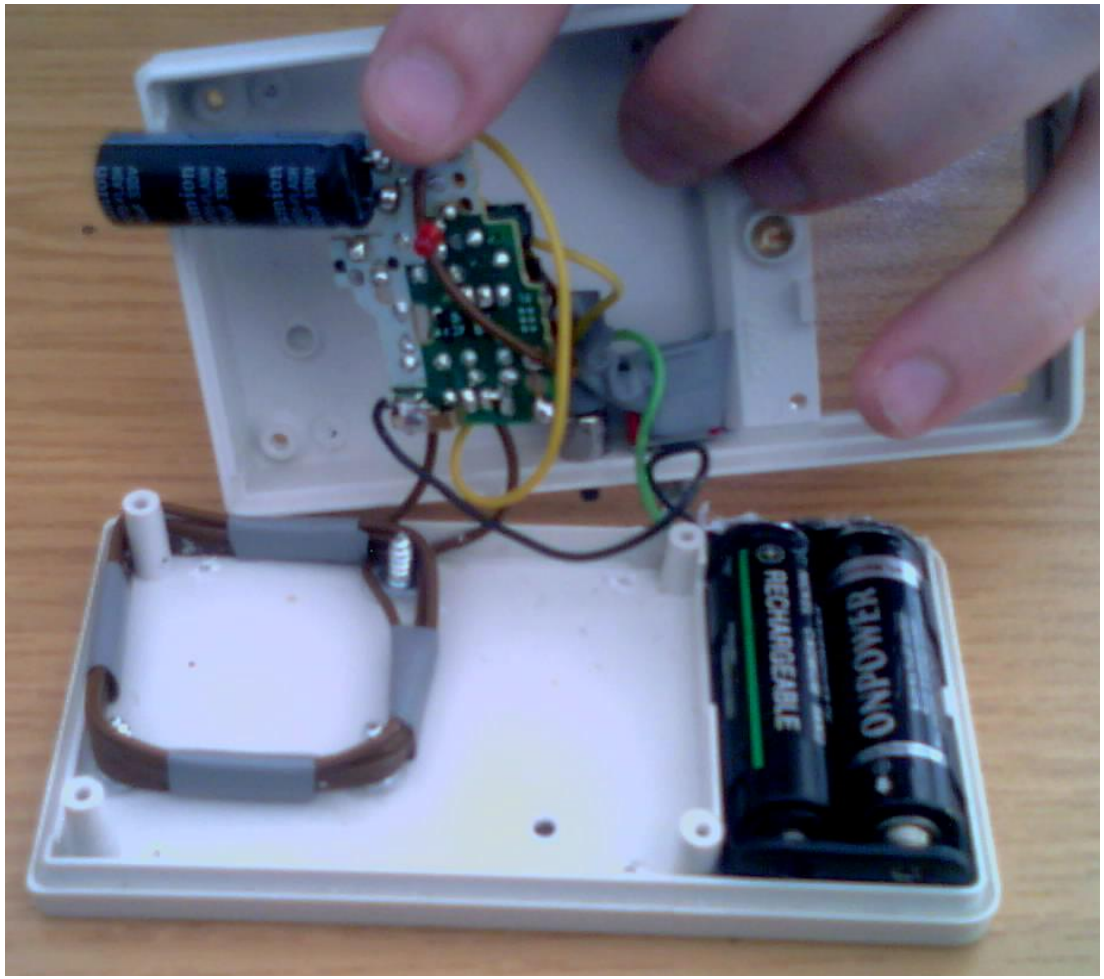
Angriff:

- Angreifer zerstört Transponder durch physikalische Gewalt
- Oder: Angreifer zerstört Transponder durch zu starkes elektromagnetisches Feld
  ($\rightarrow$ hinterlässt keine äußerlich sichtbaren Spuren)

Gegenmaßnahme:

- Keine?!

