Sicherheit in Rechnernetzen

Mehrseitige Sicherheit in verteilten und durch verteilte Systeme

Folien zur Vorlesung: Datensicherheit durch verteilte Systeme

Andreas Pfitzmann
TU Dresden, Fakultät Informatik, D-01062 Dresden
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Schutz des Empfängers: Verteilung

A. Pfitzmann, M. Waidner 1985

Leistung? leistungsfähigeres Übertragungssystem

Adressierung (wo möglich: Kanäle schalten)
explizite Adressen: Routing
implizite Adressen: Merkmal für Station des Adressaten

verdeckt <==> Konzelationssystem
offen Bsp. Pseudozufallszahlen(generator),
Assoziativspeicher für Erkennung

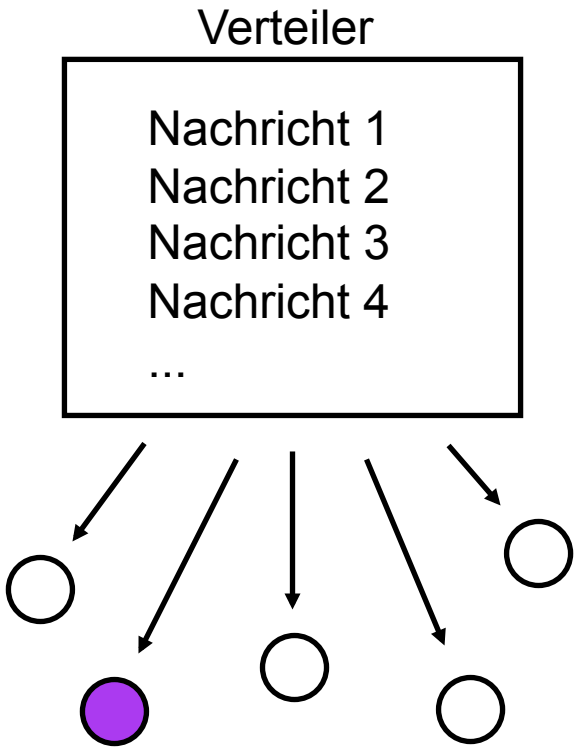
		Adreßverwaltung	
		öffentliche Adresse	private Adresse
implizite Adres-sierung	verdeckt	sehr aufwändig, für Kontaktaufnahme nötig	aufwändig
	offen	abzuraten	nach Kontaktaufnahme ständig wechseln

Äquivalenz: Konzelationssysteme und implizite Adressierung

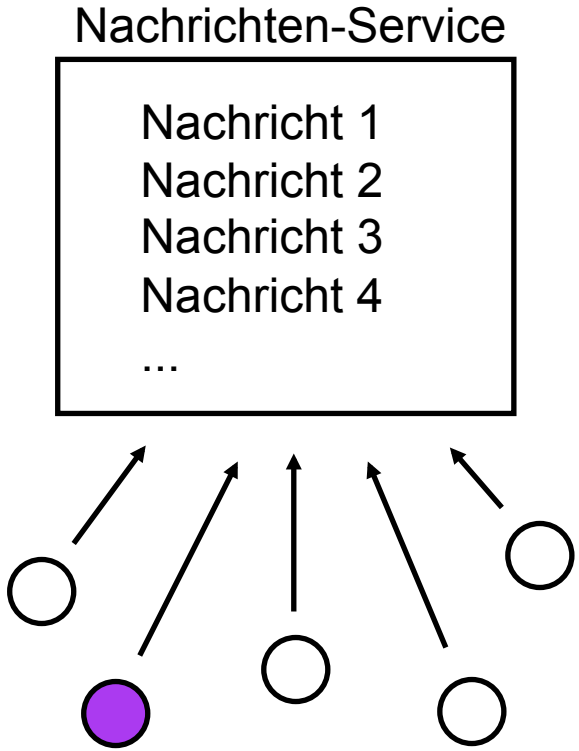
verdeckte öffentliche Adresse <==> asymmetrisches Konzelationssystem

verdeckte private Adresse <==> symmetrisches Konzelationssystem

Verteilung vs. Abfragen



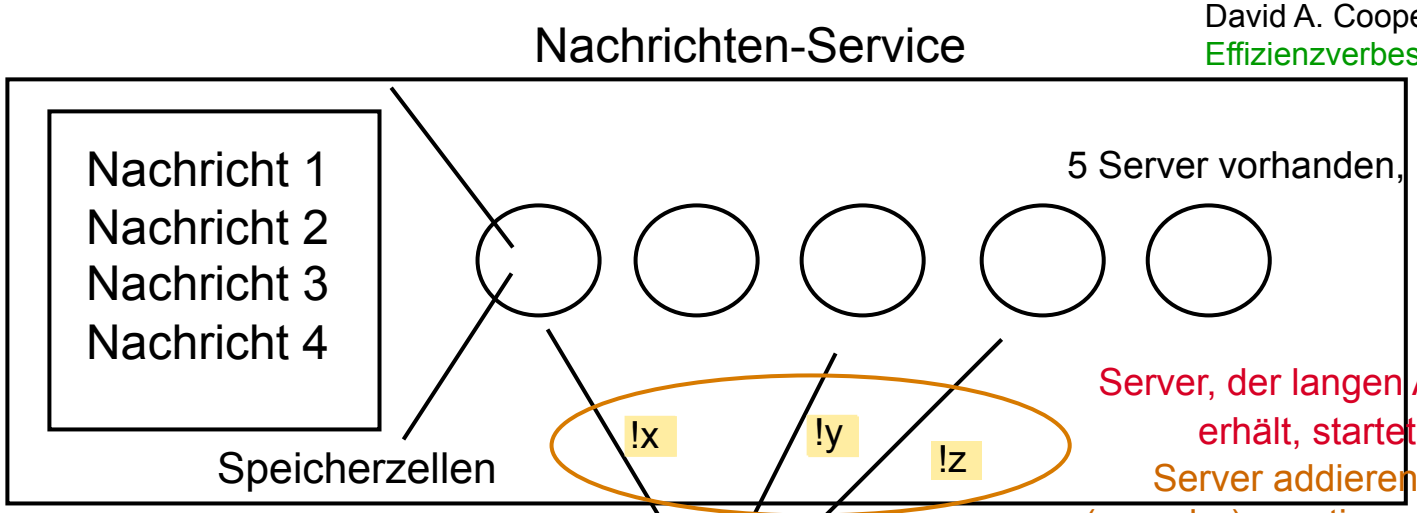
Verteilung der einzelnen Nachrichten an alle



Jeder kann alle Nachrichten abfragen

Beispiel für Nachrichten-Service

David A. Cooper, Kenneth P. Birman 1995
Effizienzverbesserungen: A. Pfitzmann 2001



5 Server vorhanden, alle enthalten die gleichen Nachrichten in derselben Reihenfolge

Server, der langen Abfragevektor erhält, startet Umlauf
Server addieren Antworten, die mit (pseudo-) one-time pads verschlüsselt sind

3 Server benutzt für überlagertes Abfragen

XOR

von Servern bei Umlauf selbst generiert

Pseudo-zufällig ~~kurz~~

Bitposition entspricht Speicherzelle

?x = 1001
?y = 1100
?z´ = 0101

**

?z = 0111

0

~~1/3~~

1/3

Teilnehmer

invertiere Bit der interessierenden Speicherzelle

Antwort vom Nachrichten-Service:

~~!x~~ = Nachricht 1 XOR Nachricht 4 XOR pad_x
~~!y~~ = Nachricht 1 XOR Nachricht 2 XOR pad_y
~~!z~~ = ~~Nachricht 2~~ XOR Nachricht 3 XOR Nachricht 4 XOR pad_z

= pad_x XOR pad_y XOR Nachricht 2 XOR Nachricht 3 XOR pad_z

daraus folgt durch lokale Überlagerung der pads
~~!x XOR !y XOR !z~~ => Nachricht 3 XOR Nachricht 2
(entspricht Summe der gewünschten (**) Speicherzellen)

Abfragevektoren

Abfrage mehrerer Speicherzellen

„Abfragen und Überlagern“ statt „Verteilung“

Speicherzelle, in die mehrfach geschrieben werden kann = implizite Adresse

Schreiben = Addition mod 2 (ermöglicht, viele Speicherzellen in einem Schritt zu lesen)

Kanäle trivial realisierbar

Zweck impliziter Adressen

Verteilung: Effizienz (Auswertung impliziter Adressen sollte schneller gehen als das Verarbeiten ganzer Nachrichten)

Abfragen und Überlagern: Mehrfachzugriff; Effizienz (sollte die Zahl zu lesender Speicherzellen reduzieren)

Speicherzelle fest = offene implizite Adresse

Implementierung: feste Abfragevektoren für Server 0 ↗ ↙ 1

Anzahl Adressen wächst *linear* mit dem Aufwand (des Überlagerns).

Verbesserung: Eine *Menge* von Speicherzellen = implizite Adresse

Nachricht m wird in einer Menge von Speicherzellen gespeichert, indem a–1 Werte zufällig gewählt werden und der Wert der a-ten Speicherzelle so, dass die Summe aller a Zellen m ist.

Für insgesamt n Speicherzellen gibt es nun 2^n–1 nutzbare implizite Adressen, aber wegen der Überlappungen ihrer Zellen können sie nicht unabhängig voneinander genutzt werden.

Falls wegen Überlappung Kollisionen auftreten, versuche Wiederholung der Übertragung nach zufällig gewähltem Zeitintervall.

Jede Menge von Zellen wie auch jede Menge von Mengen von Zellen kann in einem Schritt gelesen werden.

Verdeckte implizite Adressen bei „Abfragen und Überlagern“

Speicherzelle variiert (Speicherzellenhopping) = verdeckte implizite Adresse

Idee: Teilnehmer, der verdeckte implizite Adresse zum Zeitpunkt *t* verwenden will, liest zum Zeitpunkt *t*-1 Werte aus bekannten Speicherzellen, die Speicherzelle zum Zeitpunkt *t* bestimmen.

Impl.:
- Adressinhaber gibt jedem Server *s* einen PBG_s.
- Jeder Server *s* ersetzt zu jedem Zeitschritt *t* den Inhalt der ihm zugeordneten bekannten Speicherzelle S_{Adr} durch $PBG_s(t)$:

  $S_{Adr} := PBG_s(t)$
- Teilnehmer fragt über MIXe $\sum_s PBG_s(t)$ ab. (Geht in einem Schritt.)

  Teilnehmer verwendet $S_{\sum_s PBG_s(t)}$ für Nachricht. 1↗↙1
- Adressinhaber bildet $\sum_s PBG_s(t)$ und liest mittels „Abfrage und Überlagern“ $S_{\sum_s PBG_s(t)}$

  Optimierung: für alle seine verdeckten impliziten Adressen gemeinsam: 1↗↙2 (wenn ≤ 1 Nachricht)

Adresse ist insoweit verdeckt, dass zu jedem Zeitpunkt nur ein sehr kleiner Teil der möglichen Kombinationen der Speicherzellen S_{Adr} gelesen werden kann.

Verdeckte implizite Adressen bei „Abfragen und Überlagern“

Speicherzellenhopping = verdeckte implizite Adresse

Kann erweitert werden auf:

Springen zwischen *Mengen von* Speicherzellen

= verdeckte implizite Adresse

Fehlertoleranz (und Verhinderung verändernder Angriffe)

Was wenn Server (absichtlich)

1. **nicht antwortet oder**
2. **falsch antwortet?**

1. **Schicke denselben Abfragevektor an einen anderen Server.**
2. **Nachrichten sollten authentisiert sein, so dass der Teilnehmer ihre Integrität prüfen kann und so entdecken, ob mindestens ein Server eine falsche Antwort gegeben hat. Falls ja, sollte eine disjunkte Menge von Servern genutzt werden oder Fallen gelegt werden, indem derselbe Abfragevektor an mehrere Server geschickt wird und deren Antworten verglichen werden.**

Schutz des Senders

Bedeutungslose Nachrichten

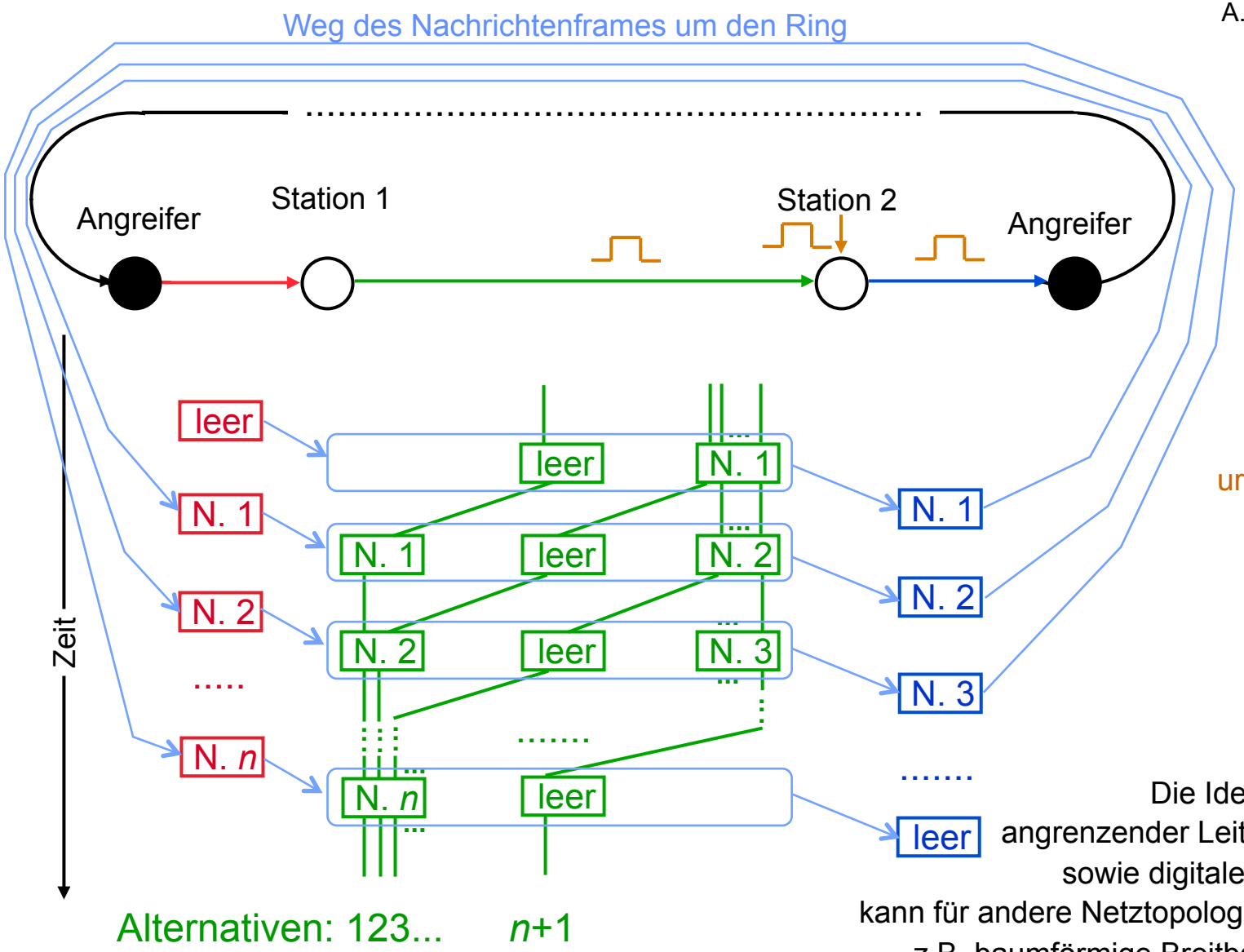
- schützen nicht vor Adressaten bedeutungsvoller Nachrichten
- machen Schutz des Empfängers ineffizienter

Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung

Beispiel: RING-Netz

Beweis der Anonymität eines Ringzugriffsverfahrens

A. Pfitzmann 1983 - 1985



Digitale Signalregenerierung:

Bits sind bezüglich ihrer analogen Charakteristika unabhängig vom ursprünglichen Sender.

Die Idee Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung kann für andere Netztopologien adaptiert werden, z.B. baumförmige Breitbandkabelverteilnetze.

Die Idee wurde in einem anderen Kontext in Crowds wiederentdeckt.

Fehlertoleranz beim RING-Netz

Anforderung

In möglichst jedem (Fehler-)Fall muss die Anonymität garantiert werden

Problem

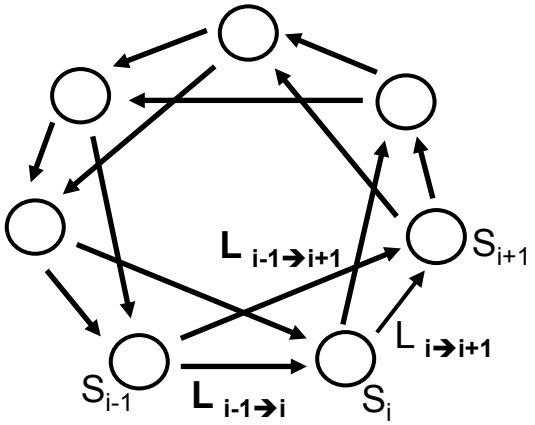
Anonymität: wenig globale Information
Fehlertoleranz: viel globale Information

Prinzipien

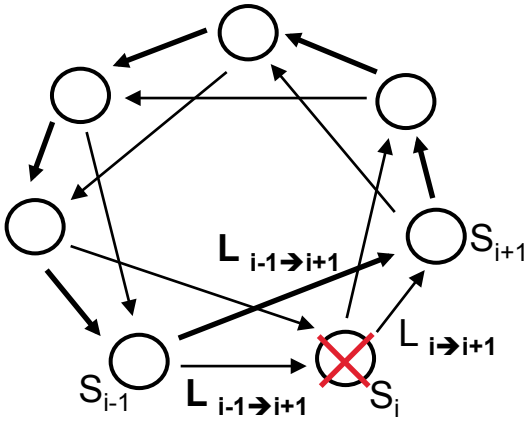
Fehlertoleranz durch abgeschwächte Anonymität im einzigen Betriebsmodus (Anonymitäts-Modus)

Fehlertoleranz durch extra Betriebsmodus (Fehlertoleranz-Modus)

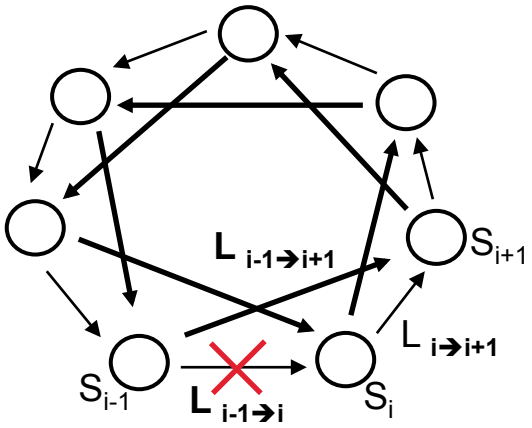
Geflochtener Ring



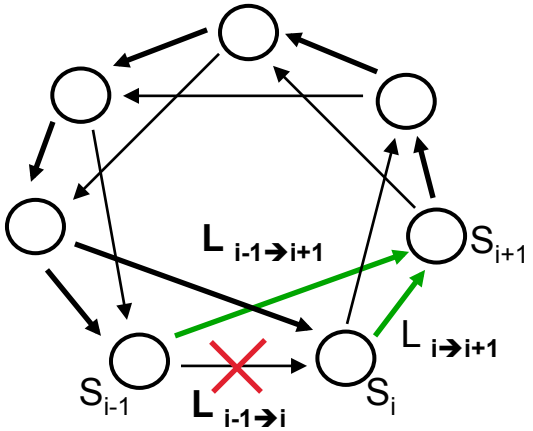
Betrieb zweier Ringe
sofern keine Ausfälle



