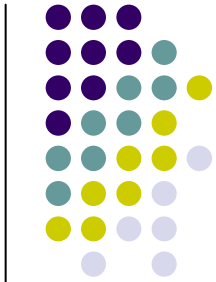
Privatsphäre von RFID

Fachseminar von Jutta Bonan
Betreuer: Christian Flörkemeier

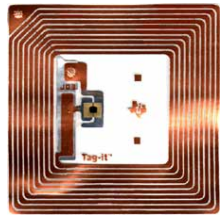
Übersicht:

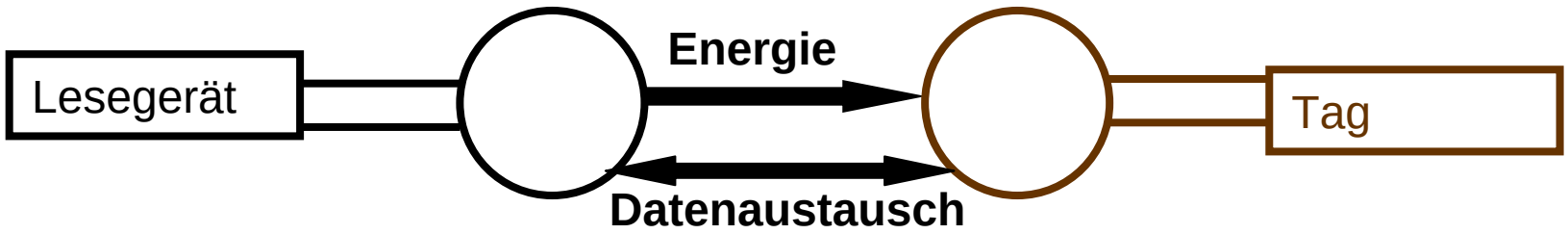


- Was ist RFID?
- Problem: Privatsphäre in RFID
- Hash-Based RFID Protokoll
- RFID-Reisepass
- Zusammenfassung
- Vortrag Oliver Zweifel

Was ist RFID?
(Radio Frequency Identification)