RFID-Zapper



Random Identifier

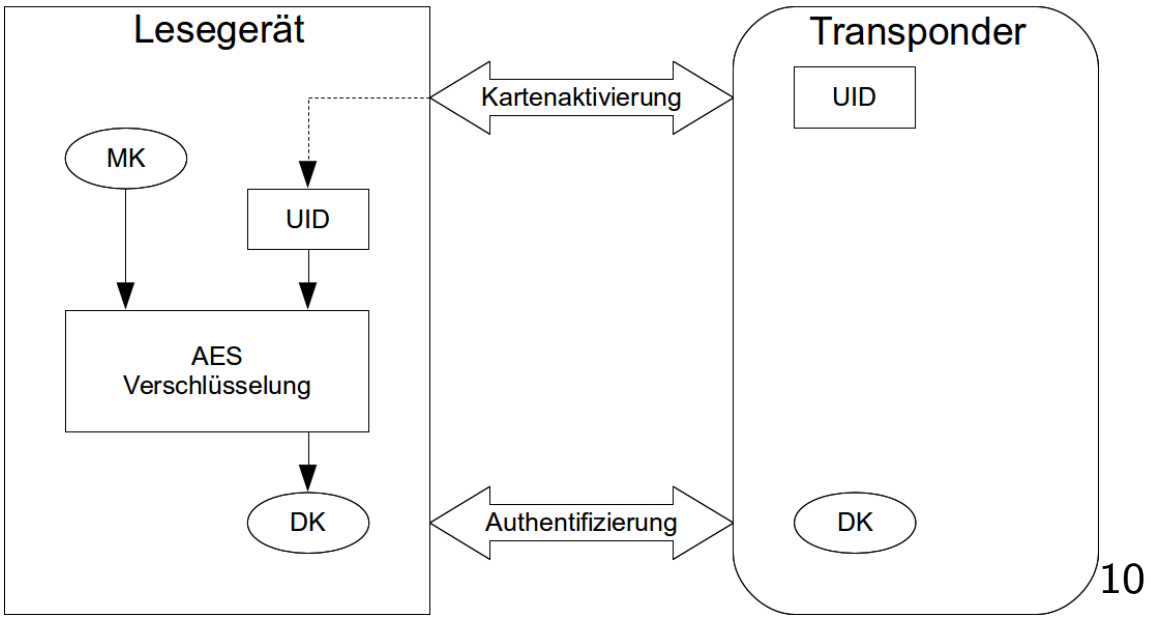
Weitere Sicherheitsmechanismen

- Zur Transponderselektierung wird anstatt der UID (Unique Identifier) eine RID (Random Identifier) verwendet
- UID kann nur verschlüsselt erfragt und übertragen werden
- Tracking durch Dritte wird verhindert (Schutzziel: Privatsphäre)

Schlüsseldiversifizierung I

Weitere Sicherheitsmechanismen

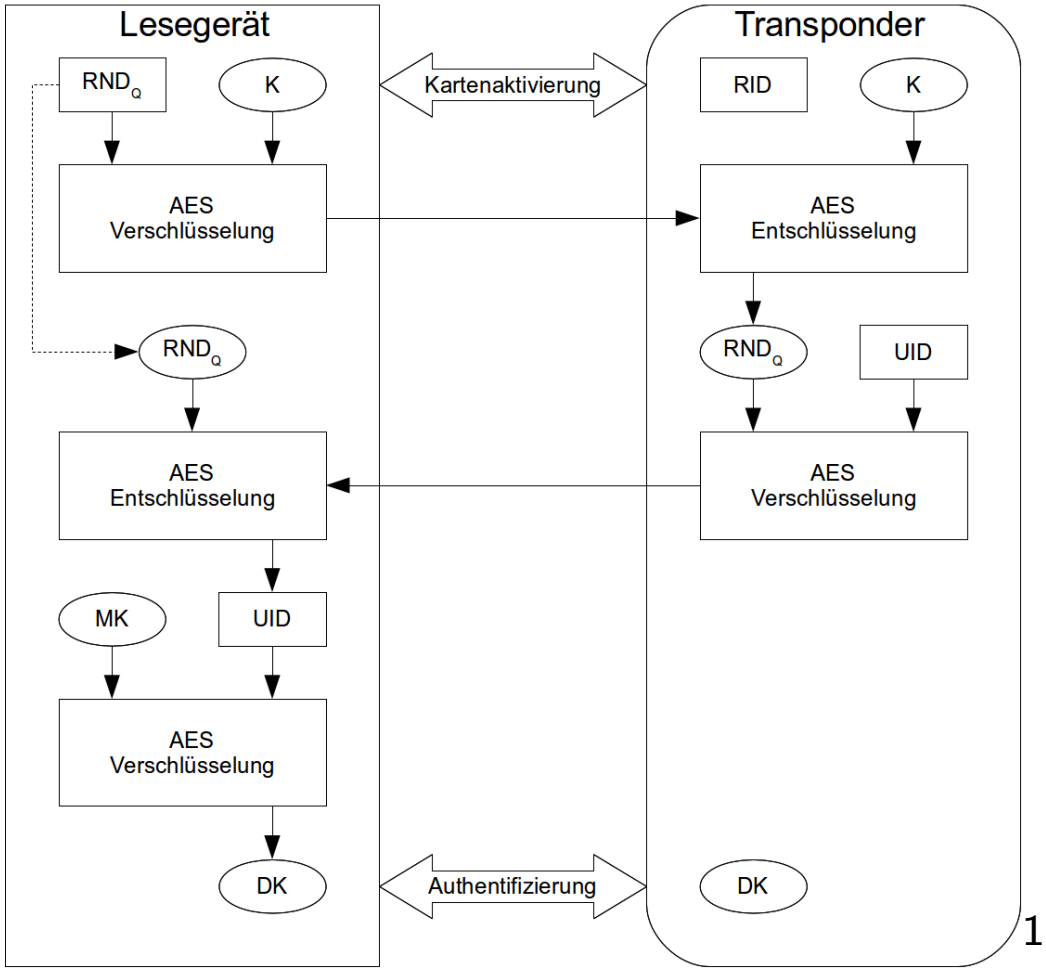
- Problem: Geheimer Schlüssel ist auf jedem Transponder der gleiche
  $\rightarrow$ Schlüsseldiversifizierung



10

Schlüsseldiversifizierung II

Weitere Sicherheitsmechanismen



[10]

[10] Quelle: Gerhard H. Schalk und Renke Bienert, RFID - MIFARE und kontaktlose Smartcards angewandt

Inhalt

Fazit

- Tags müssen billig, klein, schnell, energieeffizient, „bandbreitensparend“, und *SICHER* sein
  ($\rightarrow$ „Tradeoff“-Problem)
- Es gibt eine Vielzahl von „logischen“ Angriffen
- Transponder sind für Angreifer leicht zugänglich
  ($\rightarrow$ physikalische Angriffe)

Fazit

Wie bei jedem anderen IT-System, so bleibt auch bei RFID die Sicherheit ein Ideal, welches angestrebt werden sollte. Eine hundertprozentige Umsetzung in der Praxis ist jedoch schwer möglich.

Fragen

Danke. Fragen?