Rekonfiguration des äußeren
Rings bei Ausfall einer Station



Rekonfiguration des inneren
Rings bei Ausfall einer äußeren
Leitung



Rekonfiguration des äußeren
Rings bei Ausfall einer äußeren
Leitung

genutzte Leitung

ungenutzte Leitung

genutzte Leitung, auf
der die Hälfte aller
Nachrichten
übertragen wird

Verändernde Angriffe

verändernde Angriffe auf

bei RING-Netz durch Angreifer-modell abgedeckt

Senderanonymität

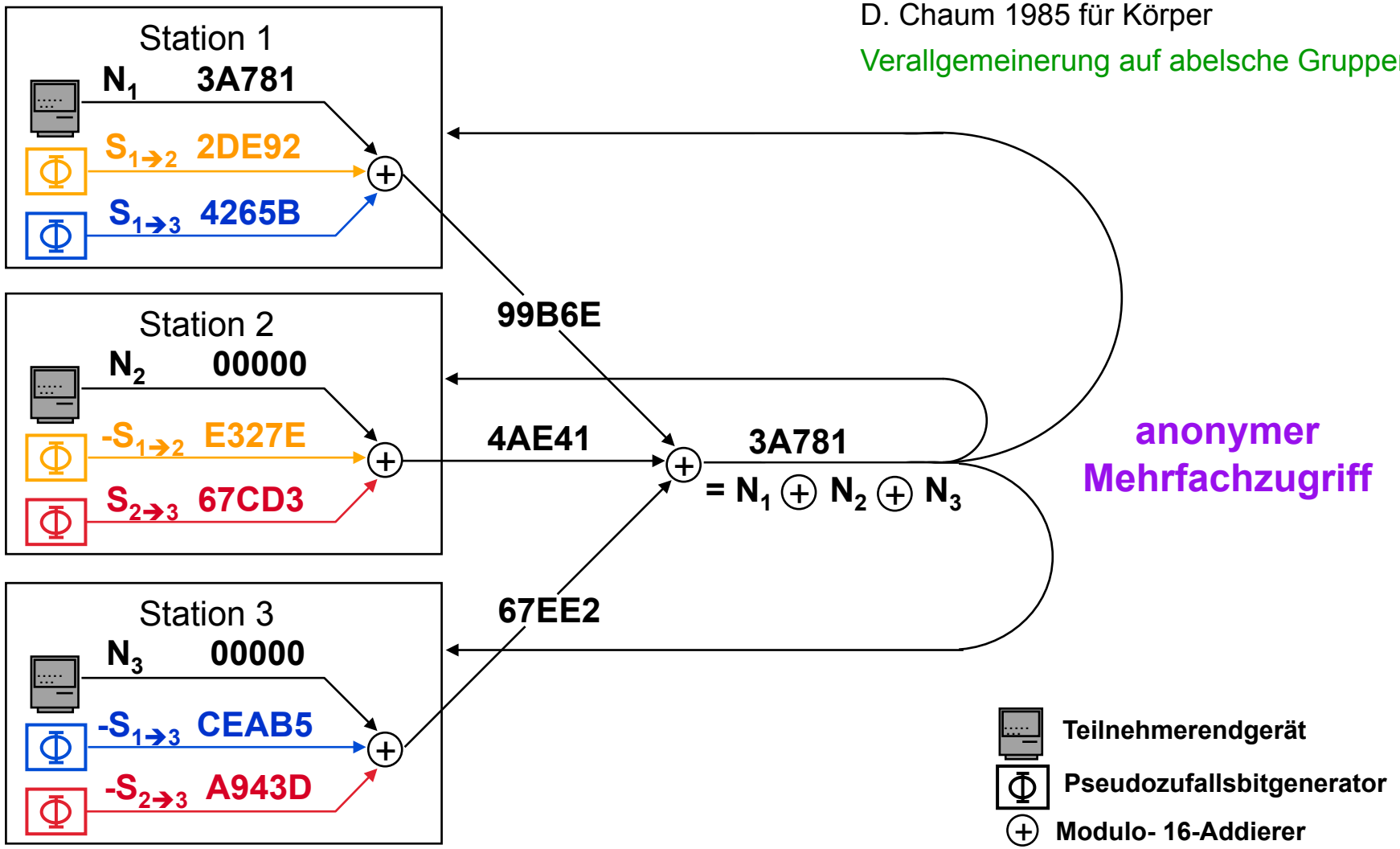
→ Zugriffsverfahren erweitern

Empfängeranonymität

Diensterbringung

Ein- und Ausgabe aufdecken
bei Disput rekonfigurieren

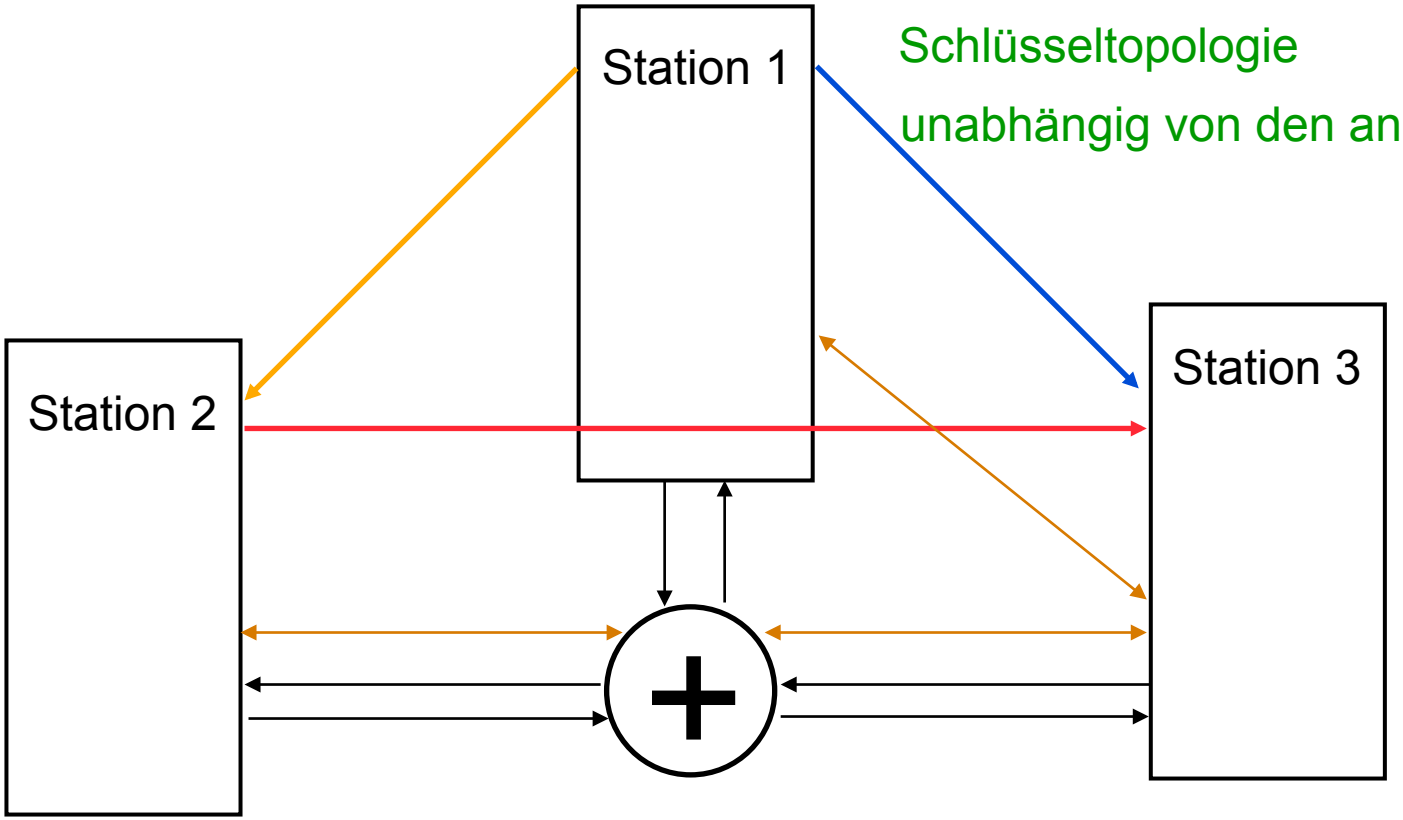
Überlagerndes Senden



Anonymität des Senders

Hängen Stationen durch geheime Schlüssel zusammen,
liefert Abhören aller Leitungen keine zusätzliche Information.

Drei zu unterscheidende Topologien



Schlüsseltopologie

unabhängig von den anderen

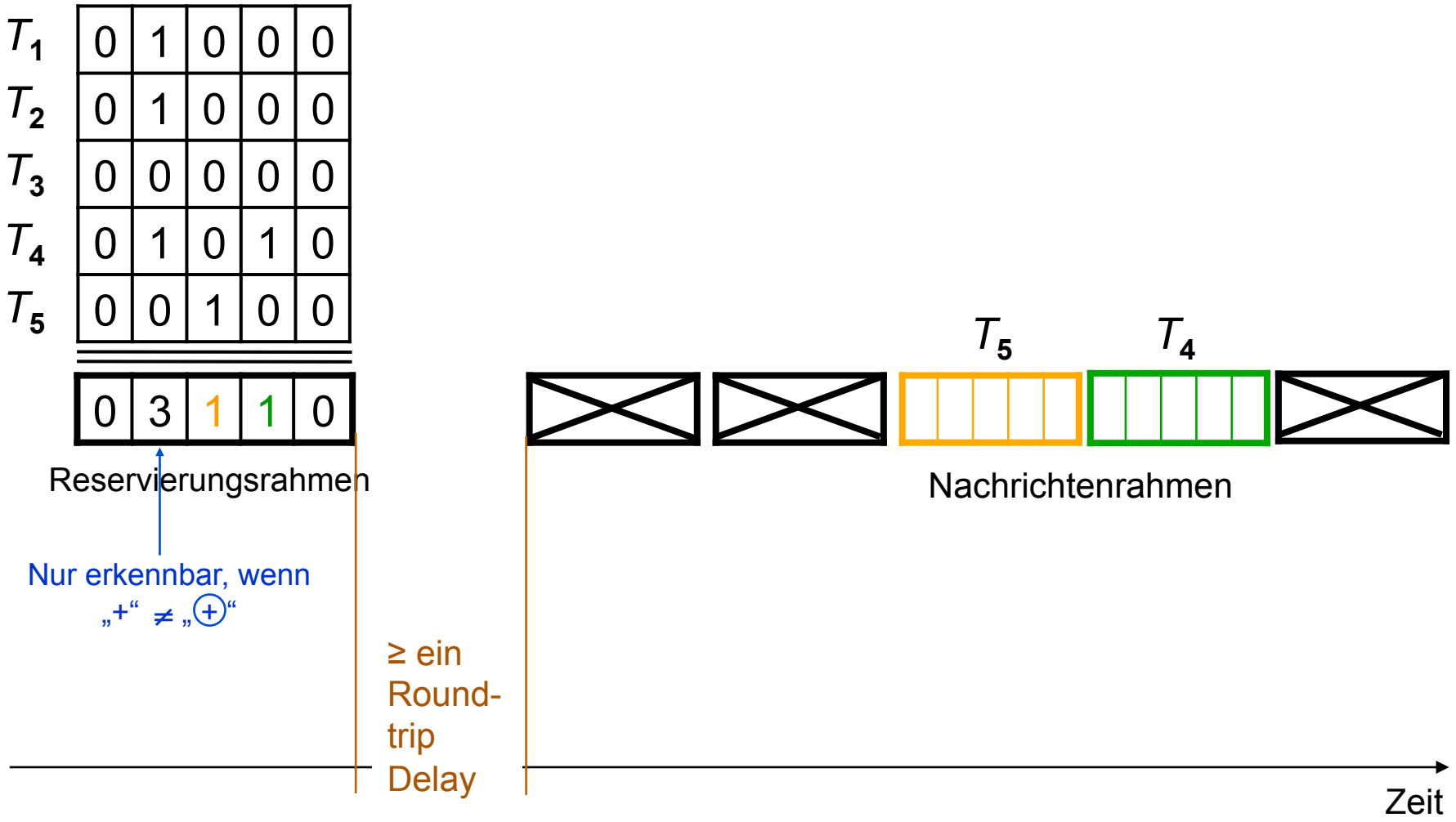
Überlagerungstopologie

Übertragungstopologie

abhängig

voneinander

Reservierungsverfahren



Überlagerndes Empfangen

Wer die Summe von *n* Zeichen sowie *n*-1 der *n* Zeichen kennt, kann das *n*-te Zeichen errechnen.

paarweises überlagerndes Empfangen (Reservierungsverfahren: $n=2$)

Zwei Stationen senden gleichzeitig.
Jede subtrahiert von der Summe ihr Zeichen, um das von der anderen gesendete Zeichen zu erhalten.
==> Duplex-Kanal in der Bandbreite eines Simplex-Kanals

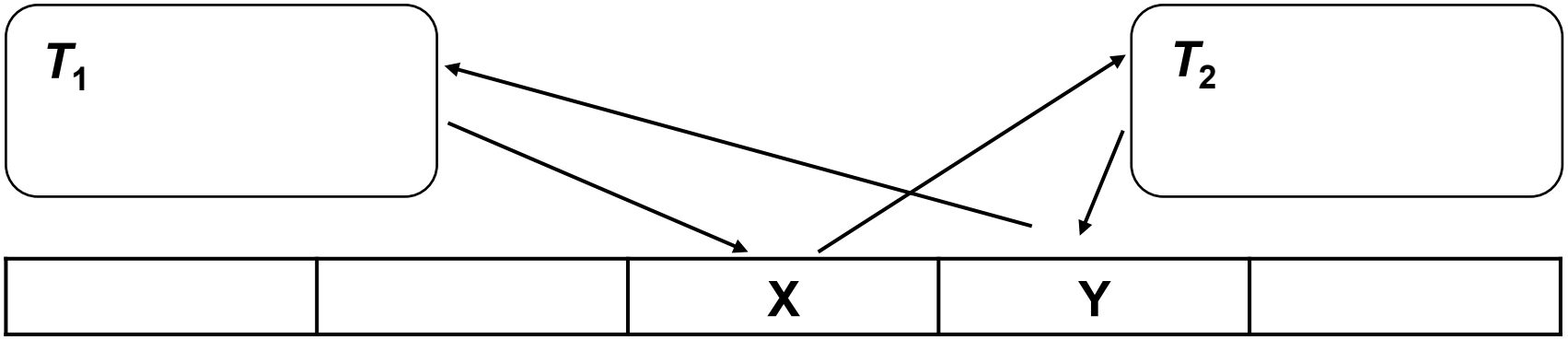
globales überlagerndes Empfangen (direkte Übertragung: $n \geq 2$)

Kollisionsergebnis wird gespeichert, so dass bei *n* kollidierten Paketen nur *n*-1 noch einmal gesendet werden müssen.

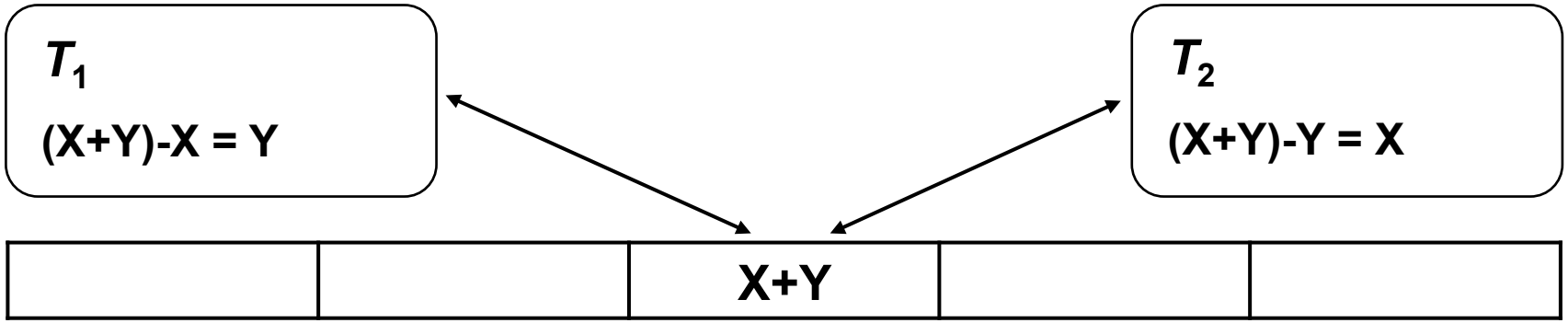
Kollisionsauflösungsalgorithmus mit Mittelwertbildung:

$\leq 2^T - 1$ Teilnehmer Addition mod 2^L

Paarweises überlagerndes Empfangen

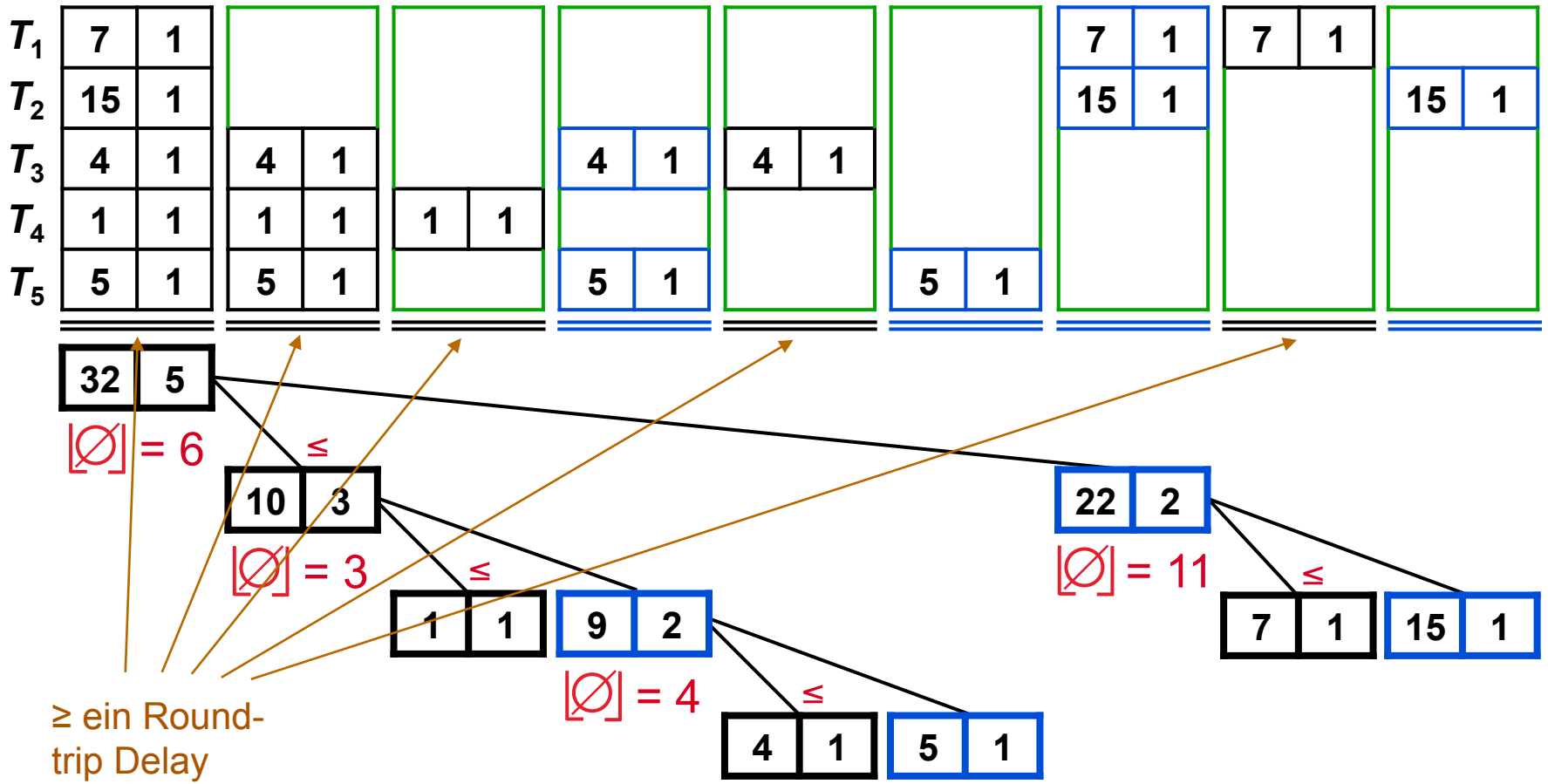


ohne überlagerndes Empfangen



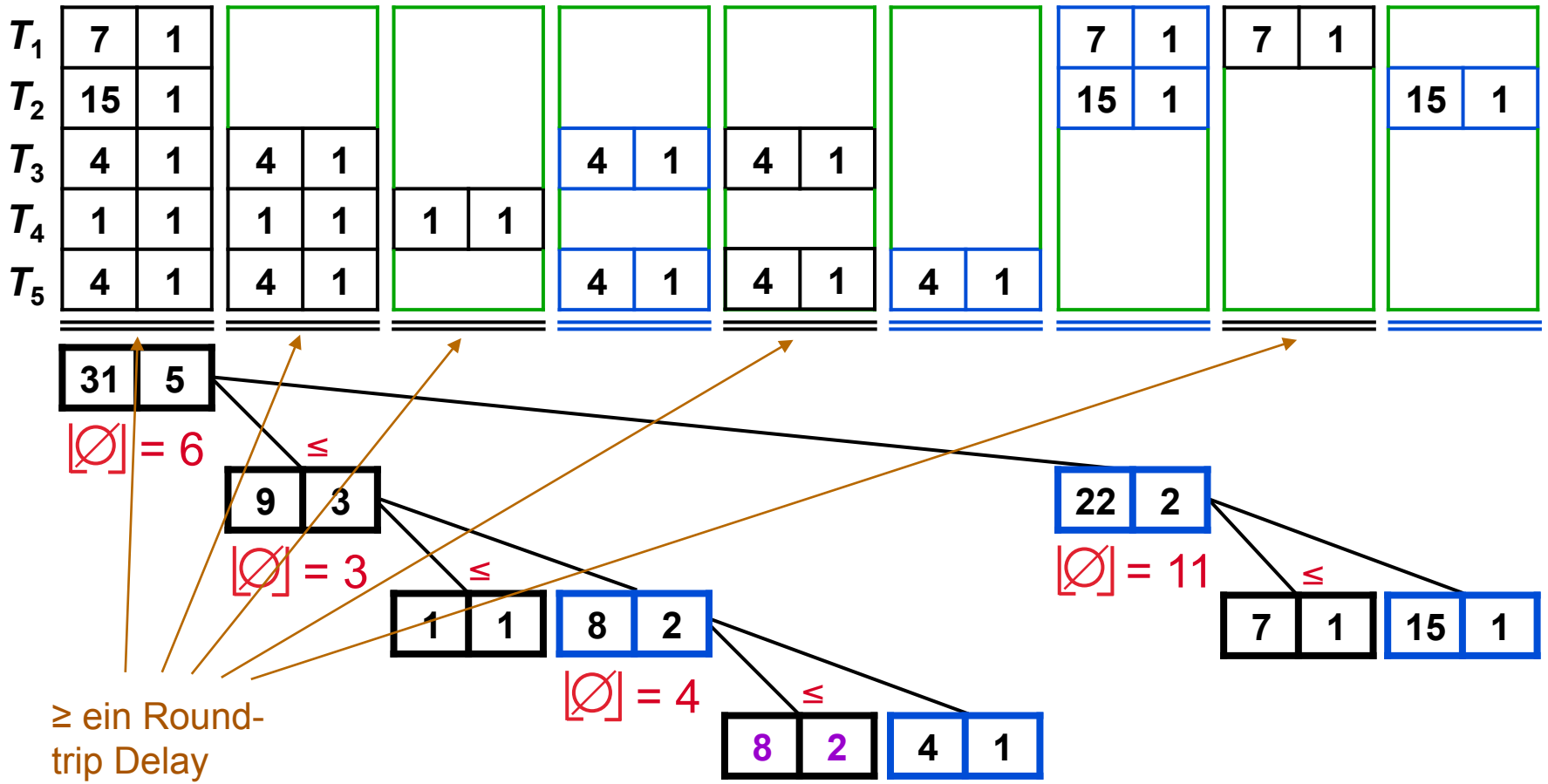
mit paarweisem überlagerndem Empfangen

Globales überlagerndes Empfangen



Kollisionsauflösungsalgorithmus mit Mittelwertbildung und überlagerndem Empfangen

Globales überlagerndes Empfangen (2 Nachrichten gleich)