Kontaktlose Datenübertragung durch Funk





Reichweite: ca. 1mm-10m

Übertragungsrate 5 kB/s

Chip: Speicherkapazität bis 2kB

Quelle: Finkenzeller, Handbuch

Anwendungen RFID

1. Vorteil:

Bibliothekverwaltung/ Handel

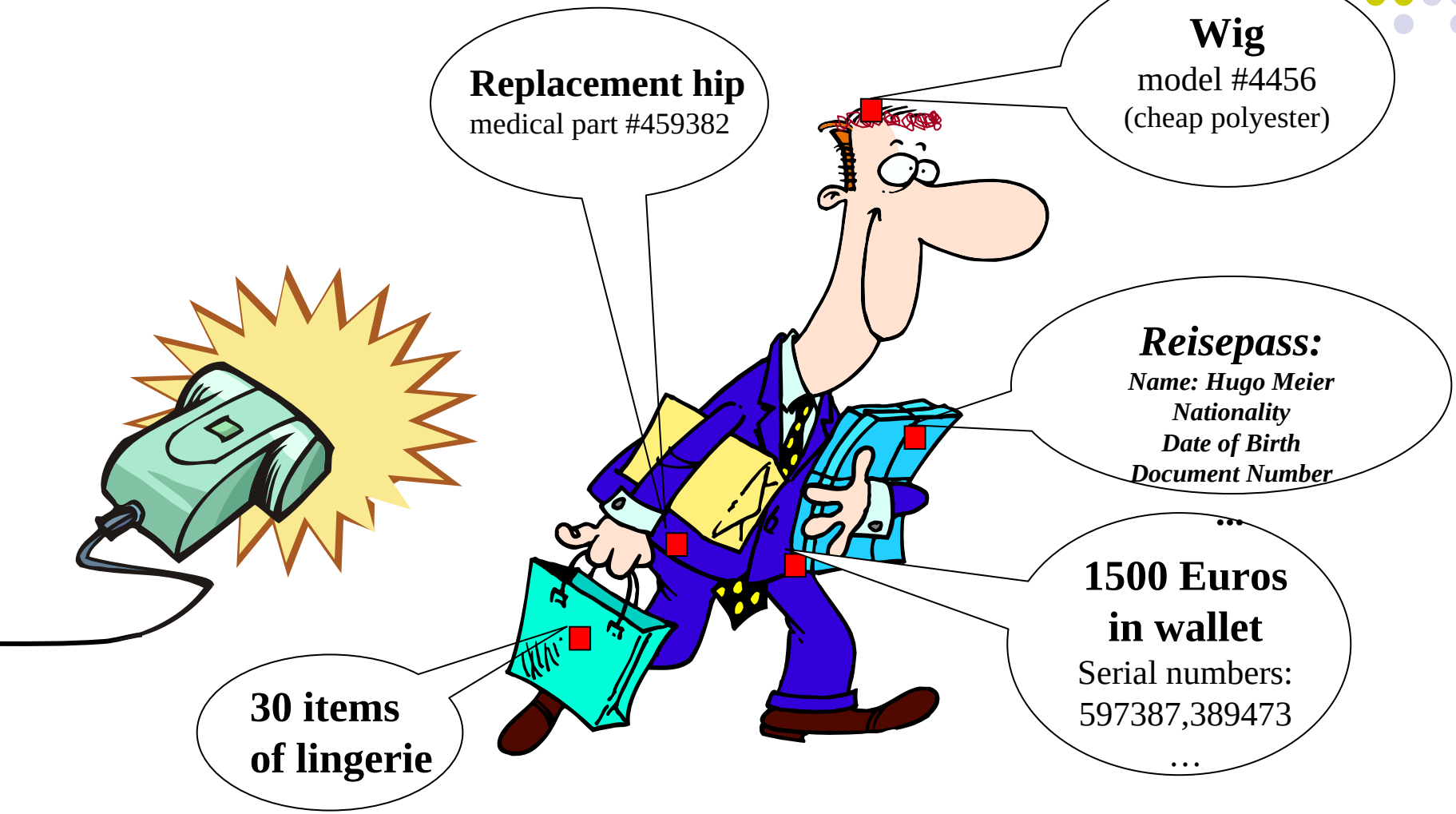
- Bücher automatisch auslesbar, ohne Sichtverbindung
- Einzelner Artikel wird beschrieben und in der Lieferkette verfolgt.

2. Vorteil:

Reisepass

- Tag im Reisepass speichert biometrische Daten
- Längere Lebenszeit, wie Smartkarte mit Kontakte

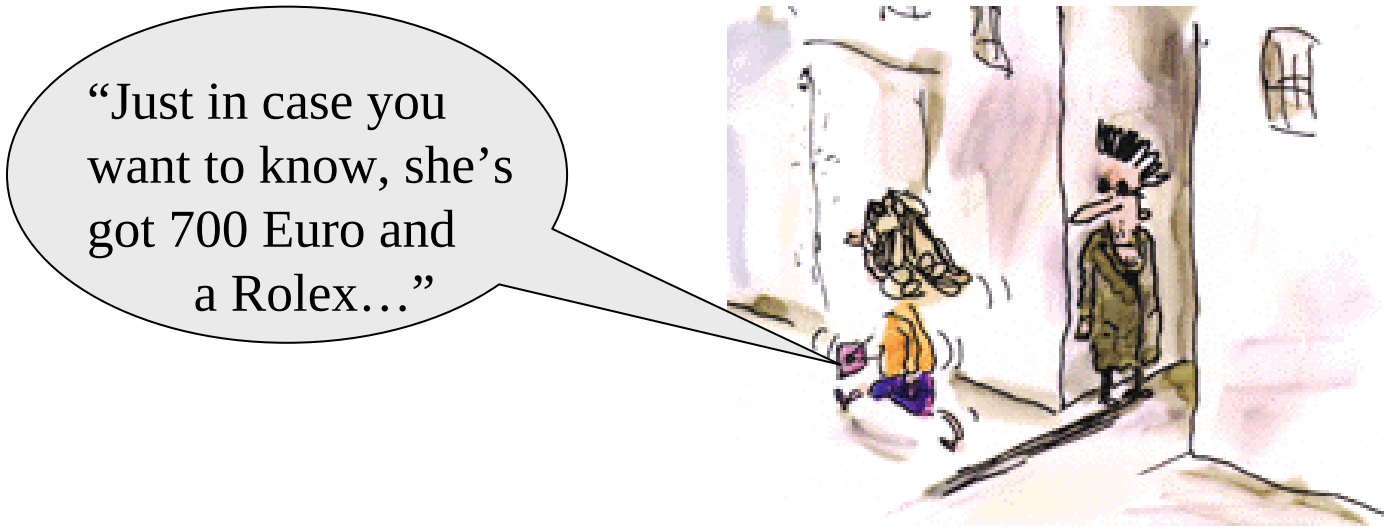
Vorteile werden zu Nachteile: Data-Privacy