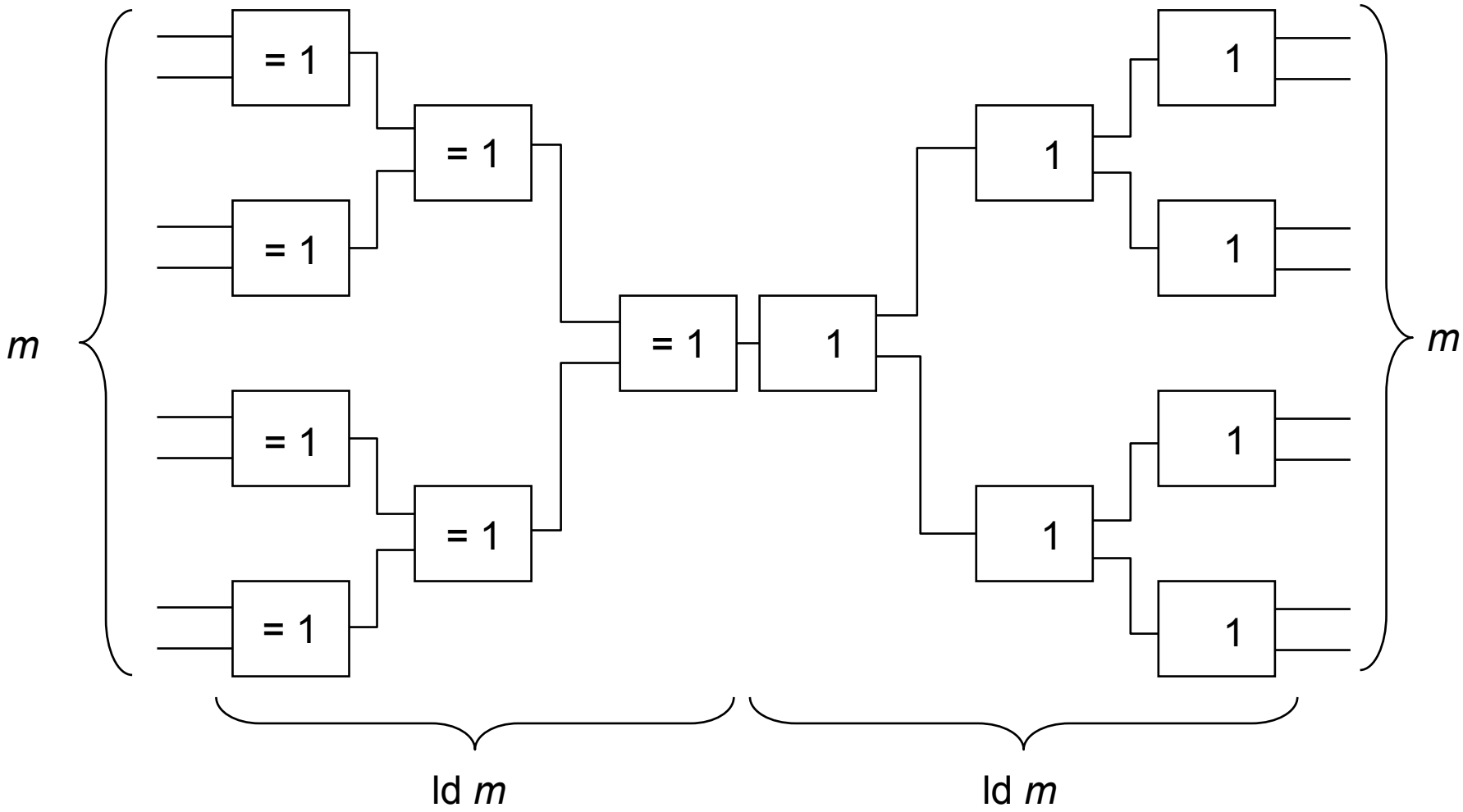


Kollisionsauflösungsalgorithmus mit Mittelwertbildung und überlagerndem Empfangen

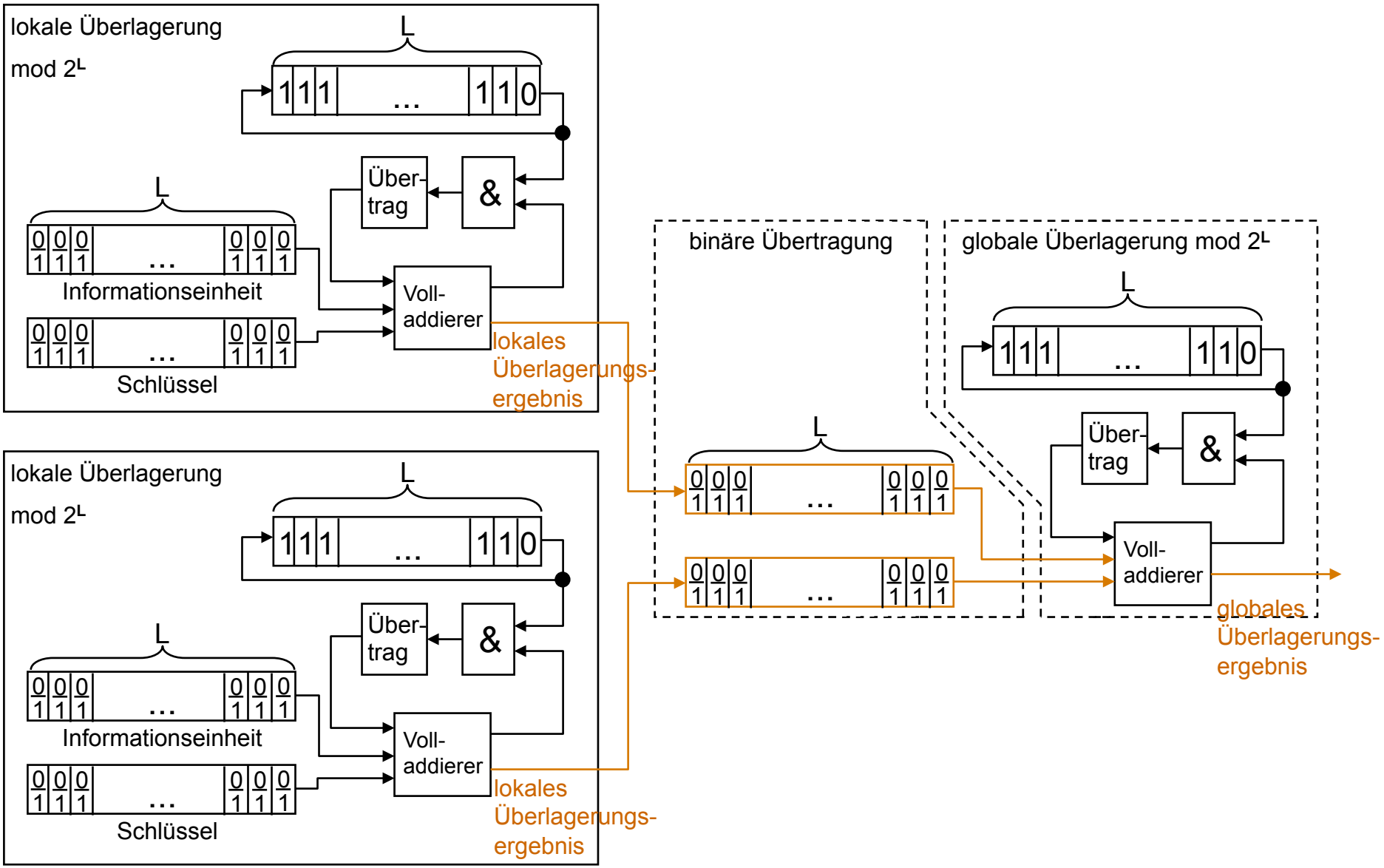
Verzögerungszeitminimale Überlagerungstopologie

Baum von XOR-Gattern zur Überlagerung der Ausgaben der Teilnehmerstationen

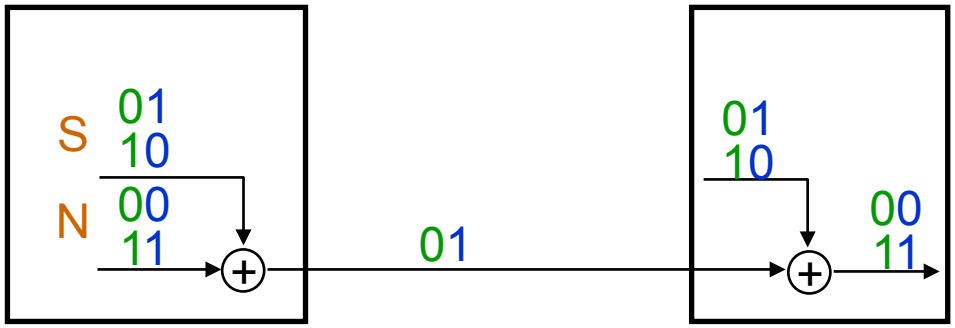
Baum von Verstärkern zur Vervielfachung der Ausgabe an die Teilnehmerstationen



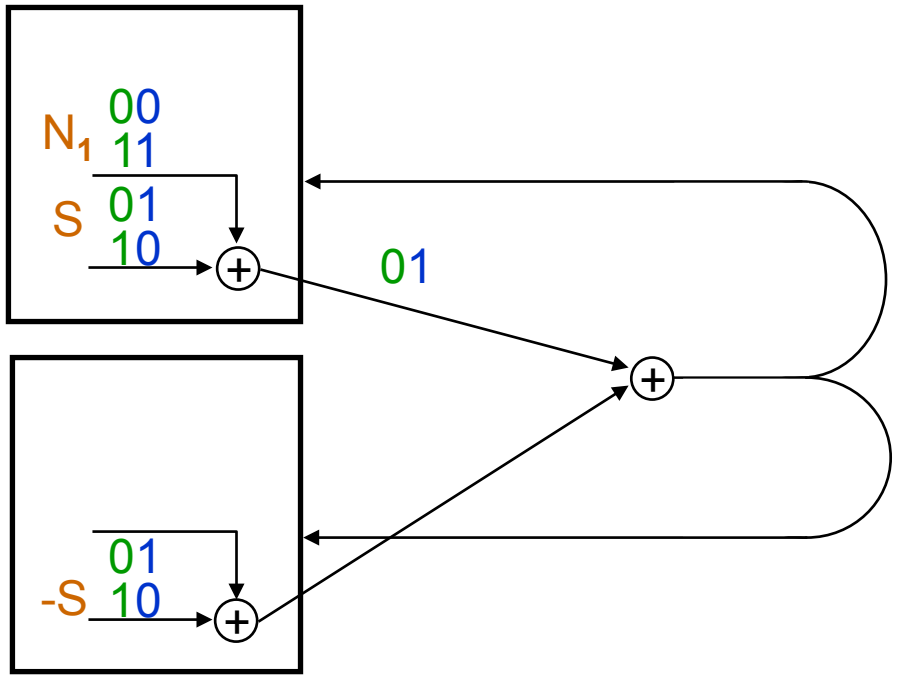
Geeignete Codierung beim überlagernden Senden



Analogie zwischen Vernam-Chiffre und überl. Senden



$S + N = C \Leftrightarrow N = C - S$ abelsche Gruppe



$N_1 + S = A_1$

$N_2 - S = A_2$

Beweis der Senderanonymität: Beh. und Induktionsanfang

Beh.:

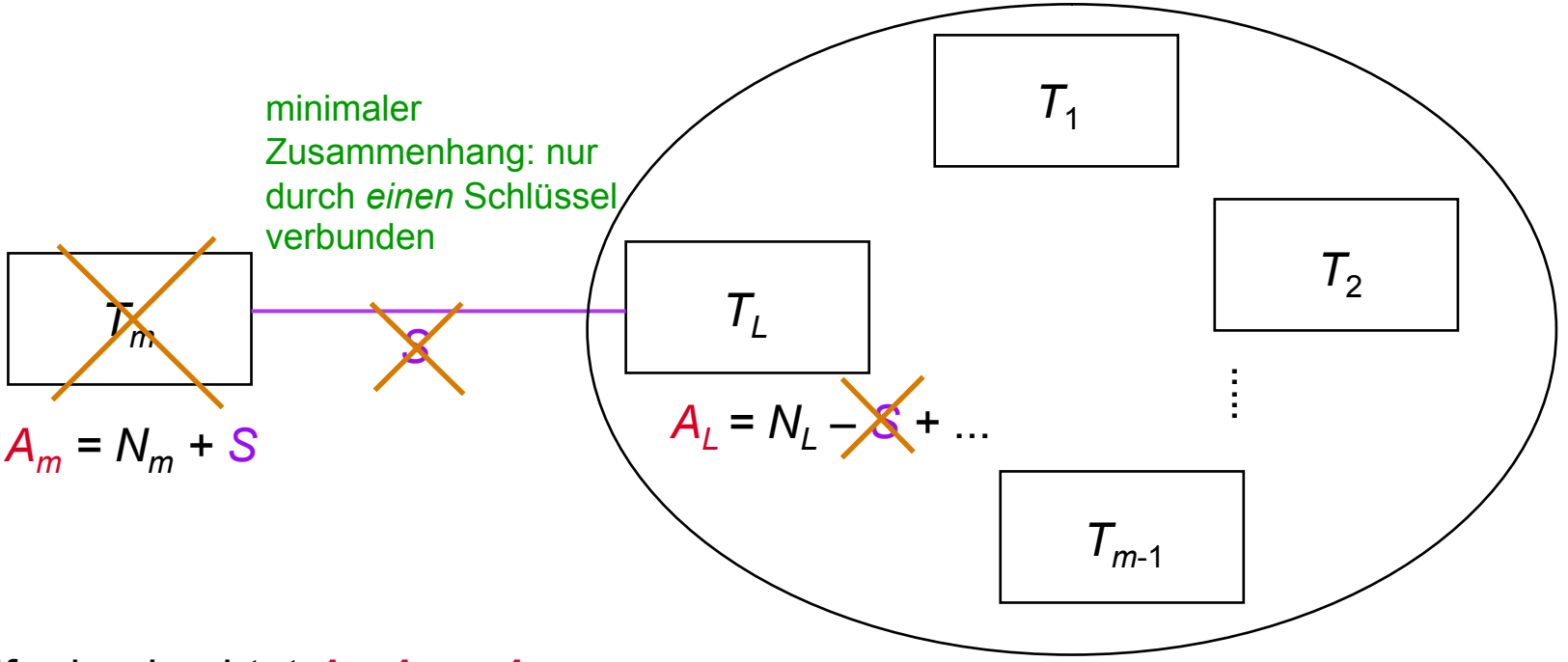
Hängen Stationen T_i über zufällig gleichverteilte, dem Angreifer unbekannte Schlüssel S_j zusammen, so erfährt er durch Beobachtung der A_i über die N_i nur $\sum_i N_i$

Bew.:

m=1, trivial

Schritt m-1 ➔ m

Beweis der Senderanonymität: Induktionsschritt



Angreifer beobachtet $A_1, A_2, \ldots A_m$.

Zu jeder Nachrichtenkombination $N'_1, N'_2, \ldots N'_m$

mit $\sum_{i=1}^{m} N'_i = \sum_{i=1}^{m} A_i$ gibt es genau eine passende Schlüsselkombination: $S' := A_m - N'_m$

Rest wie in Induktionsvoraussetzung, wobei als Ausgabe von T_L der Wert $A_L + S'$ verwendet wird.

Informationstheoretische Anonymität trotz verändernder Angriffe

Probleme:

1) Angreifer sendet Nachricht nur an manche Teilnehmer. Falls er eine Antwort erhält, war der Adressat unter diesen Teilnehmern.

2) Um einen verändernden Angriff auf die Dienstbringung ahnden zu können, müssen gestörte Nachrichten aufgedeckt werden können. Dies darf aber *nicht* für bedeutungsvolle Nachrichten protokolltreuer Teilnehmer gelten.

DC⁺-Netz zum Schutz des Empfängers gegen verändernde Angreifer: bei Verteilungsfehler gleichverteilte Schlüsseländerung

Schlüssel zwischen Station *i* und *j* für Zeitpunkt *t*

an Station *i* zum Zeitpunkt *t* verteiltes Zeichen

(Schief-) Körper

$$S_{ij}^{t} = a_{ij}^{t} + \sum_{k=t-s}^{t-1} b_{ij}^{t-k} \bullet V_i^{k}$$

Aus praktischen Gründen:
Jede Station muss alle *s* Zeitpunkte kollisionsfrei eine zufällige Nachricht senden und beobachten, ob sie „richtig“ verteilt wird.

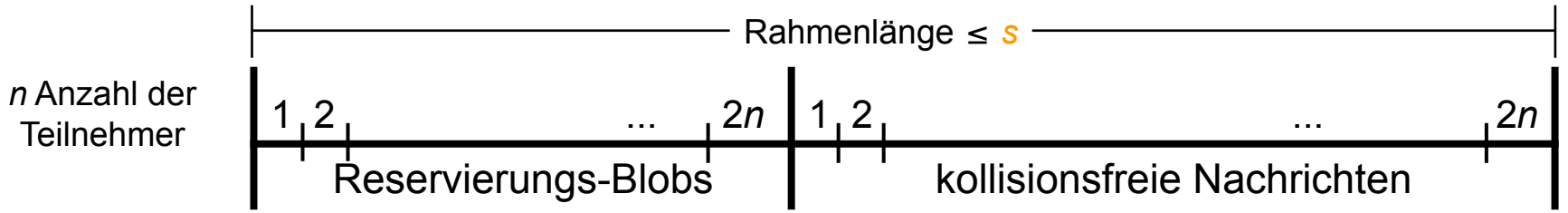
Beim Aufdecken von S_{ij}^{t} wird mit $V_i^{t-s},\ldots, V_i^{t-1}$ begonnen.

Bei Disput Abbruch dieses Aufdeckens. Ggf. neue $b_{ij}^{1},\ldots, b_{ij}^{s}$.

Sei zum Zeitpunkt $t\text{-}s$ erstmals $V_i^{t-s} \neq V_j^{t-s}$.

$$\begin{pmatrix} S_{ij}^{t+1-s} - S_{ji}^{t+1-s} \\ S_{ij}^{t+2-s} - S_{ji}^{t+2-s} \\ \vdots \\ S_{ij}^{t} - S_{ji}^{t} \end{pmatrix} = \begin{pmatrix} V_i^{t-s} - V_j^{t-s} & 0 & \cdots & 0 \\ V_i^{t+1-s} - V_j^{t+1-s} & V_i^{t-s} - V_j^{t-s} & & 0 \\ & & \ddots & \vdots \\ V_i^{t-1} - V_j^{t-1} & V_i^{t-2} - V_j^{t-2} & \cdots & V_i^{t-s} - V_j^{t-s} \end{pmatrix} \begin{pmatrix} b_{ij}^1 \\ b_{ij}^2 \\ \vdots \\ b_{ij}^s \end{pmatrix}$$

Schutz des Senders: Anonymes Fallen-Protokoll



- Jeder Teilnehmer kann direkt nach den Reservierungs-Blobs deren Aufdecken veranlassen, sofern das Senden seiner Reservierungs-Blobs nicht geklappt hat.
- Jeder Teilnehmer kann das Aufdecken seiner „kollisionsfreien“ zufälligen Nachricht veranlassen, indem er den zugehörigen Reservierungs-Blob passend öffnet.

Blob := Festlegung auf 0 oder 1, ohne den Wert zu verraten.

1) Der sich Festlegende darf den Wert nicht ändern und muß ihn aufdecken können.

2) Die anderen sollten keine Information über den Wert erhalten.

In einer „digitalen“ Welt geht genau eins ohne, das andere erfordert jeweils komplexitätstheoretische Annahmen.

Bsp:

Gegeben Primzahl *p* und die Primfaktoren von *p* -1, sowie ein Generator α von Z^*_p (multiplikative Gruppe mod *p*). Aus *y* kann jeder $\alpha^y \bmod p$ berechnen.

Umkehrung ist *nicht* effizient durchführbar!

1?

$S \in Z^*_p$ zufällig gewählt
(d.h. der sich Festlegende kann kein *e* berechnen, für das $s \equiv \alpha^e$ gilt)

$x := s^b \alpha^y \bmod p$ mit $0 \le y \le p\text{-}2$

Festlegen $\xrightarrow{x}$

Aufdecken $\xrightarrow{y}$

2?

Sei 2^u die kleinste Zahl, die *p* -1 nicht teilt

$y := y_1, b, y_2$ mit $0 \le y \le p\text{-}2$ und $|y_2| = u - 1$

$x := \alpha^y \bmod p$

Festlegen $\xrightarrow{x}$

Aufdecken $\xrightarrow{y}$

Blobs basierend auf Faktorisierungsannahme

1?

$n := p \cdot q$

$s := t^2 \bmod n$

n, s ←

$s \in QR_n$ ↔

festlegen

$x := y^2 s^b \bmod n$

x →

aufdecken

y →

2?

$n := p \cdot q$

$s \notin QR_n$, $\left(\frac{s}{n}\right) = 1$

n, s →

$n = p \cdot q$, $s \notin QR_n$ ↔

$x := y^2 s^b \bmod n$

x →

y →

Blobs basierend auf asymmetrischem Konzelationssystem

2?

Verschlüssele *b* mit asymmetrischem Konzelationssystem (zur Erinnerung: Der öffentliche Schlüssel und der Schlüsseltext zusammen legen den Klartext eindeutig fest)

- muss probabilistisch sein, denn das Raten und Durchprobieren des Klartextes ist sonst kinderleicht
- Mitteilen der für die probabilistische Verschlüsselung verwendeten Zufallszahl ist das Aufdecken des Blobs
- komplexitätstheoretisch unbeschränkte Angreifer können *b* errechnen (da sie jedes asymmetrische Konzelations-system brechen können)

Verändernde Angriffe

Verändernde Angriffe auf

- Senderanonymität
- Empfängeranonymität
- Diensterbringung

  Angreifer sendet Nutzzeichen ≠ 0,

  wenn andere ihr Nutzzeichen übertragen

  ➔ keine Übertragung von Nutzinformation

Um einen verändernden Angriff auf die Diensterbringung ahnden zu können, müssen gestörte Nachrichten aufgedeckt werden können. Dies darf aber *nicht* für bedeutungsvolle Nachrichten protokolltreuer Teilnehmer gelten.