Quelle: Ari Jules

Problem: Privatsphäre in RFID (3)

- Kann unter Umständen gefährlich werden:



Quelle: Internet

Vorteile werden zu Nachteile: Location-Privacy

Lesegerät	Zeit	Tag-ID
Lesegerät 1	09:00	12345
Lesegerät 2	11:30	21347
Lesegerät 3	13:00	12345
Lesegerät 2	16:00	98792
Lesegerät 1	22:00	21347

Existierende Lösungen (1)

IDEE: Tag-Objekte mit einer Metallfolie überdecken

- Bibliothek:
  ➔ gute Lösung, Bücher in Alutasche hineinlegen (Problem: Diebstahl)

- Handel:
  ➔ sehr kompliziert, alle Objekte einzupacken

Quelle: Ari Jules

Existierende Lösungen (2)

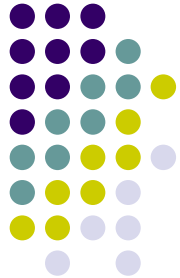
KILL-Tag

- Bibliothek:
  ➔schlechte Lösung, Bücher brauchen bei Rückgabe wieder einen neuen Tag

- Handel:
  ➔sehr schade um den Tag, er könnte im weiteren Gebrauch genützt werden

Quelle: Ari Jules

Andere Lösungen



1. Das Tag wird weiterhin benutzt
2. Nur autorisierte Lesegeräte kennen die wahre Identität

- *Ohkubo, Suzuki und Knoshita* haben ein Protokoll vorgeschlagen
- *Avoine und Oechslin* Verbesserung dieses Protokolls angestrebt

Privacy: Definition

Privacy:

Wird die ID eines Tags gelesen, kann daraus nicht auf seine wahre Identität geschlossen werd
Lesegeräte können dies.

Forward-Privacy:

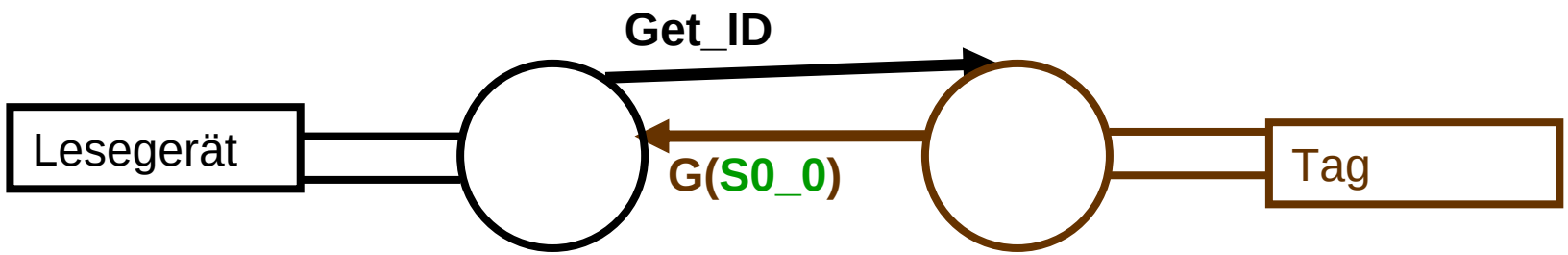
Wird zum Zeitpunkt t Identität ermittelt, l
rückwirkend alle Daten, die zum Zeitpur
gelesen wurden, der Person nicht zugec

Lesegerät	Zeit	Tag-ID
Lesegerät 1	09:00	12345
Lesegerät 2	11:30	21347
Lesegerät 3	13:00	09823
Lesegerät 2	16:00	98792
Lesegerät 1	22:00	52300

Quelle: Avoine und Oechslin

Hash-Based RFID Protokoll

Privacy:



•**ID: S0_0, S_1, S_2, …**

Hashfunktionen: G, H

Wahre ID	G(Si_0)	G(H(Si_0))	G(H(H(Si_0)))	…
S0_0	245	987		
S1_0	808	102		

•**ID: S0_0 (Anfangswert, wahre ID)**
Hashfunktionen: G, H

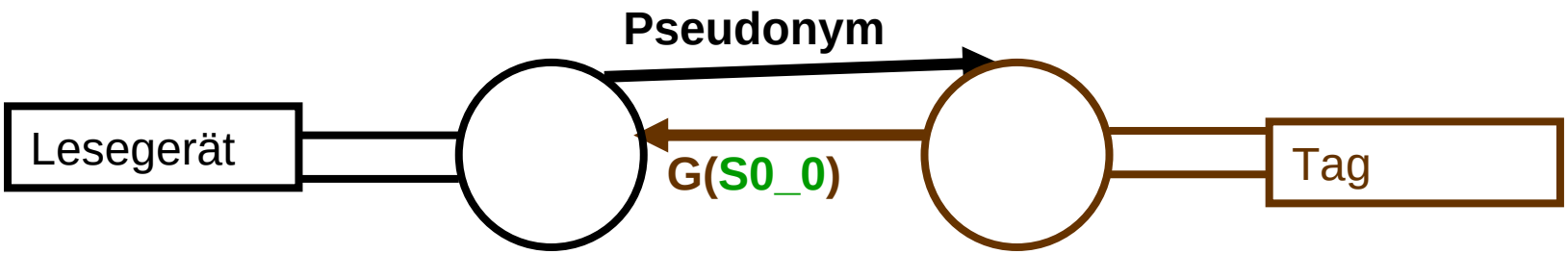
•**ID_neu: S0_1 = H(S0_0)**

Quelle: Ohkubo, Suzuki & Kinoshita

Hash-Based RFID Protokoll

Privacy ist gewährleistet:

Was ist mit Forward-Privacy?



- **S0_1 = H(S0_0)**
- **S0_2 = H(S0_1)**
- **S0_3 = H(S0_2)**

Wahre ID	G(Si_0)	G(H(Si_0))	G(H(H(Si_0)))	…
S0_0	245	987	1237	
S1_0	808	102		

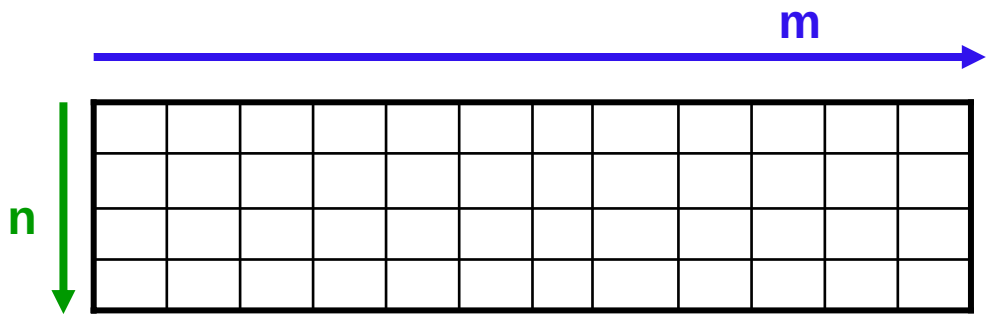
Quelle: Ohkubo, Suzuki & Kinoshita

Hash-Based RFID Protokoll

Bibliothek:

- Annahme: 1 Million Bücher: n = 2^{20}
- Annahme: Tag wird m Mal gelesen: m = 2^{10}
- Annahme: System: 2^{24} Hashoperationen/s,

Ø Zeit n*m /2 = 2^{29} ➔ 2^5 ca. **½ Minute**



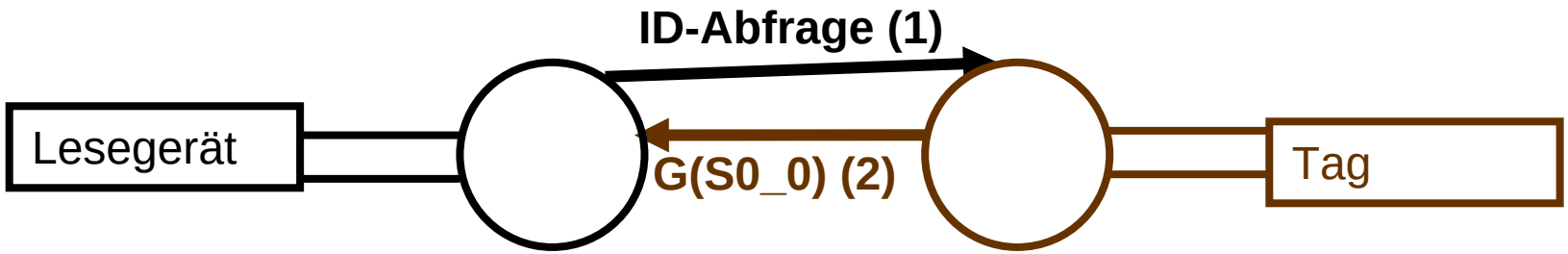
Handel ?