Kontrolle des Verhaltens der Stationen

Zur Kontrolle einer Station muss bekannt sein:

- alle Schlüssel mit anderen
- ihre Ausgabe
- alle von ihr erhaltenen globalen Überlagerungsergebnisse
- wann durfte sie nach Zugriffsprotokoll Nutzzeichen senden?
  (Ergibt sich anhand der globalen Überlagerungsergebnisse der letzten Runden; diese können aus den jeweiligen lokalen Ausgaben errechnet werden)

bekannt = *allen* protokolltreuen Stationen bekannt

Verändernde Angriffe in der Reservierungsphase

Kollisionen in der Reservierungsphase

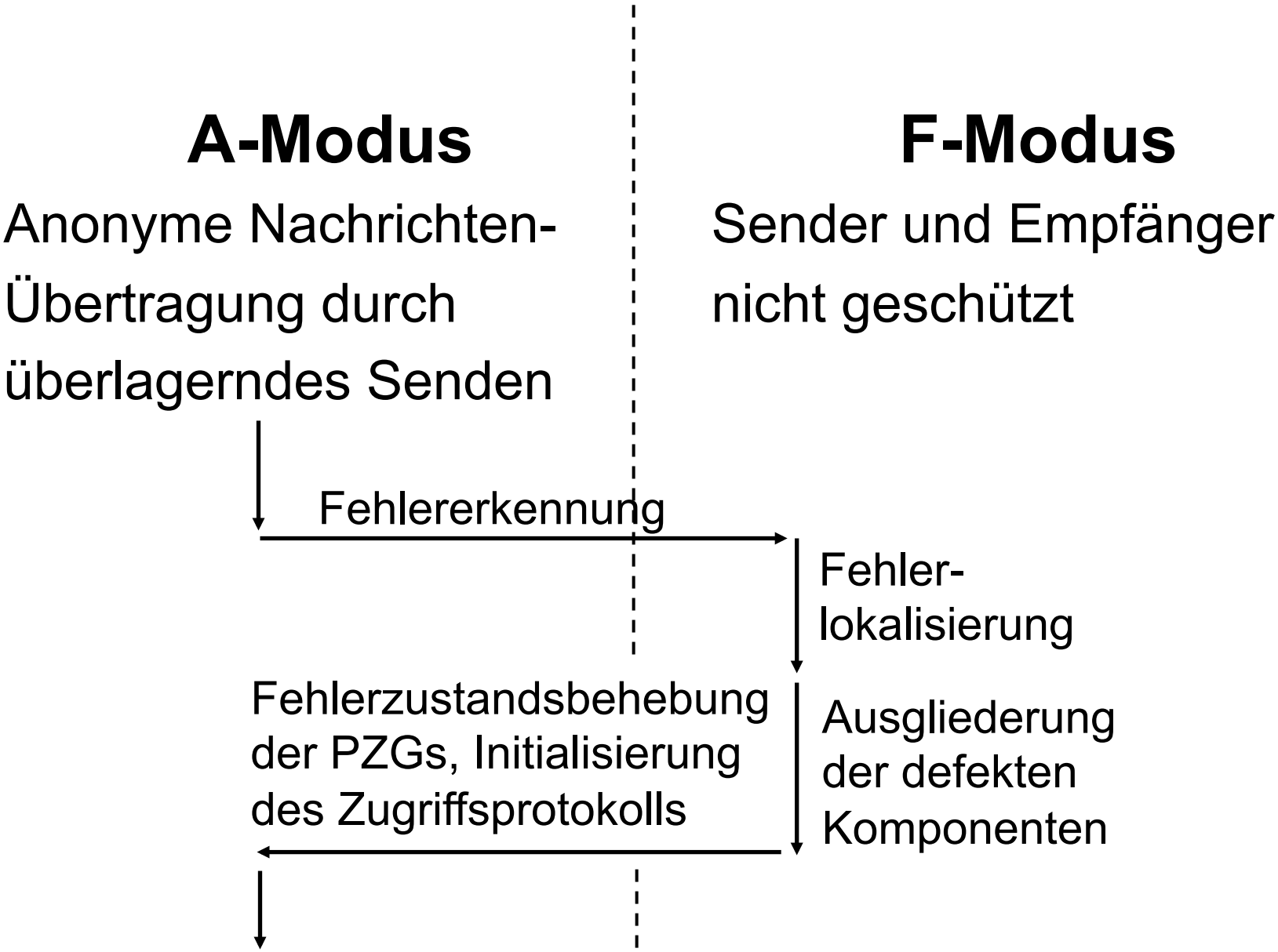
- sind immer möglich
- können deshalb *nicht* als Angriff geahndet werden

Problem: A könnte Ausgaben der protokolltreuen Stationen abwarten und dann seine so wählen, dass Kollisionen entstehen.

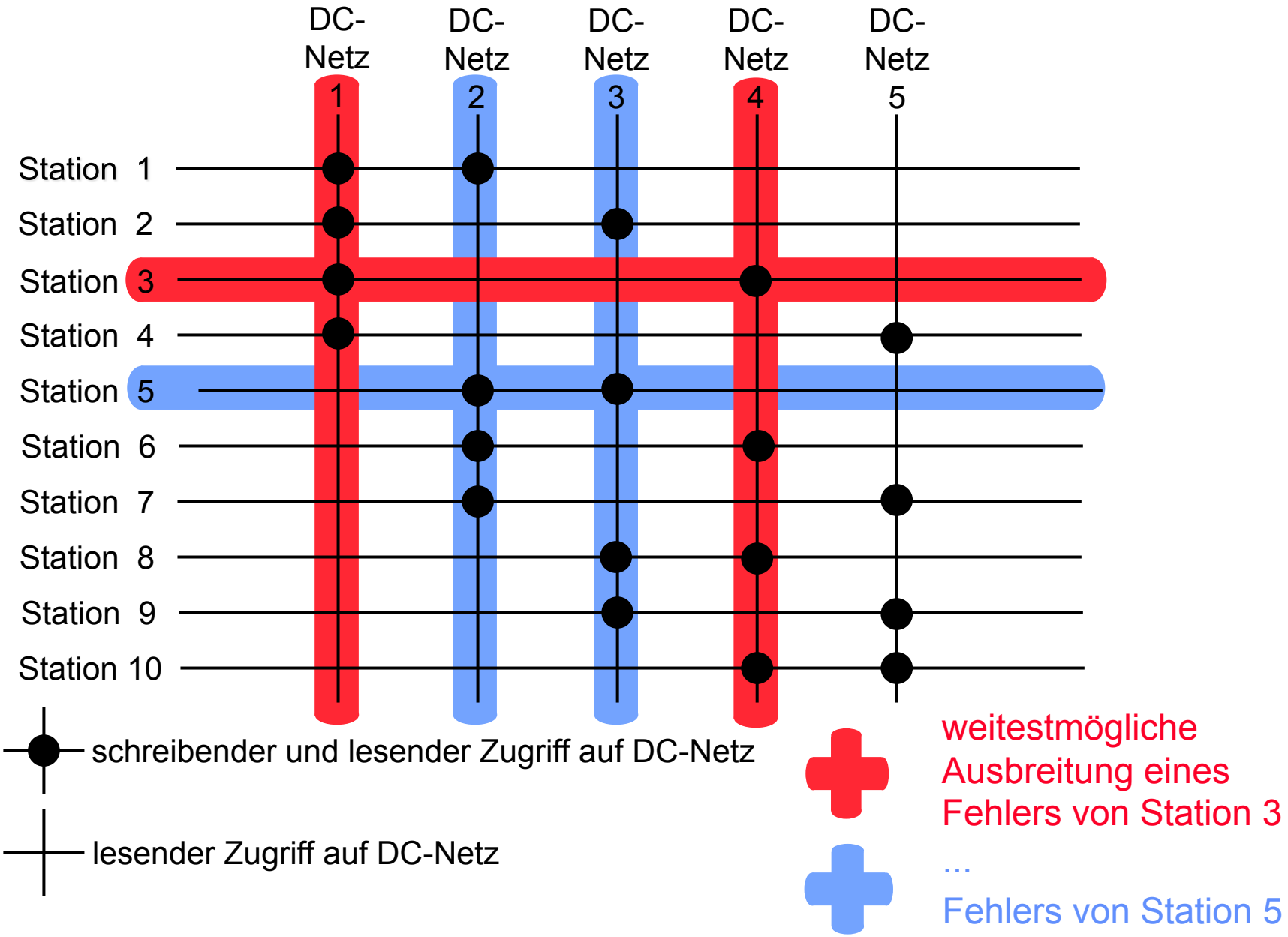
Lösung: Jede Station

1. legt sich zuerst mittels Blob auf ihre Ausgabe fest,
2. erwartet Blobs aller anderen,
3. deckt ihren Blob auf.

Fehlertoleranz: 2 Betriebsmodi

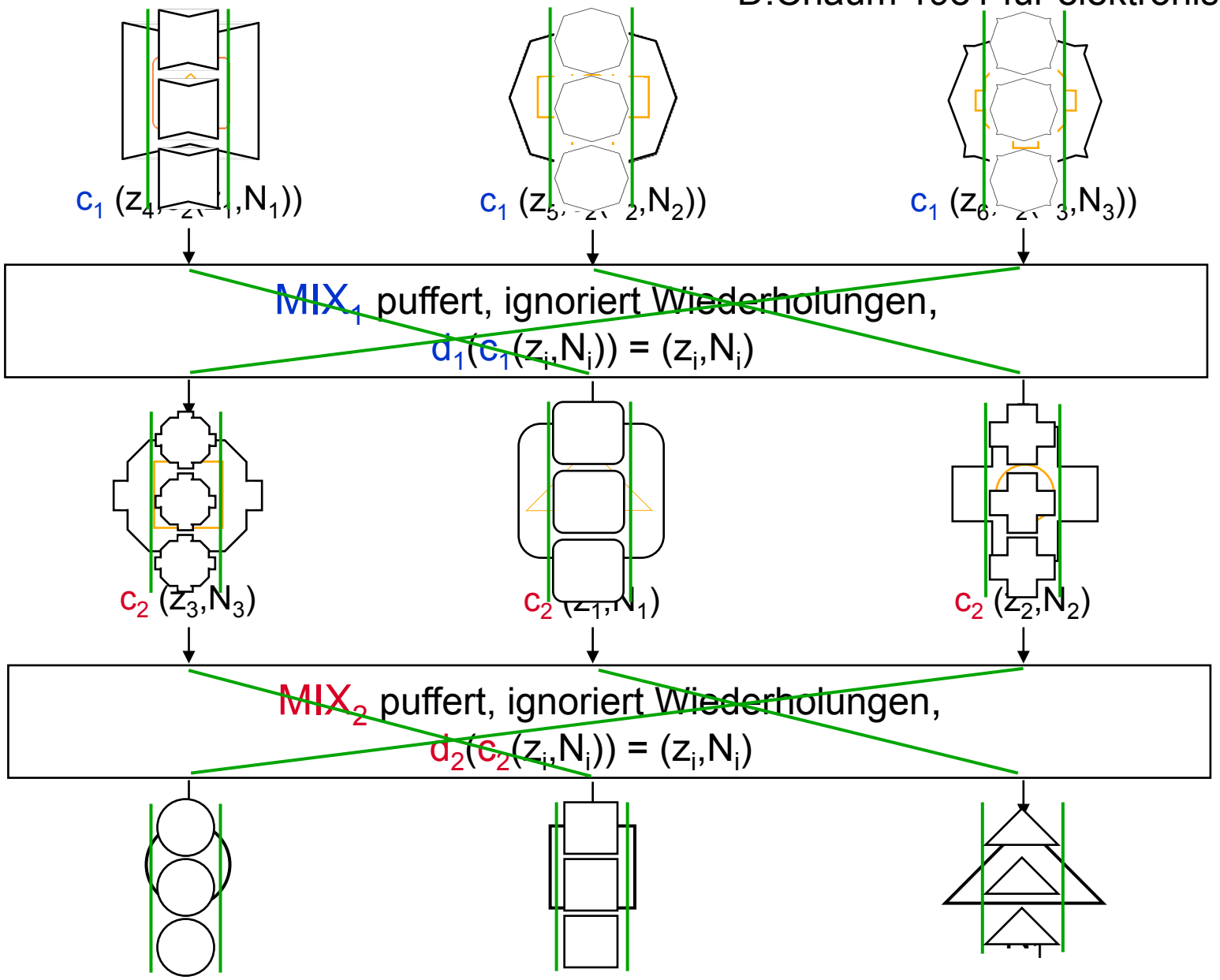


Fehlertoleranz: senderpartitioniertes DC-Netz

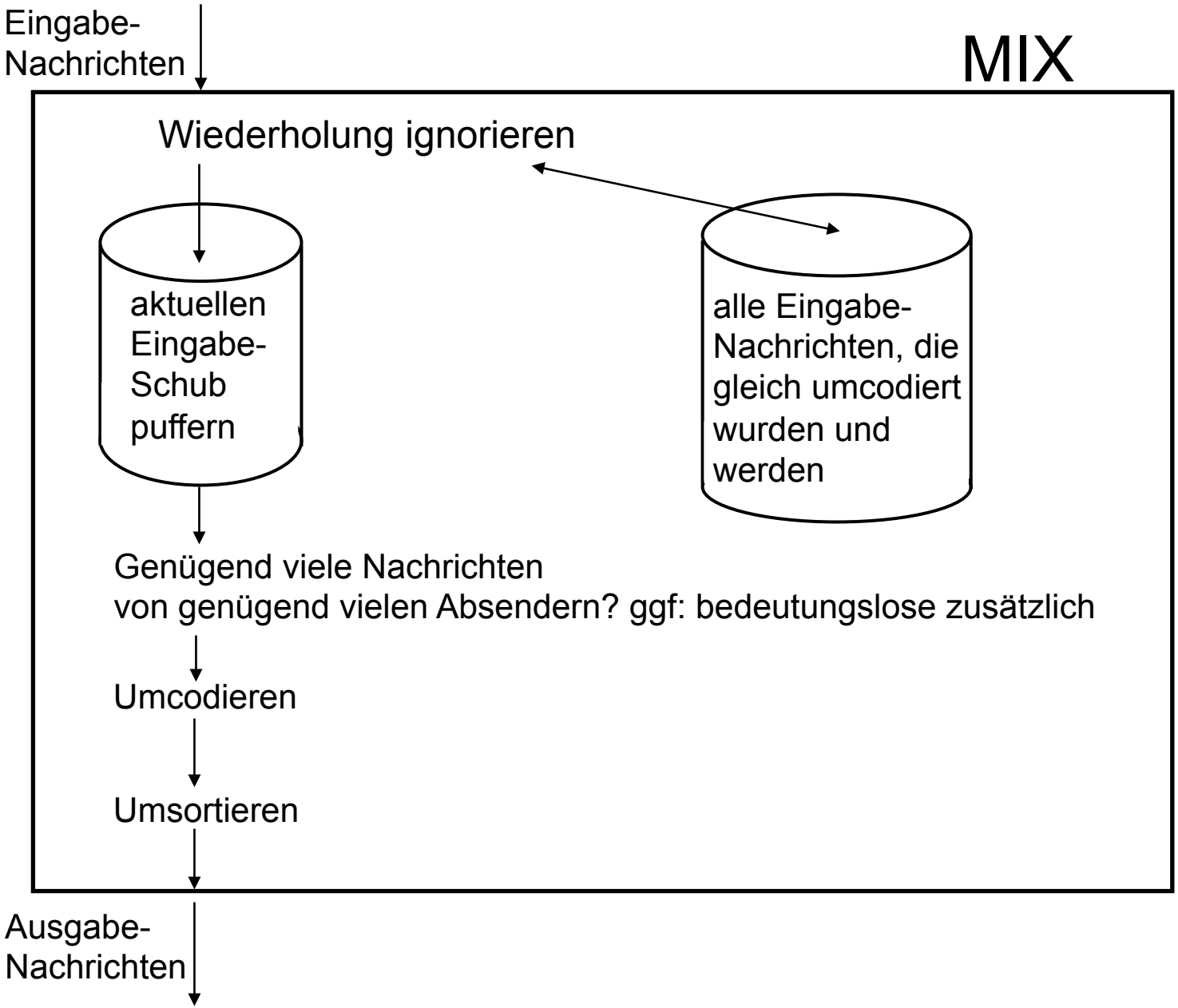


Schutz der Kommunikationsbeziehung: MIXe

D.Chaum 1981 für elektronische Post



Grundfunktionen eines MIXes



	min	max
1 Platten-zugriff	10 ms	50 ms
	nichts tun 0 ms	dig. Sig. prüfen 100 ms
	asym. Konz. spez. HW 1 ms	asym. Konz. SW 100 ms
	1 ns	10 µs
	11,000001 ms	250,01 ms

Eigenschaften von MIXen

MIXe unabhängig
- entworfen
- hergestellt
- betrieben
- gewartet ...

Nachrichten gleicher Länge
- puffern
- umcodieren
- umsortieren

} schubweise

Jede Nachrichten nur einmal!
- innerhalb eines Schubes
- zwischen Schüben

sym. Konzelationssystem nur für
- ersten
- letzten

} MIX

asym. Konzelationssystem notwendig
- für mittlere MIXe

Möglichkeiten und Grenzen des Umcodierens

Ziel: (ohne dummy traffic)

Kommunikationsbeziehung kann gegen den Willen von Sender oder Empfänger nur durch

- *alle* anderen Sender und Empfänger gemeinsam oder
- *alle* durchlaufenen MIXe gemeinsam

aufgedeckt werden.

Folgerungen:

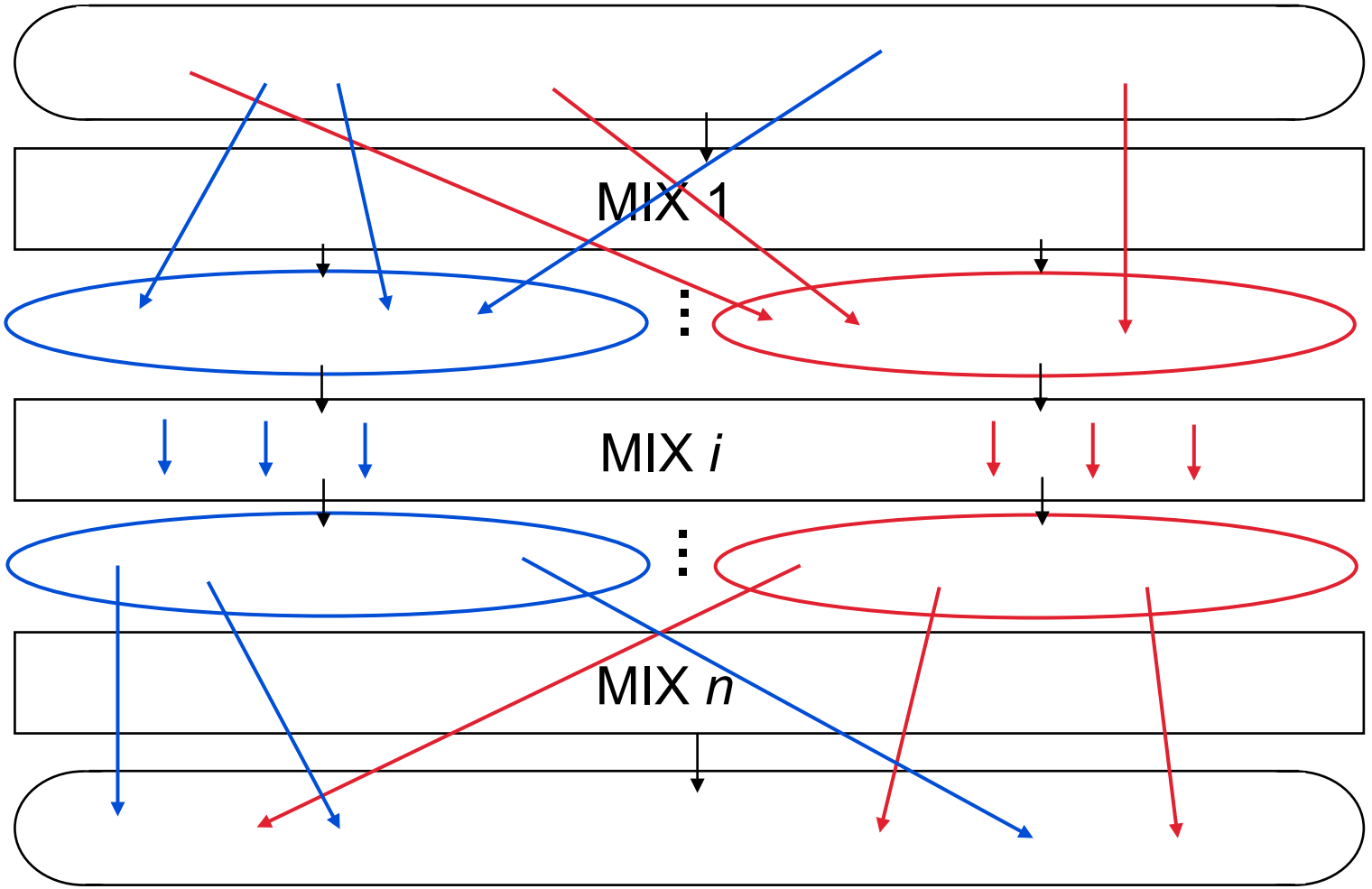
1. Umcodierung: nie Ver- gefolgt von Entschlüsselung

   Begr. Ver- und Entschlüsselung notwendigerweise mit passendem Schlüssel;
   ➔ davor und danach gleich ➔ Umcodierung ist irrelevant

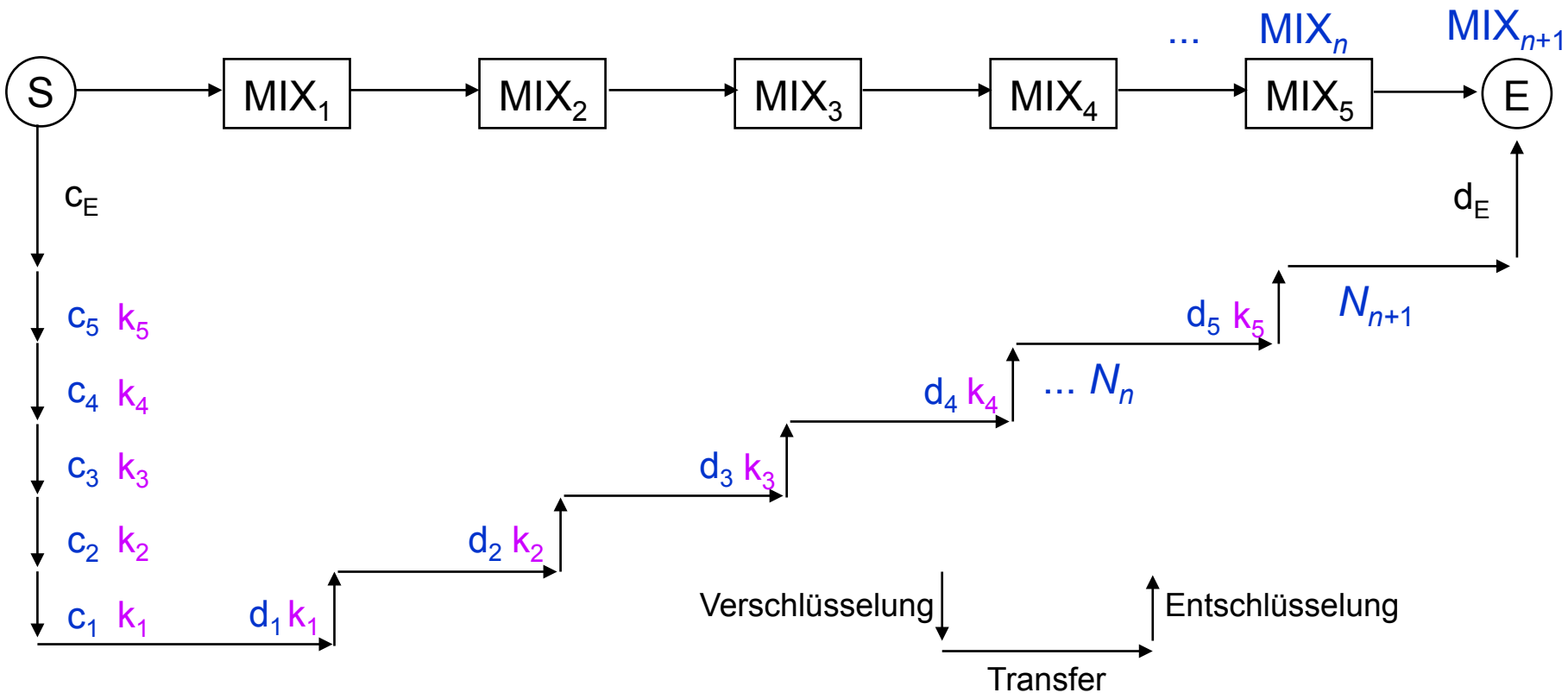
2. Maximaler Schutz:
   MIXe gleichzeitig und deshalb in gleicher Reihenfolge durchlaufen

Maximaler Schutz

MIXe in gleicher Reihenfolge durchlaufen



Umcodierungsschema für Senderanonymität



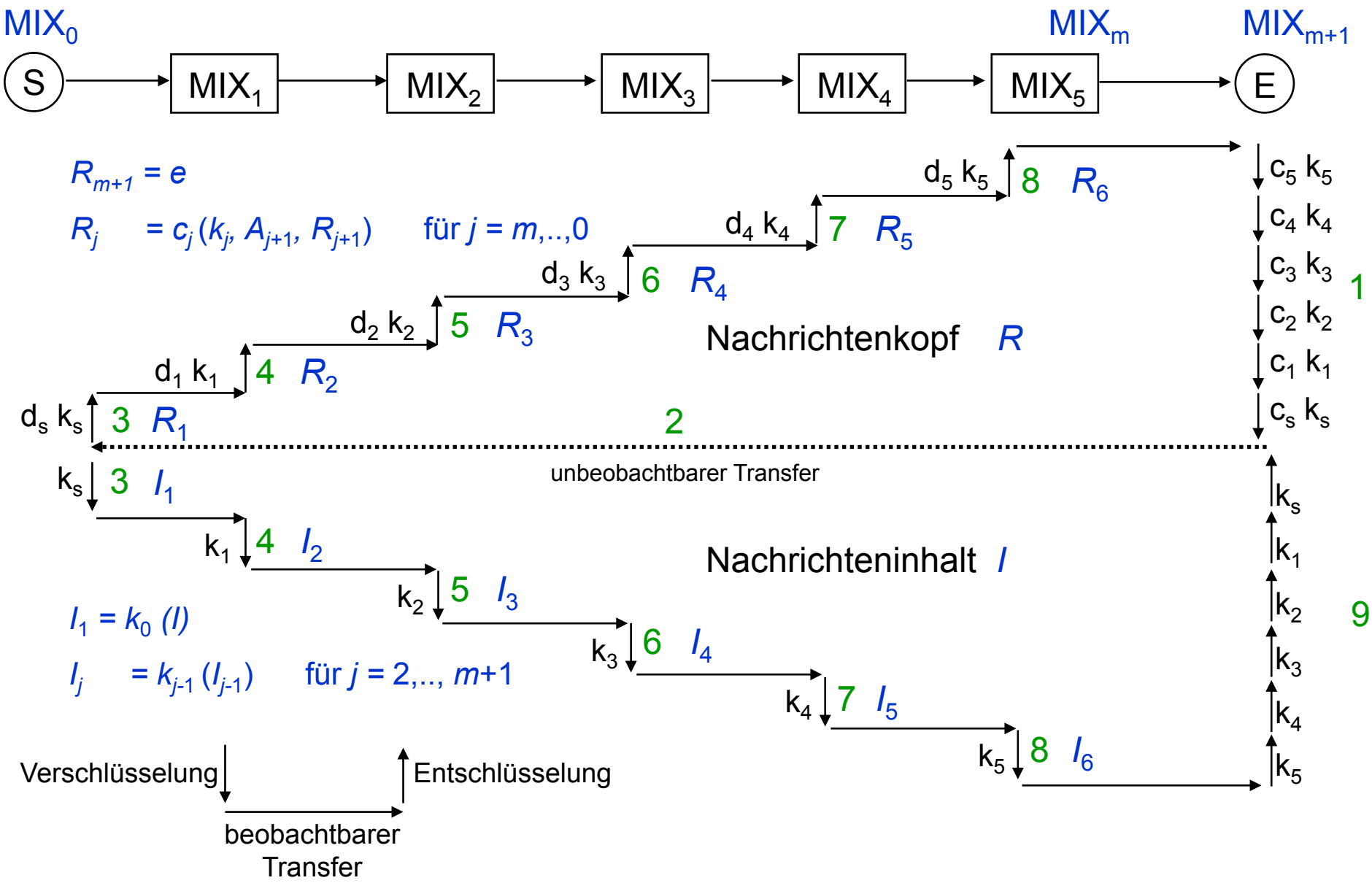
indirektes Umcodierungsschema für Senderanonymität

$N_{n+1} = c_{n+1}(N)$

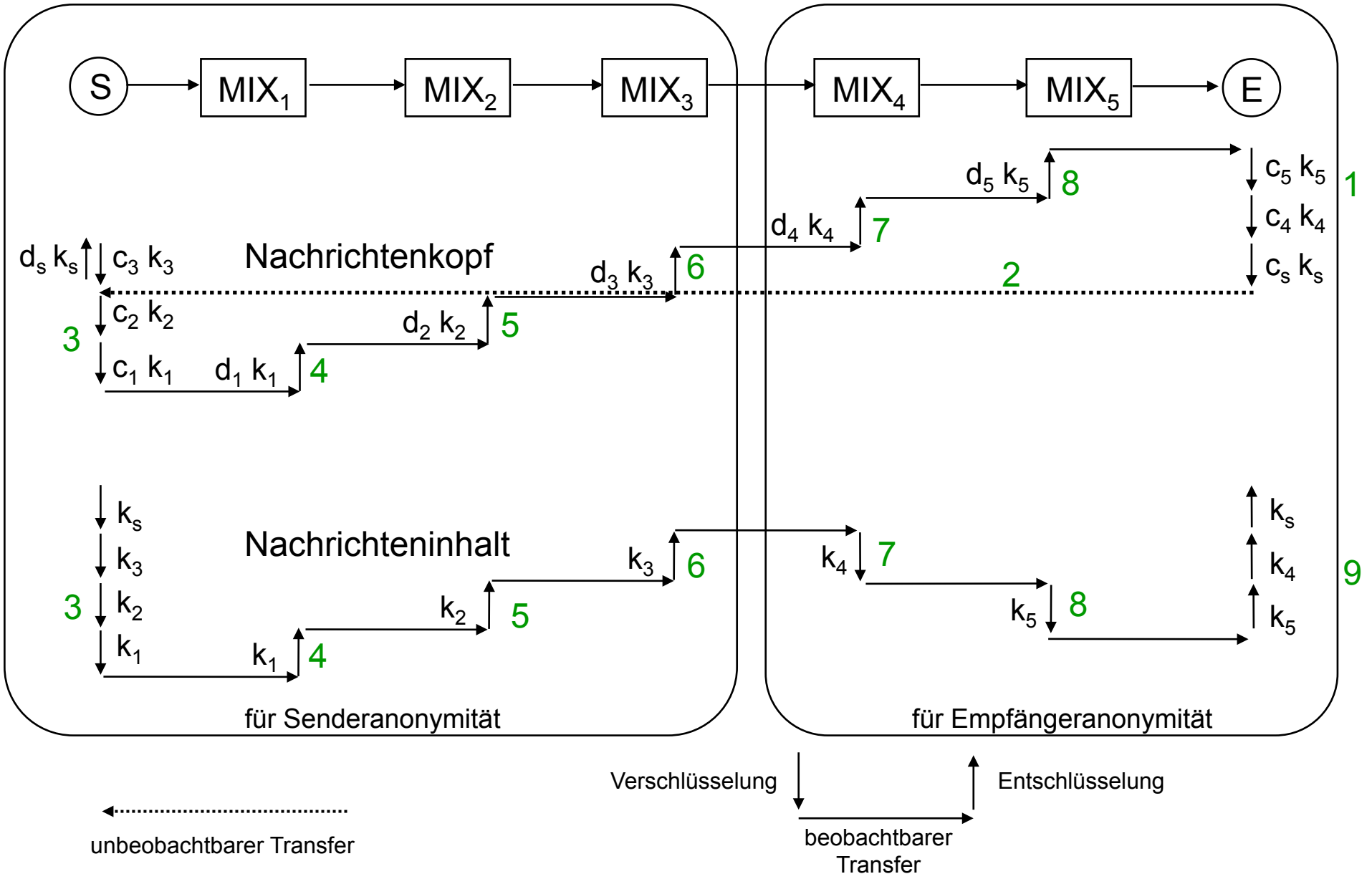
$N_i = c_i(z_i, A_{i+1}, N_{i+1})$ für $i = n,..,1$

$N_i = c_i(k_i, A_{i+1}); k_i(N_{i+1})$

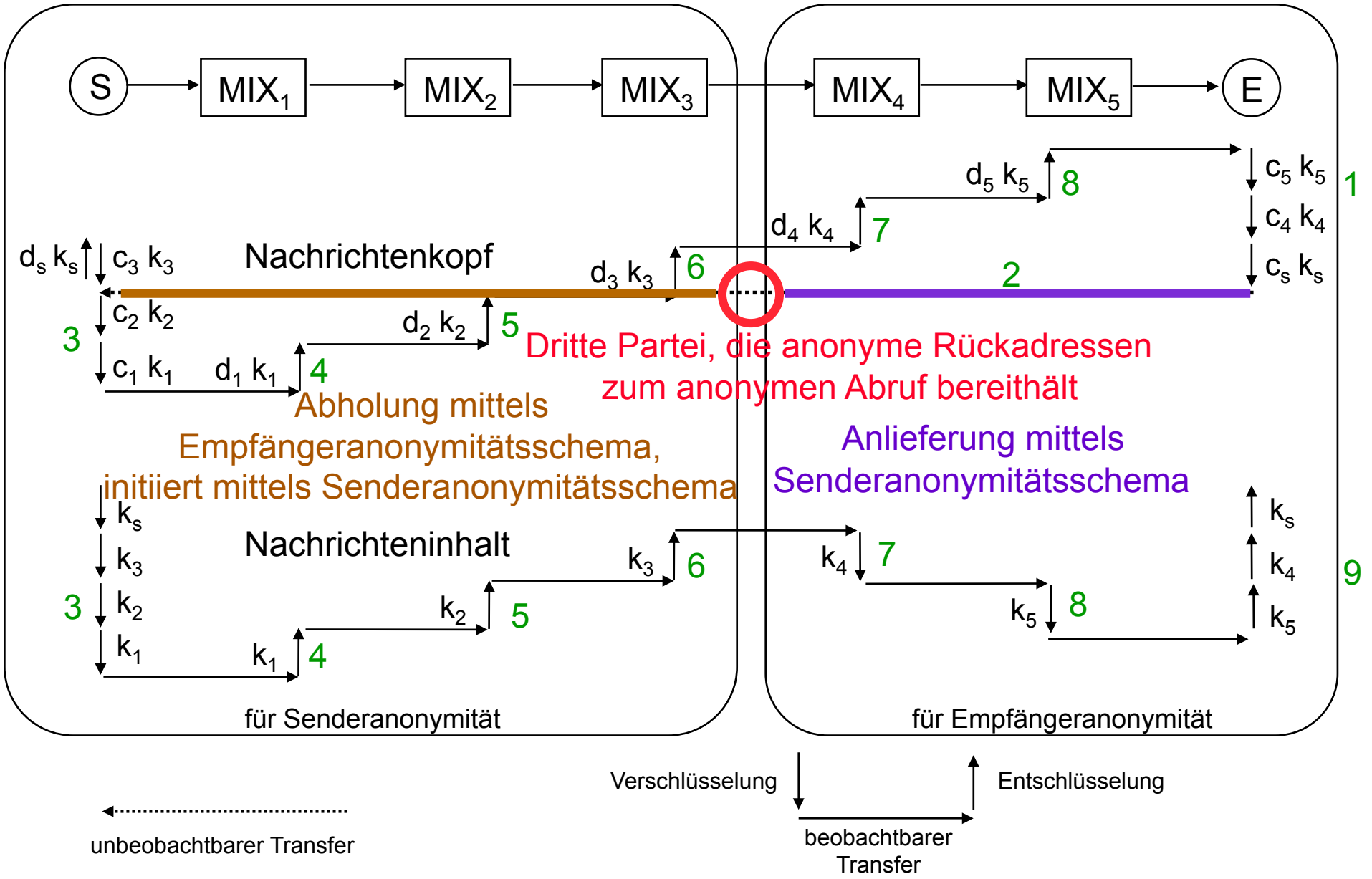
Indirektes Umcodierungungs. für Empfängeranonymität



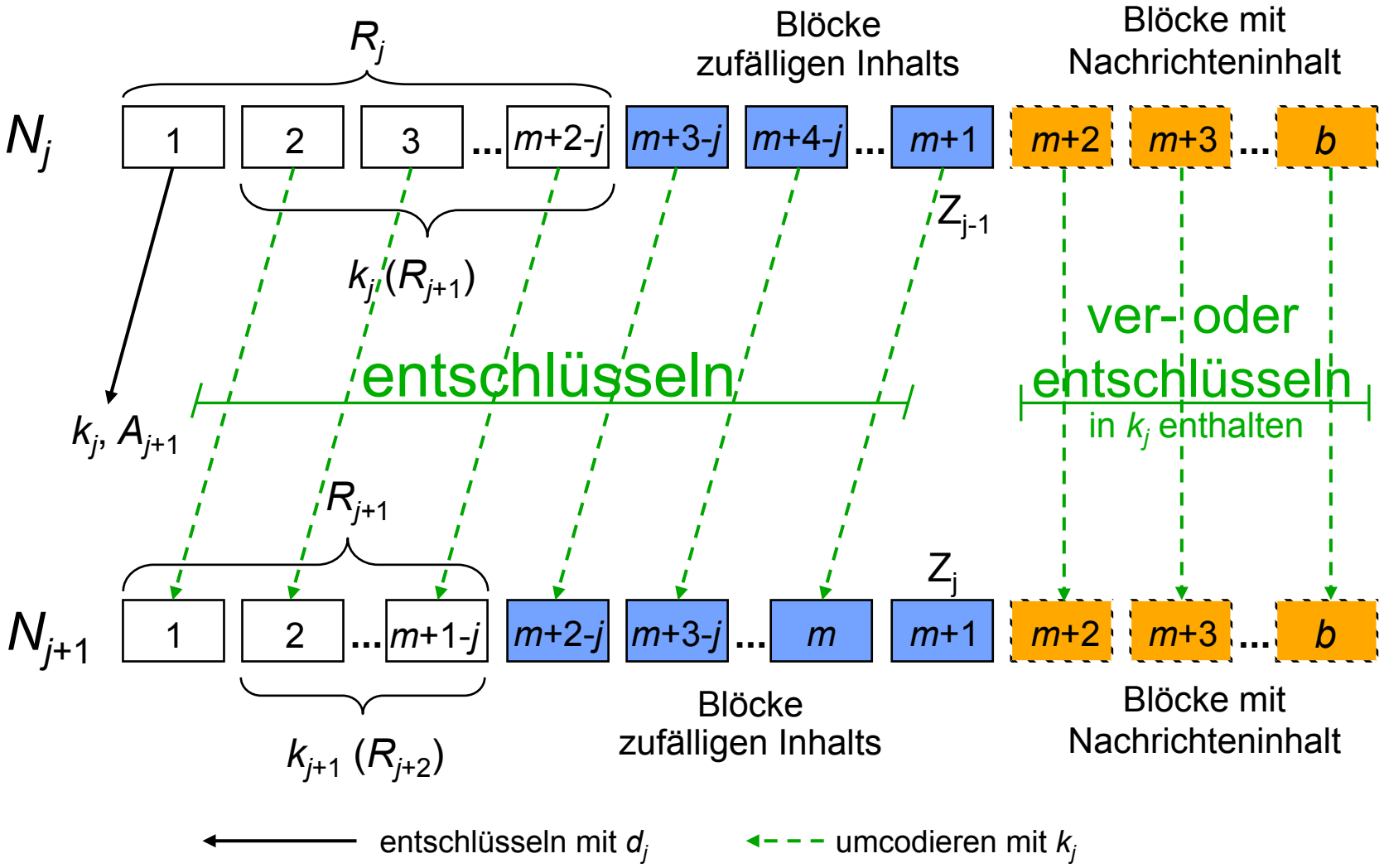
Indirektes Umcodierungsschema für Sender- und Empfängeranonymität



Indirektes Umcodierungsschema für Sender- und Empfängeranonymität



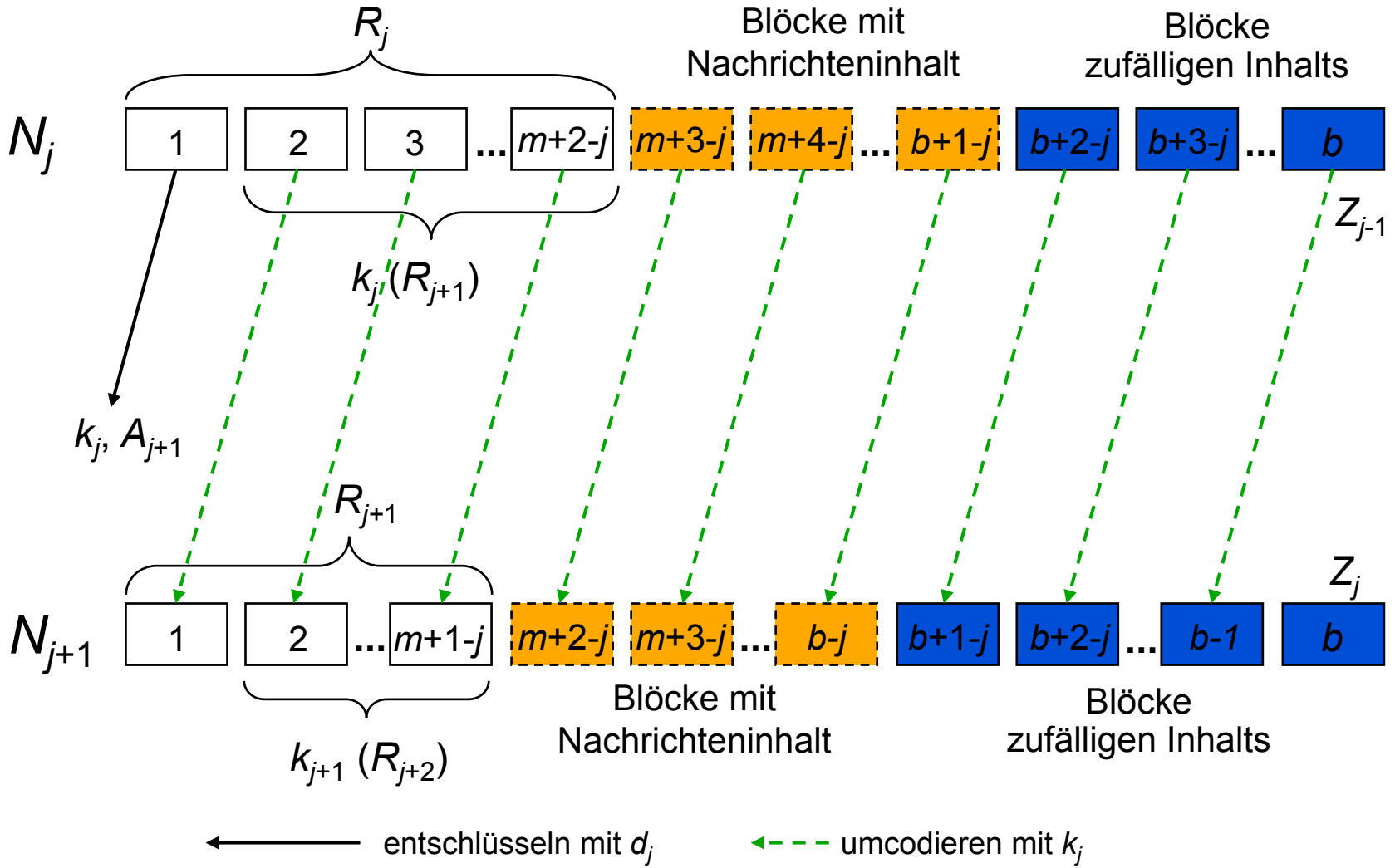
Indirektes längentreues Umcodierungsschema