- Länge des Schlüssels S0_0 im Tag: 128 Bits = 2^7
- Speichern von 1 Million Tag-Id benötigt **16 MBytes**

Quelle: Ohkubo, Suzuki & Kinoshita

Verbesserung:

- IDEE: Vorausberechnung der Hashwerte

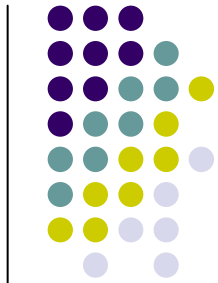


Tag_id	G(Si_0)	G(H(Si_1))	G(H(H(Si_1)))	…
S0_0	45	33	1238	122
S1_0	12	26	1233	554

- Vorteil: Nur noch sequenzieller Scan nötig
- Nachteil: Sehr grosser Bedarf an Speicherplatz

Quelle: Avoine und Oechslin, EPFL

Time-memory trade-off



IDEE:

Optimales Verhältnis zwischen Berechnungsoperationen und Speicherplatz

Wie viele Spalten der Tabelle im voraus berechnet und abgespeichert werden soll.

Bibliotheksbeispiel:

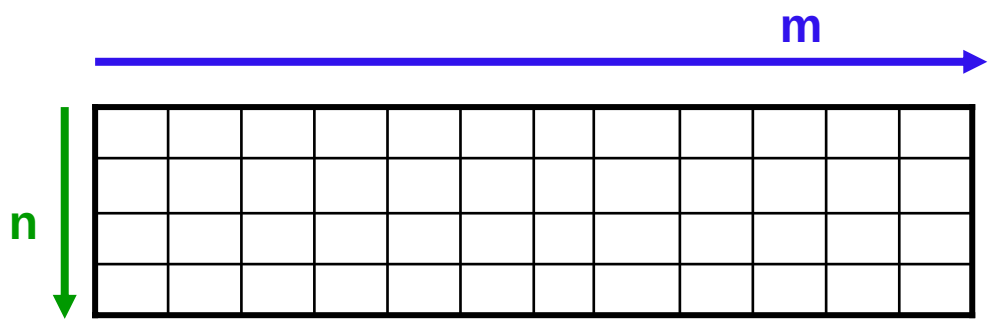
Zugriffszeit auf 0,0016s reduzieren

Quelle: Avoine und Oechslin, EPFL

Hash-Based RFID-Protokoll

FAZIT

- m ➔ Schwäche des Systems
- Kosten vom Tag werden teuerer (Hashfunktion)
- Lesegerät muss Si_0 geheim halten



RFID-Reisepass (Data-Privacy)

November 2005: RFID im EU-Pass

neu:

- Digitales Gesichtsbild
- (Fingerabdrücke)

Ziel:

- stärkere Bindung zw. Person u. Reisepass
- Fälschungssicherheit (zusätzliche Signaturen)

Vorteile werden zu Nachteile: Data-Privacy

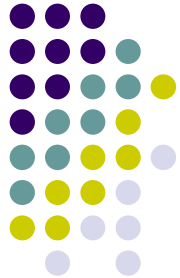
Reisepass:

Name: Hugo Meier
Nationality: CH
Date of Birth: 1.4.46
Document Number: 1234
Sex: m
Date of Expiry or Valid Until Date: 2015
Optional Data: blalbalbla
...

Verhindern, dass Speicher ausgelesen wird!

Quelle: Ari Jules

RFID-Reisepass (Data-Privacy)



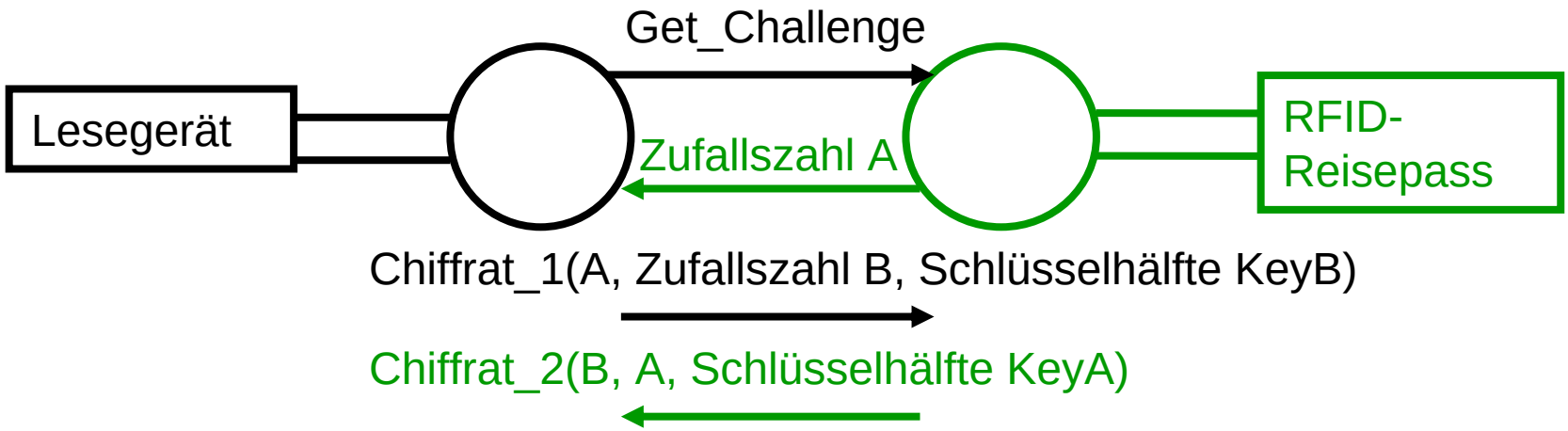
- Lösungsansatz (1):
  - Keine Schutzfunktion, Lesebereich einschränken
- Probleme:
  - manipuliertes Lesegerät, kann auslesen
  - Passives Mithören einer Kommunikation immer noch möglich

RFID-Reisepass (Data-Privacy)

- Lösungsansatz (2):
  - Auslesen des Passes nur wenn optischer Zugriff möglich ➔ Inhaber „erlaubt“ das Auslesen
  - Lesegerät muss sich authentisieren
  - verschlüsselte Kommunikation

RFID-Reisepass: Challenge-Response Authentifikations-Protokoll

Key = Code vom Pass

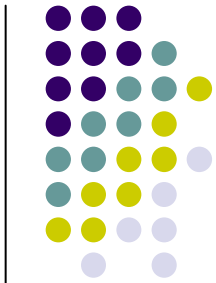


Vorteile:

- authentisieren von Lesegerät gegenüber Tag und umgekehrt
- Key (Code vom Pass) nur einmal übertragen (sichere Kanal, optisch)
- Sicherer Kommunikationskanal mit längerem Key:= KeyAKeyB

Quelle: Risiko Reisepass?, Kügler

RFID-Reisepass (Data-Privacy)



- FAZIT:

  Authentifizierung erfolgreich:
  - keiner kann die Kommunikation mithören
  - Data-Privacy ist gewährleistet
  - Location-Privacy auch gewährleistet

- FRAGE:

  Warum nicht so etwas bei der Bibliothek einsetzen?
- ANTWORT:
  - Tag wird zu teuer
  - Dauert lange

Zusammenfassung

Privatsphärenprobleme im RFID-Bereich

- 2 Probleme:
  - Location-Privacy
  - Data-Privacy
- Vorgestellte Lösungen:
  - Hash-based-Protokoll,
  - Reisepass

Quellen

- A Scalable and Provably Secure Hash-Based RFID Protokoll (Avoine and Oechslin, EPFL)
- Cryptographic approach to „privacy-friendly“ tags. In RFID Privacy Workshop (M. Ohkubo, K. Suzuki, and S. Kinoshita, MIT, USA, 2003)
- Risiko Reisepass? (Dr. Dennis Kügler)
- Risiken und Chancen des Einsatzes von RFID-Systemen (Bundesamt für Sicherheit in der Informationstechnik)
- Bilder: Internet, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker_slides.pdf

FRAGEN?

Privatssphäre von RFID

… Sicherheit von RFID