$R_{m+1} = [e]$

$R_j \quad = [c_j(k_j, A_{j+1})], k_j(R_{j+1}) \quad$ für $j = m,..,1$

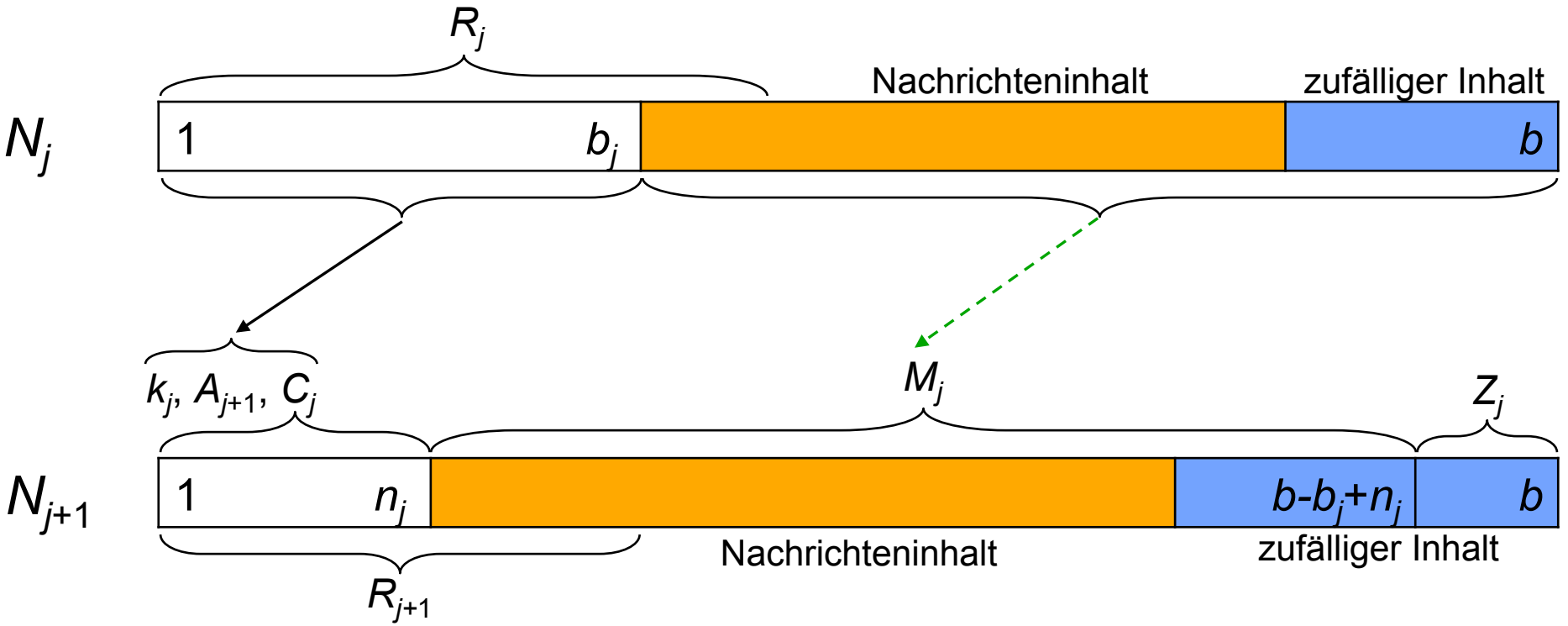
Indirektes längentreues Umcodierungsschema für spezielle symmetrische Konzelationssysteme



falls $k^{-1}(k(N)) = N$

und $k(k^{-1}(N)) = N$

Minimal nachrichtenexpandierendes längentreues Umcodierungsschema



entschlüsseln mit d_j

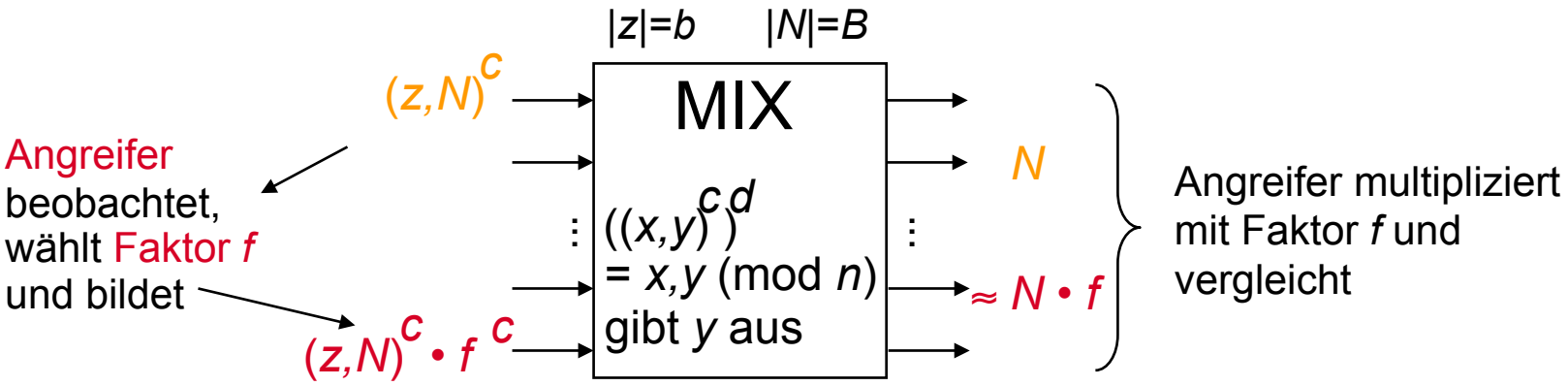
umcodieren mit k_j

falls $k^{-1}(k(N)) = N$

und $k(k^{-1}(N)) = N$

Brechen der direkten RSA-Implementierung

Implementierung von MIXen mittels RSA ohne Redundanzprädikat und mit zusammenhängenden Bitketten (David Chaum, 1981) ist unsicher:



Unverkettbarkeit, wenn viele Faktoren f möglich.

$2^b \cdot 2^B \leq n\text{-}1$ gilt immer und normalerweise $b << B$.

Stehen die zufälligen Bitketten an den Bitstellen höherer Wertigkeit, so gilt

$(z,N) = z \cdot 2^B + N$ und

$(z,N) \cdot f \equiv (z \cdot 2^B + N) \cdot f \equiv z \cdot 2^B \cdot f + N \cdot f.$

Brechen der direkten RSA-Implementierung (Forts.)

Seien die Bezeichner z' und N' definiert durch

$$(z,N)\bullet f \equiv z'\bullet 2^B + N' \Rightarrow$$

$$z\bullet 2^B\bullet f + N\bullet f \equiv z'\bullet 2^B + N' \Rightarrow$$

$$2^B\bullet (z\bullet f - z') \equiv N' - N\bullet f \Rightarrow$$

$$z\bullet f - z' \equiv (N' - N\bullet f) \bullet (2^B)^{-1} \qquad (1)$$

Wählt Angreifer $f \leq 2^b$, so gilt

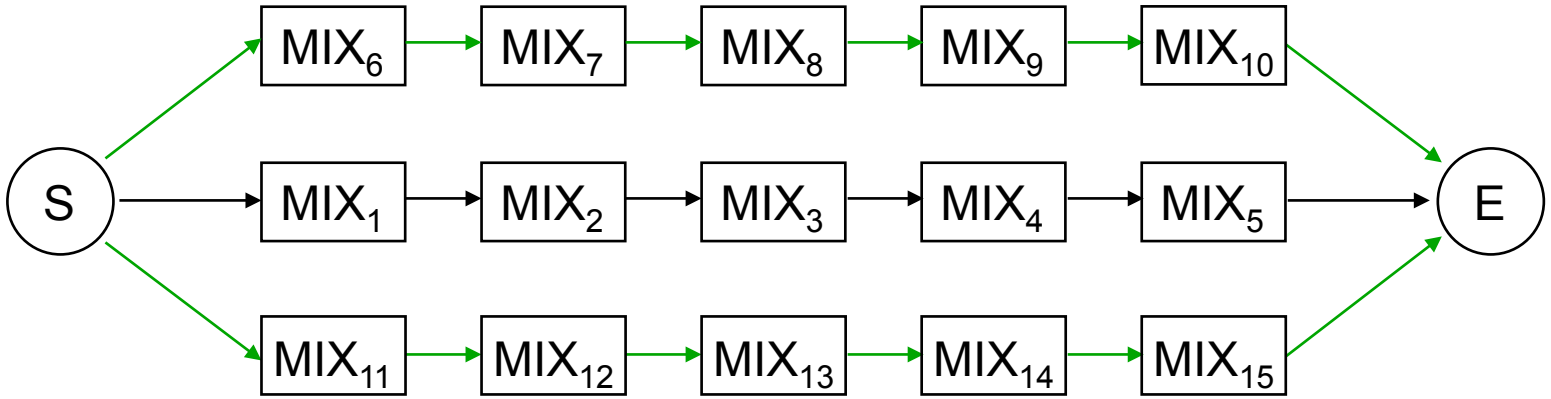
$$-2^b < z\bullet f - z' < 2^{2b} \qquad (2)$$

Angreifer setzt in (1) für N und N' alle Ausgabe-Nachrichten-Paare des Schubes ein und prüft (2).

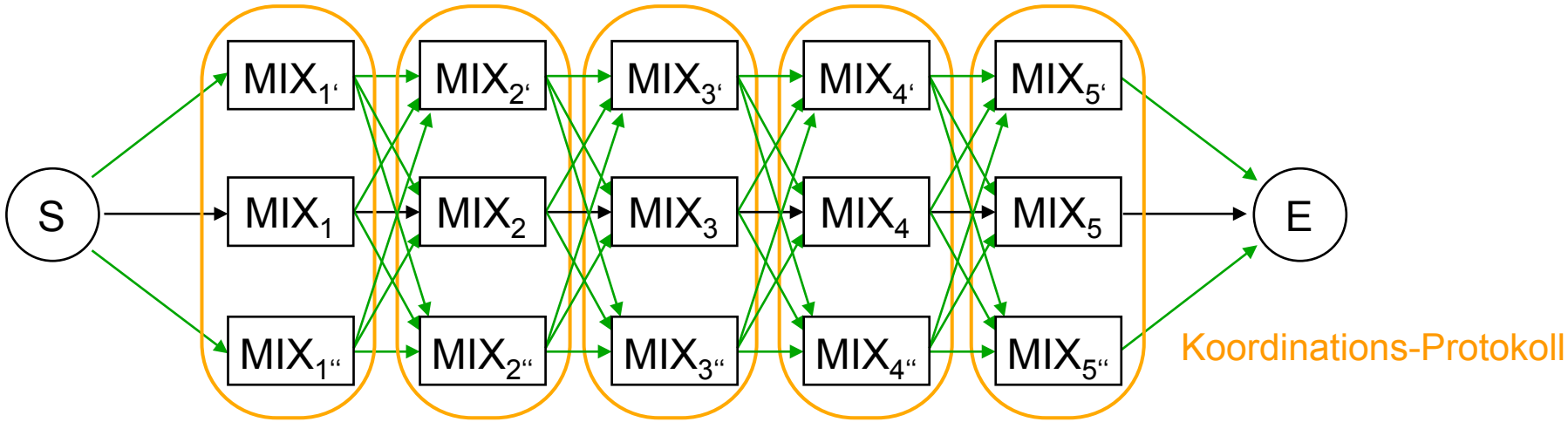
(2) gilt, wenn $b<<B$, sehr wahrscheinlich nur für ein Paar (P1,P2). P1 ist Ausgabe-Nachricht zu $(z,N)^c$, P2 zu $(z,N)^c\bullet f^c$.

Gilt (2) für mehrere Paare, wird Angriff mit neuem Faktor wiederholt.

Fehlertoleranz beim MIX-Netz

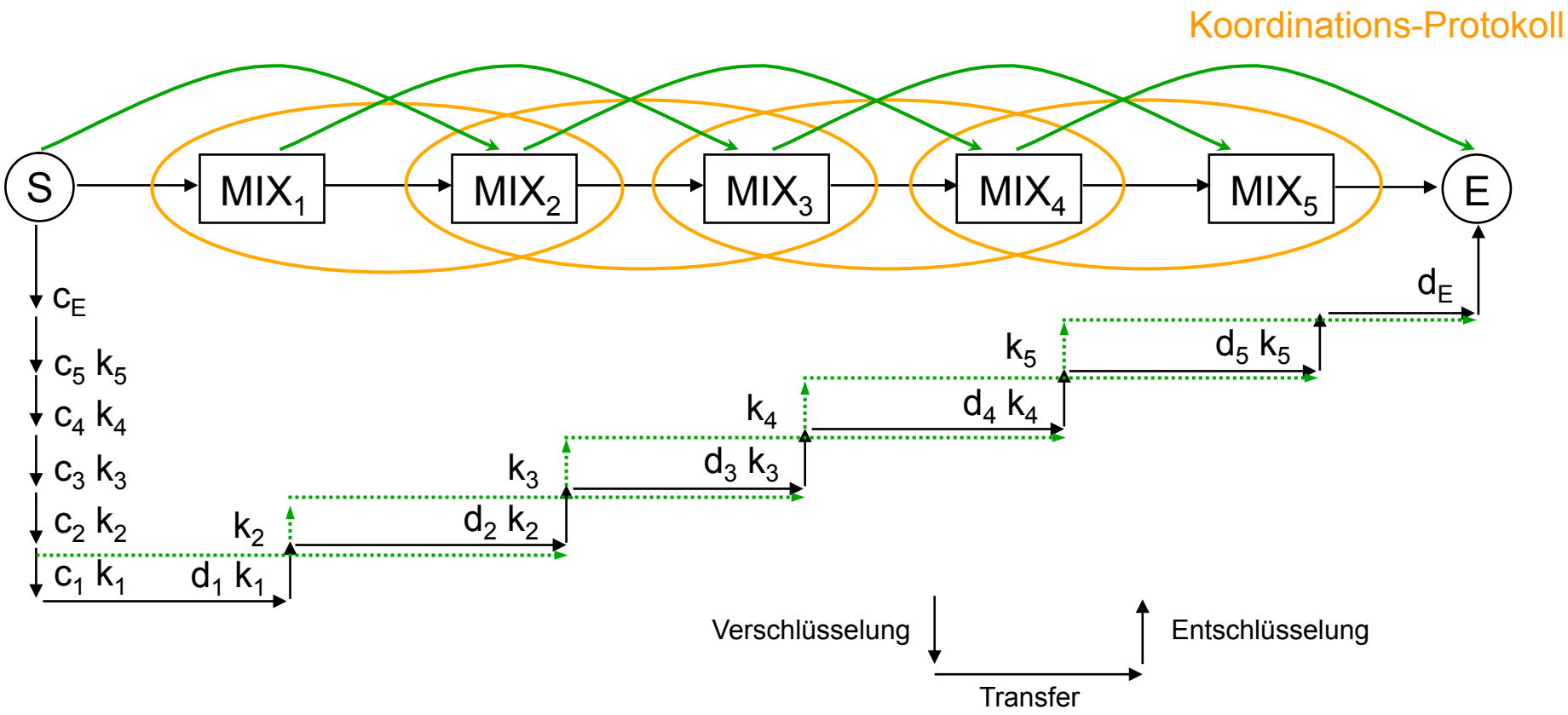


2 alternative Weg über disjunkte MIXe



$MIX_{i‘}$ oder $MIX_{i“}$ kann MIX_i ersetzen

Fehlertoleranz beim MIX-Netz (Forts.)



Jeweils ein MIX kann ausgelassen werden

Aufwand der Grundverfahren

	Unbeobachtbarkeit angrenzender Leitungen und digitale Signalregenerierung RING-Netz	DC-Netz	MIX-Netz
Angreifer-modell	physisch beschränkt	bzgl. Diensterbringung komplexitätstheoretisch beschränkt --- komplexitätsth. beschr. • kryptographisch stark • wohluntersucht	komplexitätstheoretisch beschränkt nicht einmal wohluntersuchte, gegen adaptive aktive Angriffe sichere asym. Konzelationssysteme bekannt
Aufwand pro Teilnehmer	$O(n)$ $(\geq \frac{n}{2})$ Übertragung	$O(n)$ $(\geq \frac{n}{2})$ Übertragung $O(k \bullet n)$ Schlüssel	$O(k)$, praktisch: ≈ 1 Übertragung im Teilnehmeranschluss-bereich ... im Innern des Netzes $O(k^2)$, praktisch: $\approx k$

n = Teilnehmerzahl

k = Zusammenhang Schlüsselgraph DC-Netz bzw. Anzahl MIXe

Verschlüsselung in Schichtenmodellen

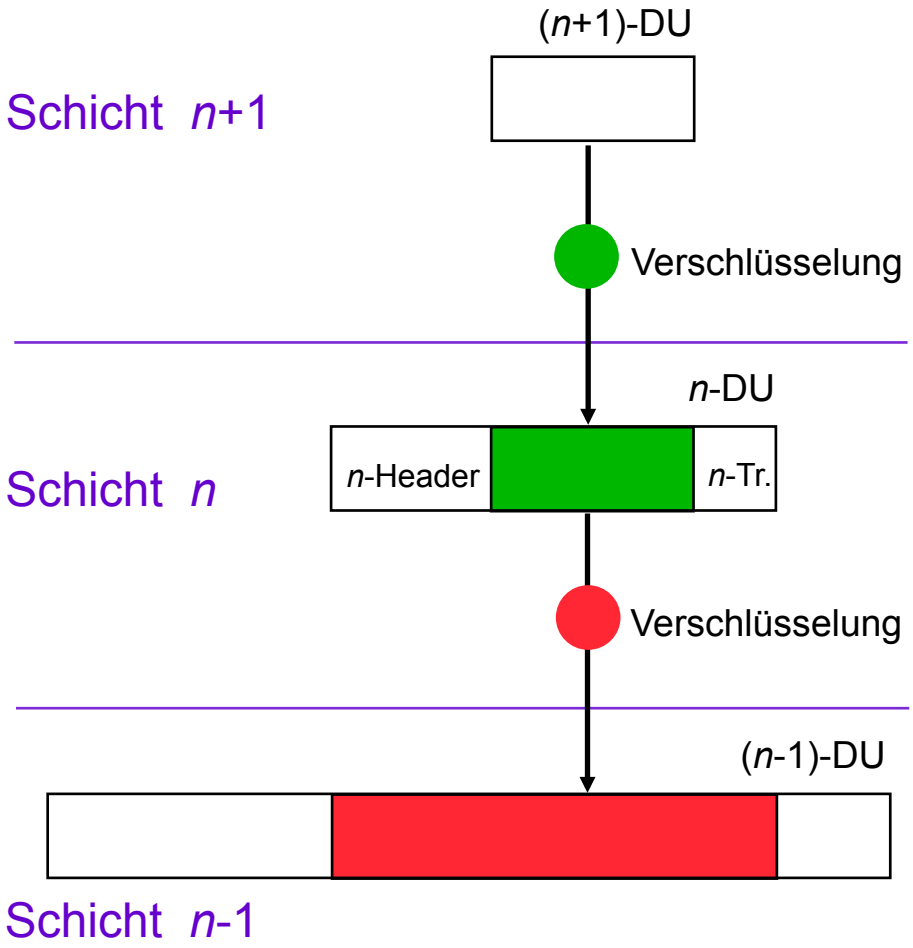
Im OSI-Modell gilt:

Schicht *n* braucht sich die Data Units (DUs) von Schicht *n*+1 nicht anzuschauen, um ihren Dienst zu erbringen. Also kann Schicht *n*+1 die (*n*+1)-DUs verschlüsselt an Schicht *n* übergeben.

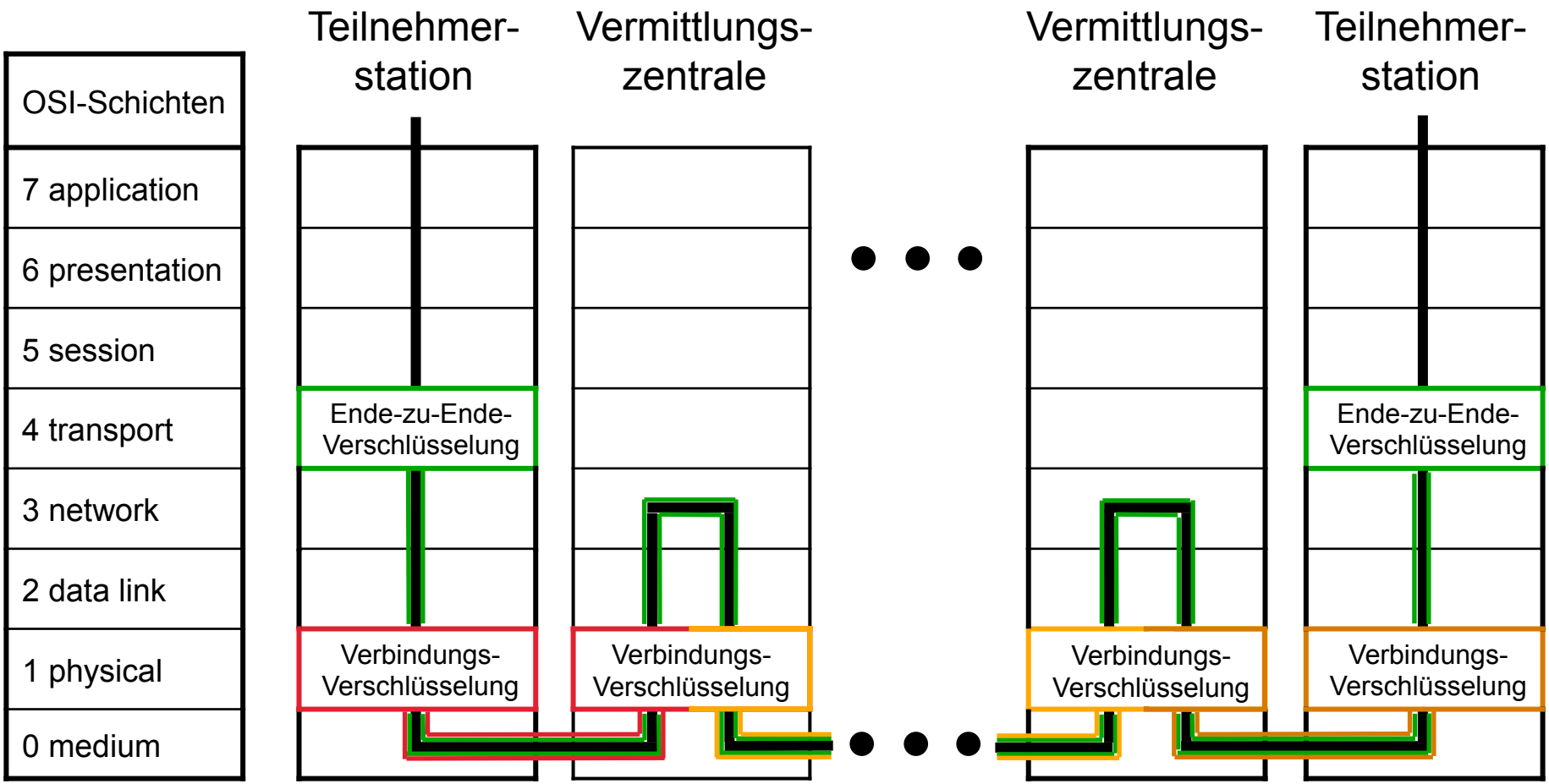
Schicht *n* versieht die (*n*+1)-DUs bei paketorientierten Diensten typischerweise mit einem *n*-Header und ggf. auch einem *n*-Trailer, und übergibt dies als *n*-DU an Schicht *n*-1. Auch dies kann wiederum verschlüsselt erfolgen.

usw.

Alle Verschlüsselungen sind sowohl bzgl. des Kryptoverfahrens wie der Schlüssel unabhängig voneinander.



Einordnung in ein Schichtenmodell



Einordnung in ein Schichtenmodell

OSI-Schichten	Verteilung		Abfragen	MIX-Netz	DC-Netz	RING-Netz
7 application						
6 presentation						
5 session						
4 transport	implizite Adressierung		implizite Adressierung			
3 network	Verteilung		Abfragen u. Überlagern	Puffern und Umschlüsseln		
2 data link					anonymer Mehrfachzugriff	anonymer Mehrfachzugriff
1 physical		Kanalselektion			Schlüssel und Nachrichten überlagern	digitale Signalregenerierung
0 medium						Ring

muss Anonymität vor dem Kommunikationspartner erhalten

Ende-zu-Ende-Verschlüsselung

muss Anonymität erhalten

ohne Rücksicht auf Anonymität realisierbar

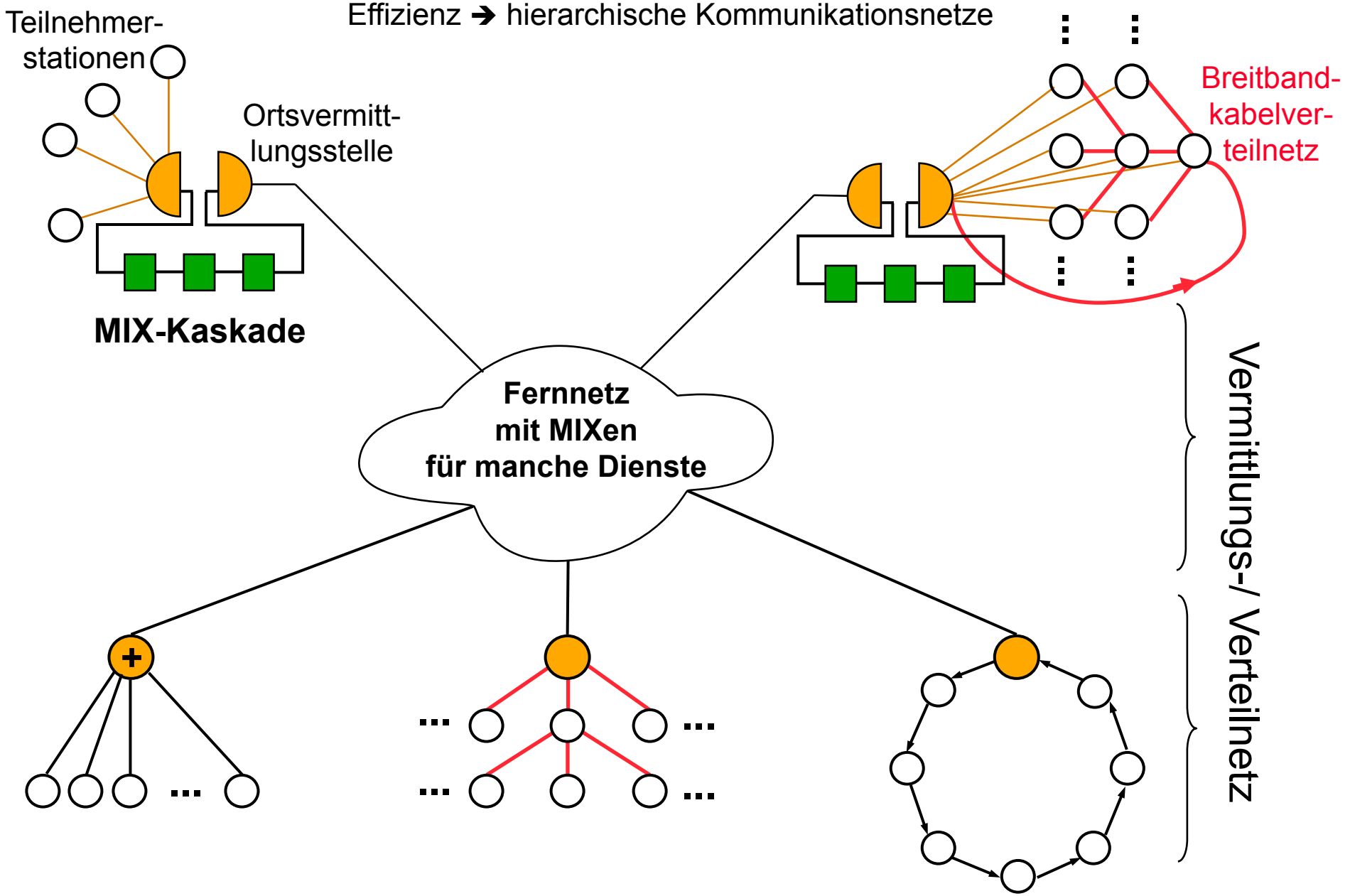
Tolerierung von Fehlern und aktiven Angriffen

Probleme: Seriensysteme bzgl. Zuverlässigkeit

Anonymität „braver“ Teilnehmer erhalten

Es gibt geeignete Verfahrenserweiterungen

Etappenweiser Netzausbau



Lösung für das ISDN: Telefon-MIXe

Anforderung: ISDN-Dienste auf ISDN-Übertragungstechnik

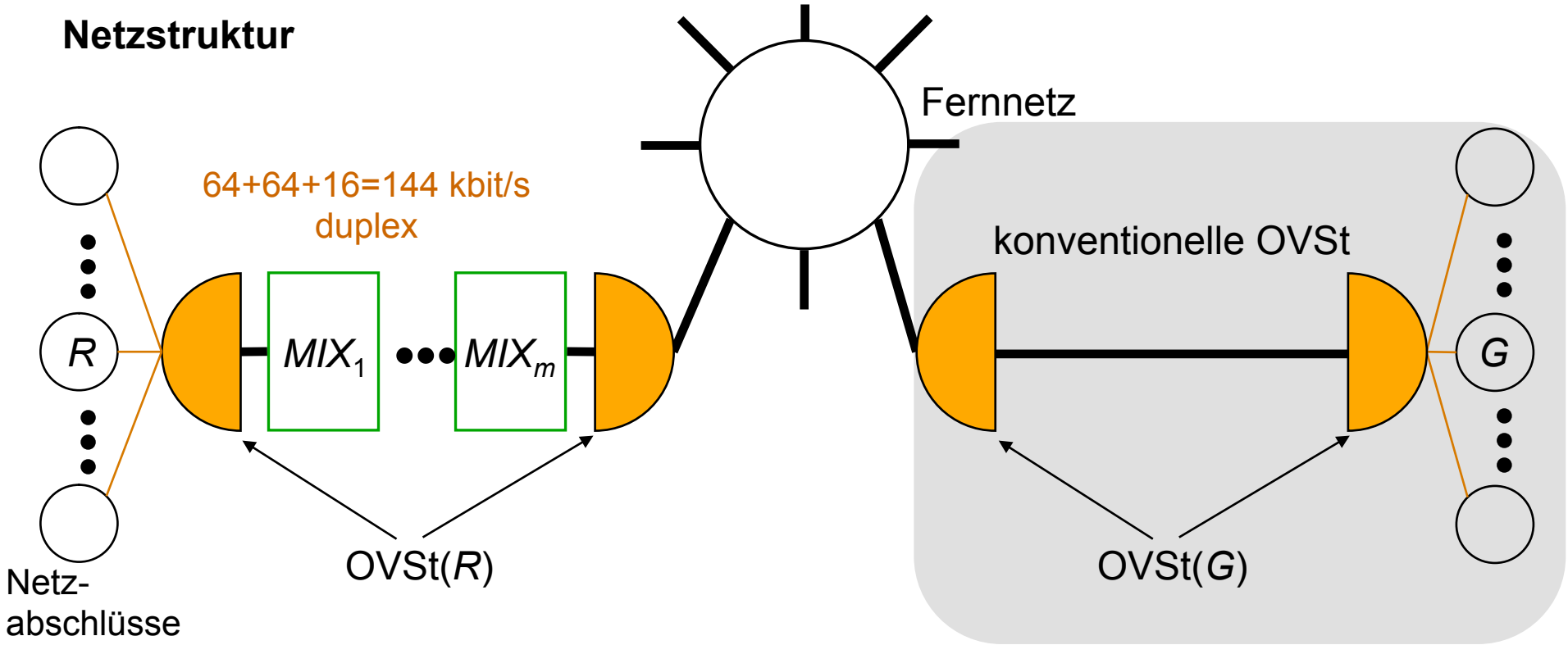
2 unabhängige 64-kbit/s-Duplexkanäle auf 144-kbit/s-Anschluss

Fast keine zusätzliche Verzögerung auf bestehenden Kanälen

Schalten eines Kanals innerhalb von 3 s

Keine zusätzlichen Fernnetzbelastung

Netzstruktur



Lösung für das ISDN: Telefon-MIXe

Anforderung: ISDN-Dienste auf ISDN-Übertragungstechnik

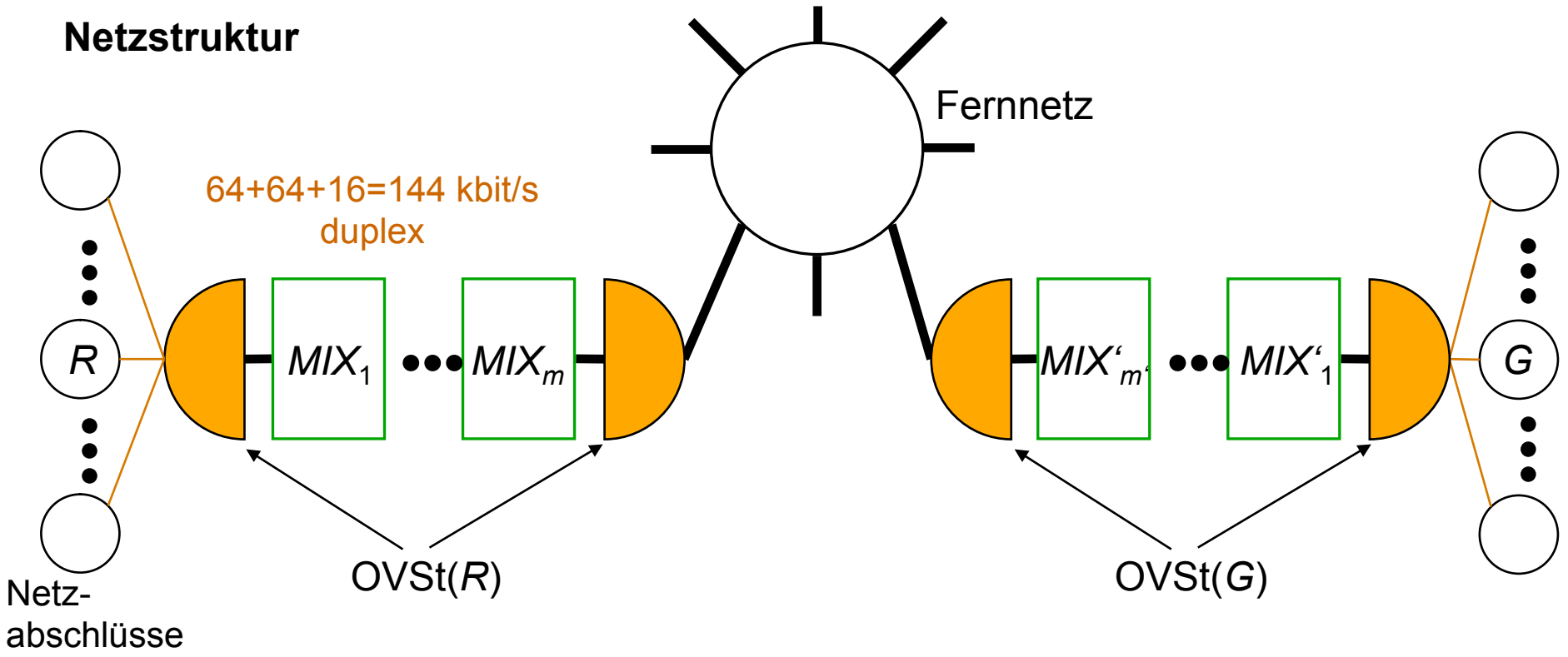
2 unabhängige 64-kbit/s-Duplexkanäle auf 144-kbit/s-Anschluss

Fast keine zusätzliche Verzögerung auf bestehenden Kanälen

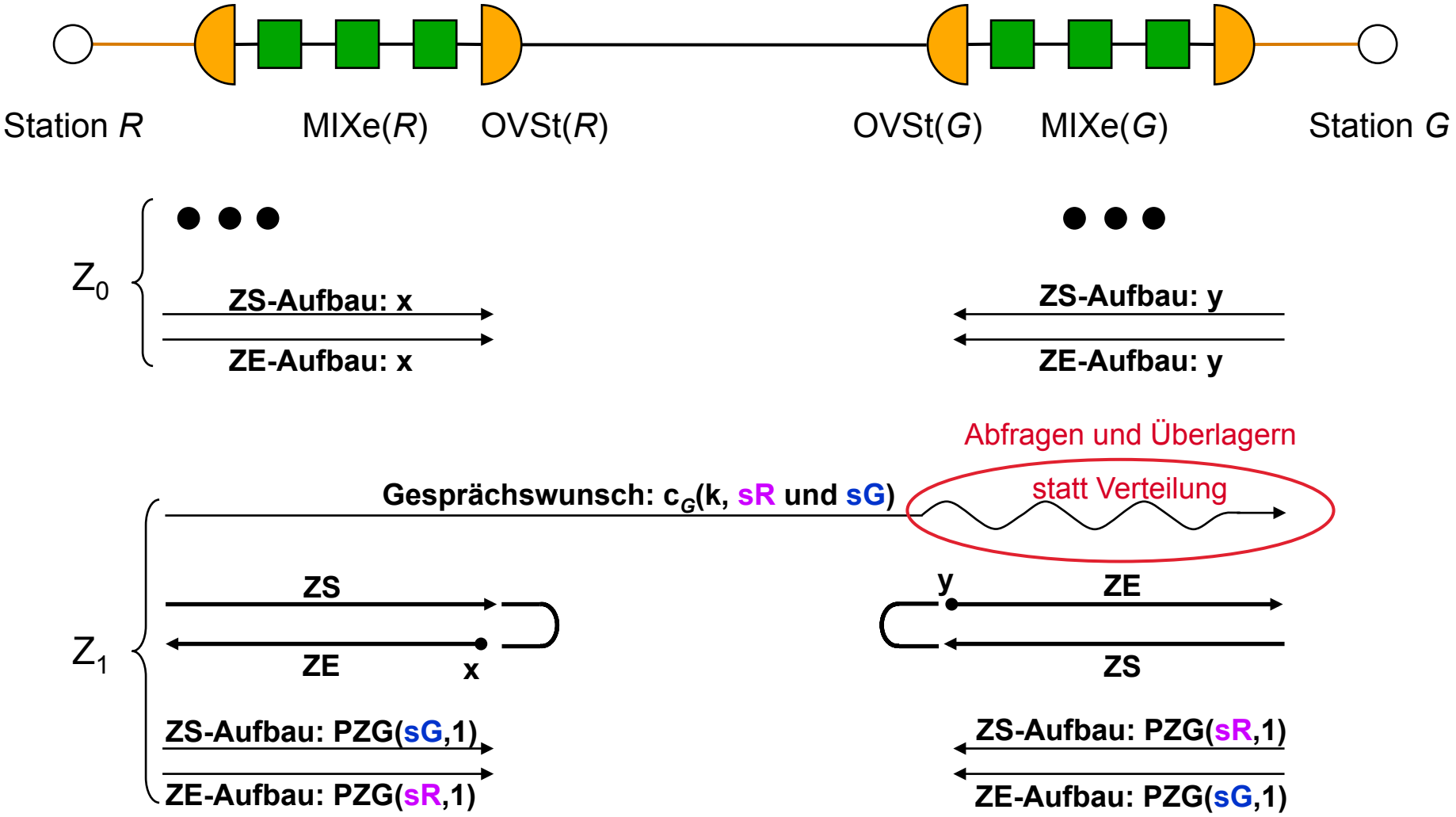
Schalten eines Kanals innerhalb von 3 s

Keine zusätzlichen Fernnetzbelastung

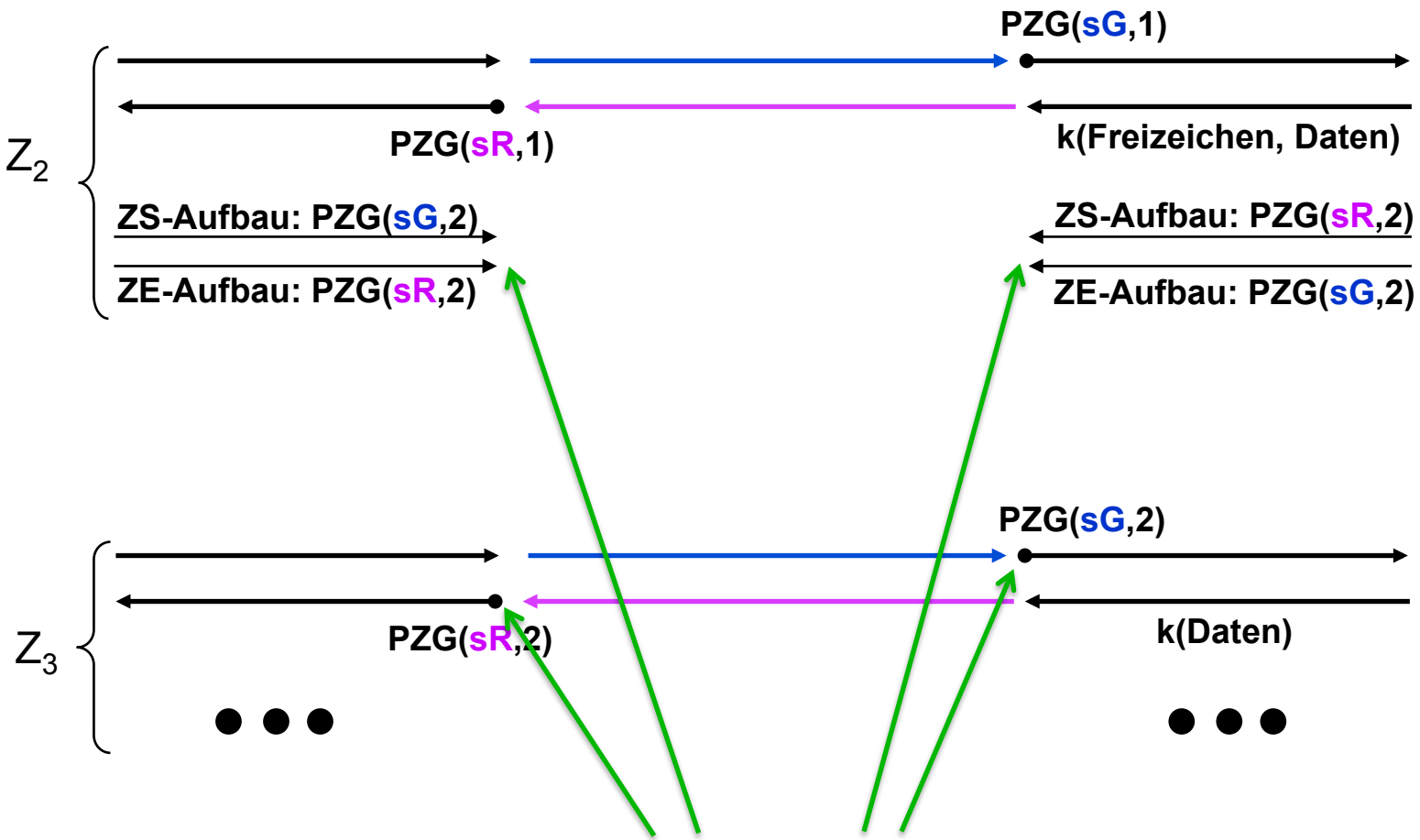
Netzstruktur



Verfahren der Zeitscheibenkanäle

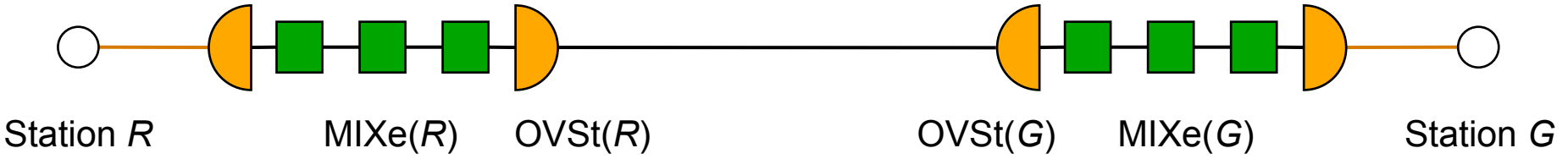


Verfahren der Zeitscheibenkanäle (Forts.)



Dieser Aufbau von Empfangskanälen
ist ein sehr flexibles Schema für
Empfängeranonymität.

Verbindungsaufbau später



Z_0

ZS-Aufbau: x

ZE-Aufbau: x

ZS-Aufbau: PZG(sP,0)

ZE-Aufbau: PZG(sQ,0)

Z_1

Gesprächswunsch: c_G(k, sR und sG)

ZS

ZE **x**

von P **PZG(sQ,0)** **ZE**

an P

ZS

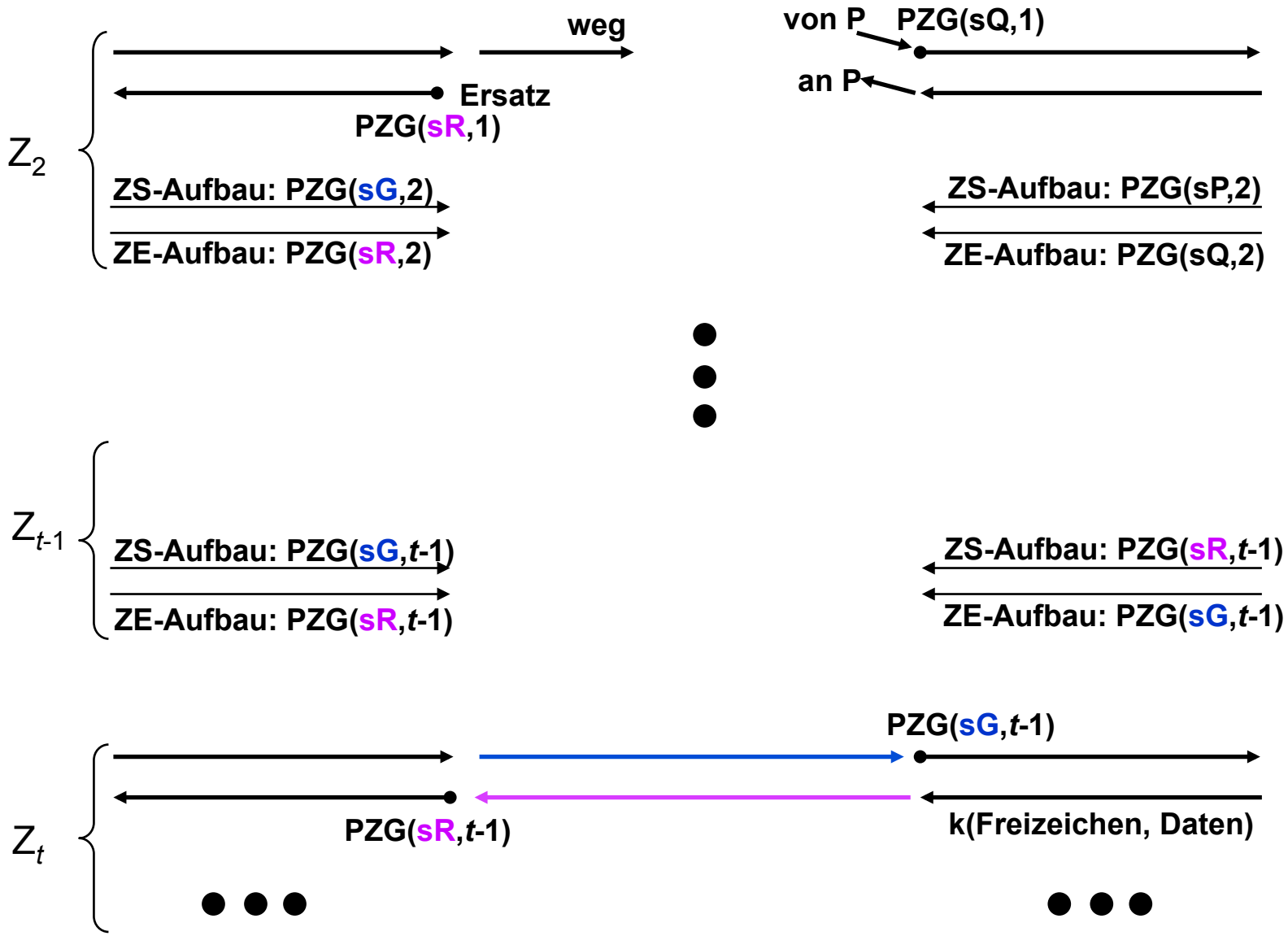
ZS-Aufbau: PZG(sG,1)

ZE-Aufbau: PZG(sR,1)

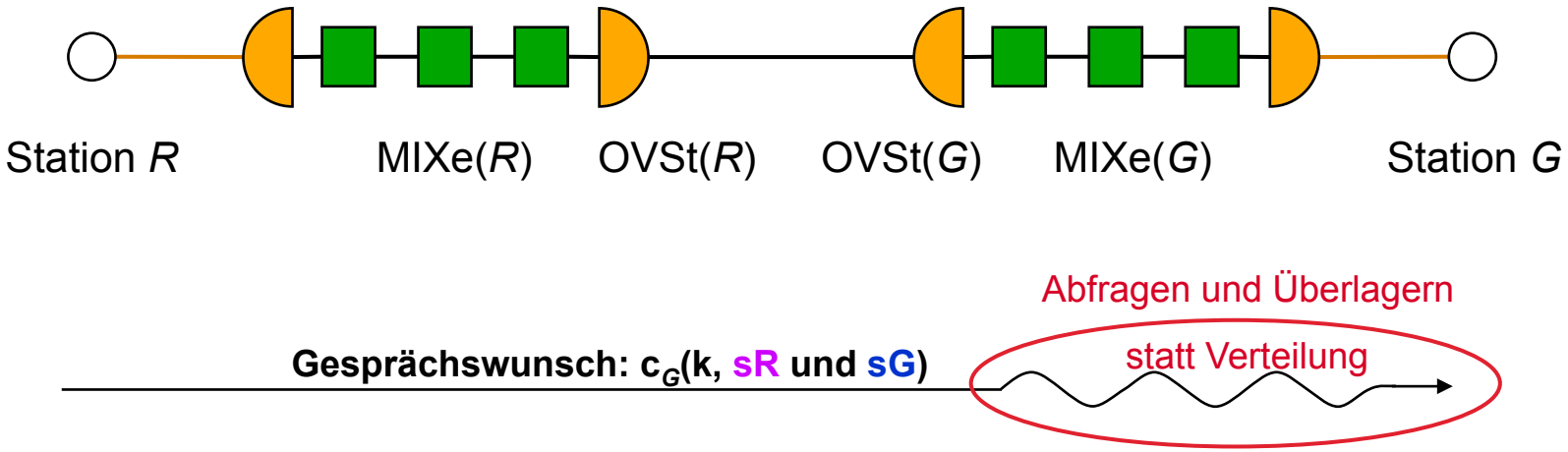
ZS-Aufbau: PZG(sP,1)

ZE-Aufbau: PZG(sQ,1)

Verbindungsaufbau später (Forts.)



Abfragen und Überlagern zum Erhalt der Gesprächswünsche



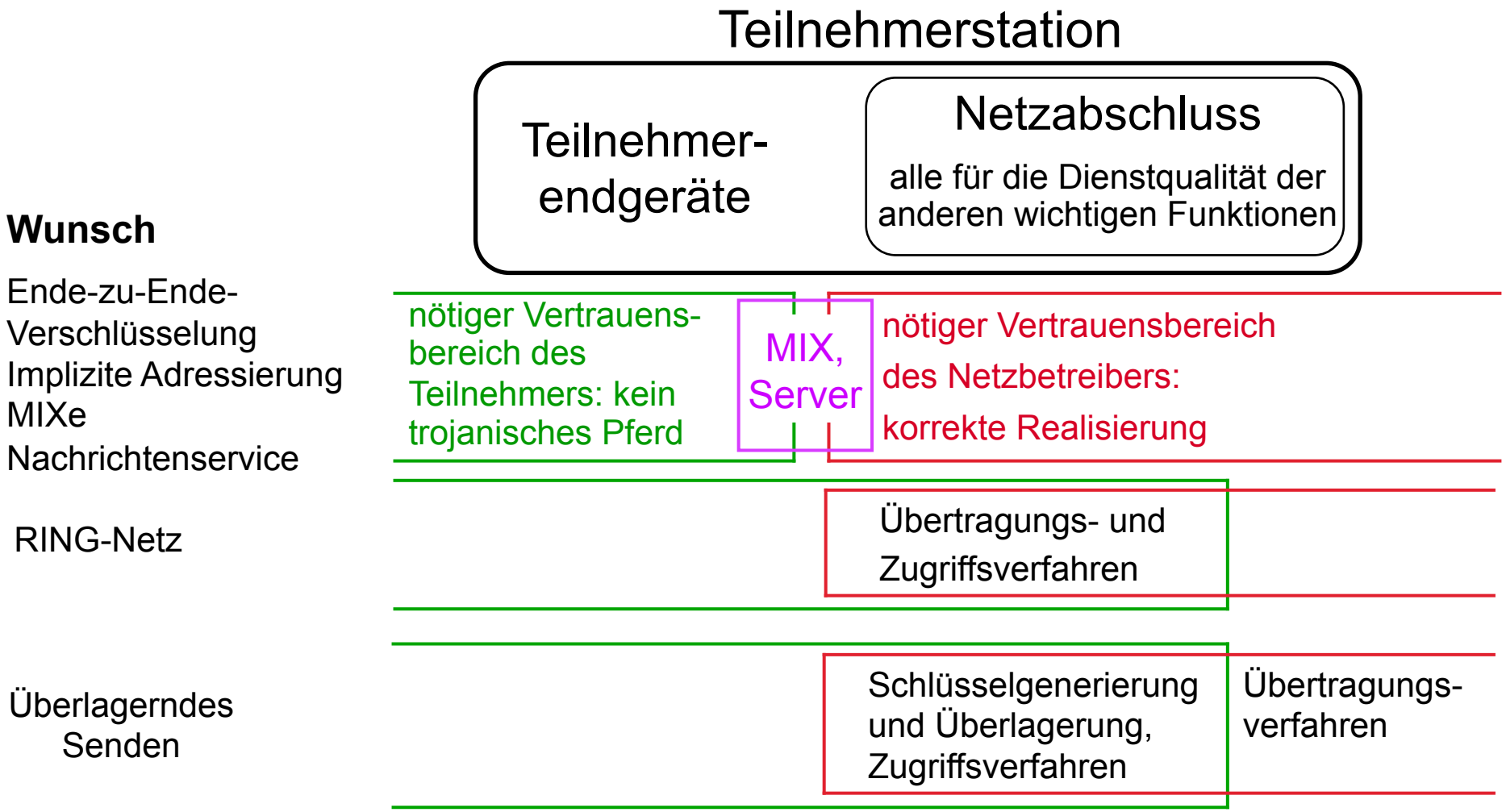
Abfragen und Überlagern:

- In jeder Zeitscheibe muss *jede* Station abfragen (sonst zerfällt Anonymitätsmenge)
- Bei jeder Abfrage sollte jede Station *alle* ihre impliziten Adressen abfragen

(geht bei offenen wie auch verdeckten impliziten Adressen ohne Mehraufwand)

–> Anonymitätsmengengröße ist nicht mehr durch Übertragungskapazität auf der Teilnehmeranschlußleitung begrenzt, sondern nur noch durch Additionsleistung der Nachrichtenserver.

Netzbetreiberschaft



Probleme hier einfacher als bei Vermittlungszentralen:

1. Netzabschluss weniger komplex
2. nicht schnell änderbar (Hardware, keine Fernwartung)

MIXe, Server: techn. leichter; organisatorisch bzgl. Vertrauen problematischer

Überlagerndes Senden: technisch aufwendiger; organisatorisch leichter

Ausblick

Netznutzung → Transaktionen zwischen anonymen Partnern

→ expliziter Identitätsnachweis stets möglich

Schutz der Verkehrs- und Interessendaten
erfordert geeignete Netzstruktur

→ rechtzeitig überlegen

} Optionen offen halten

Anonyme Netze können ohne Leistungseinbuße
nicht anonym betrieben werden,
Umkehrung gilt nicht!

Ausblick (Forts.)

Überprüfbarer Datenschutz generell oder nur bei individueller Bezahlung für Interessierte?

- Bzgl. Verkehrsdaten ist Letzteres technisch ineffizient.
- Letzteres hat gegenteiligen Effekt (Verdacht).
- Grundrechte sollten sich alle leisten können!

Funknetze

Unterschiede zu Leitungsnetzen

- Übertragungsbandbreite bleibt knapp
- Auch der momentane Ort des Teilnehmers ist zu schützen

Annahmen

- Mobile Teilnehmerstation ist *immer* identifizierbar und peilbar, wenn sie sendet.
- Mobile Teilnehmerstation ist *nicht* identifizierbar und peilbar, wenn sie nur (passiv) empfängt.

Welche Maßnahmen sind anzuwenden?

+ Ende-zu-Ende-Verschlüsselung

+ Verbindungs-Verschlüsselung

- bedeutungslose Nachrichten, Unbeobachtbarkeit angrenzender Leitungen und Stationen, sowie digitale Signalgenerierung, überlagerndes Senden

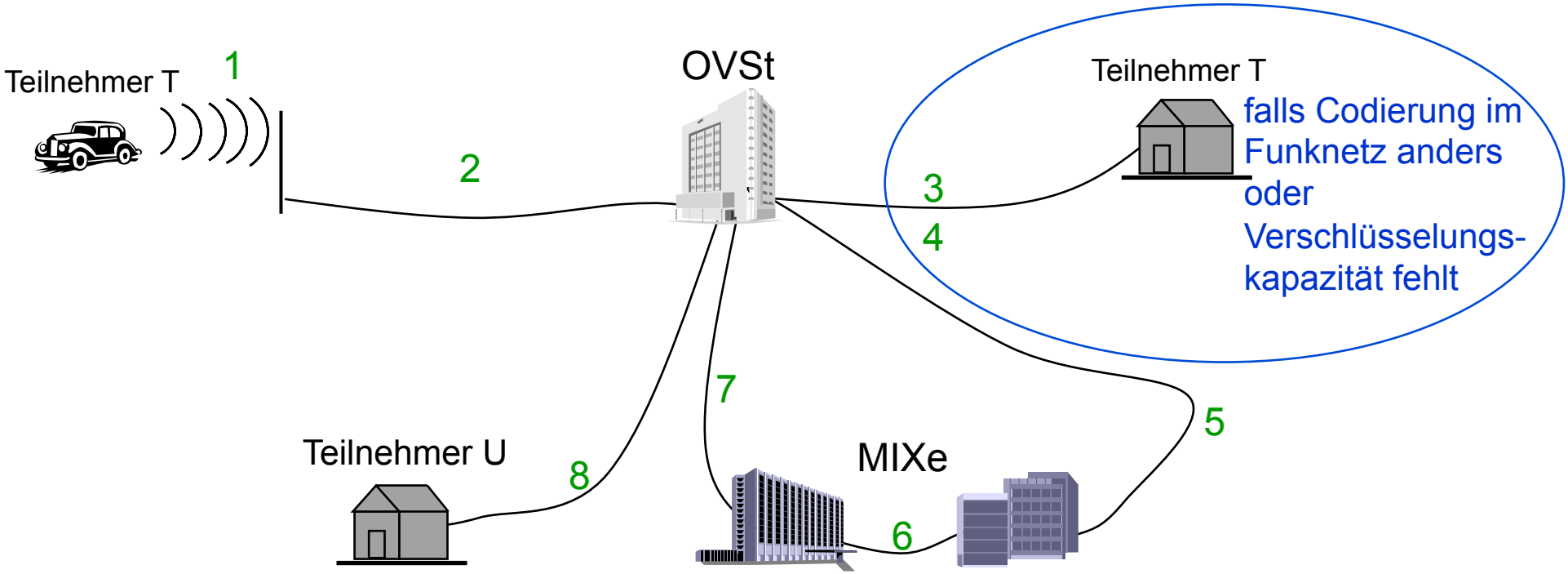
nicht empfeh-lenswert

nicht anwend-bar

➔ alle Maßnahmen zum Schutz der Verkehrs- und Interessensdaten müssen im ortsfesten Teil des Kommunikationsnetzes abgewickelt werden

Funknetze (Forts.)

+ MIXe



+ Verbindungswunsch im ganzen Funknetz verteilen, erst dann meldet sich Mobilstation. Danach Übertragung nur in einer Funkzelle.

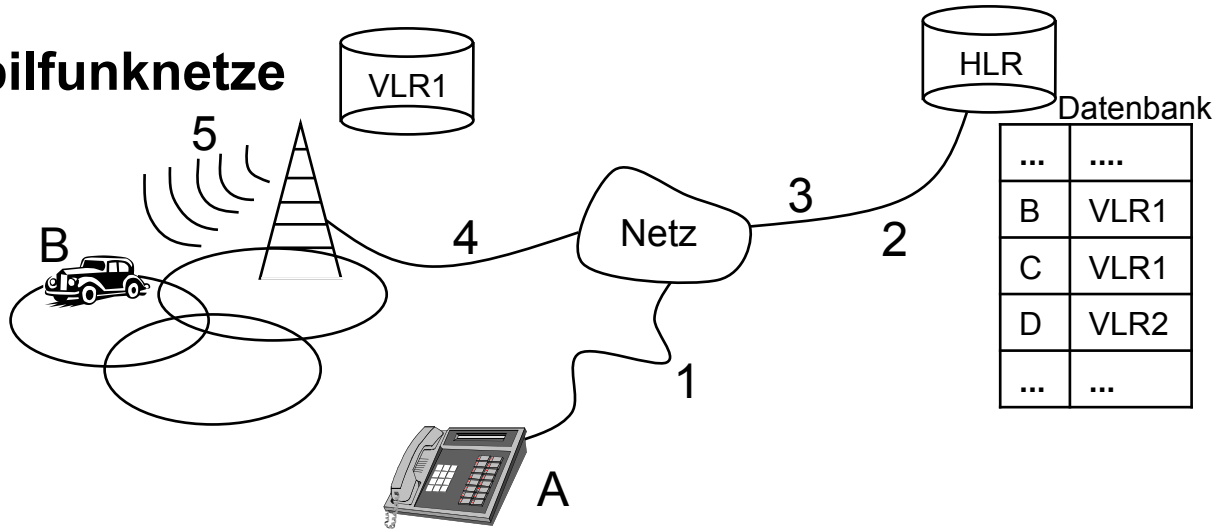
+ filtern + offene implizite Adressgenerierung + Region einschränken

+ Benutzer und SIM vor Sendestation anonym halten.

Keine Bewegungsprofile in Funknetzen

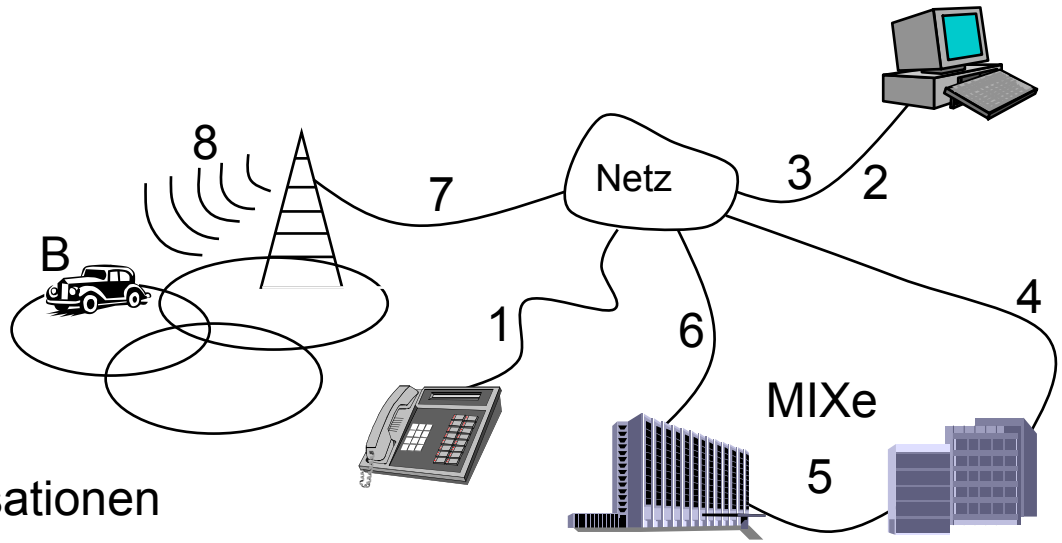
GSM/UMTS – zellulare Mobilfunknetze

- Aufenthaltsinformation in zentrale Datenbanken
- Netzbetreiber können die Information erfassen



Alternatives Konzept

- Verwaltung der Aufenthalts-information in vertrauenswürdiger Umgebung
  - zu hause (HPC)
  - bei vertrauenswürdigen Organisationen
- Schutz der Kommunikationsbeziehung durch MIXe



Electronic Banking

Motivation

- Papierbanking – Komfortversion

  Kunde erhält von Bank fertige personalisierte Formulare, in die nur noch der Betrag einzusetzen ist. Keinerlei Unterschrift!

  Electronic Banking – übliche Version

  Kunde erhält von Bank Karte und PIN, TAN

  demnächst

  Kunde erhält von Bank Chipkarte mit

  oder → Schlüssel für MAC

  oder → Schlüsselpaar für digitale Signatur

- Planspiel der US-Geheimdienste: UdSSR-Bürger überwachen (1971, Foy 75)

Hauptteil (Alles etwas genauer)

- Zahlungssysteme ist sicher...

  MAC, digitale Signatur

  Zahlungssystem mit digitalen Signaturen

- Pseudonyme (Personenkennzeichen ↮ Rollenbeziehungspseudonyme)

Sicherheitseigenschaften digitaler Zahlungssysteme

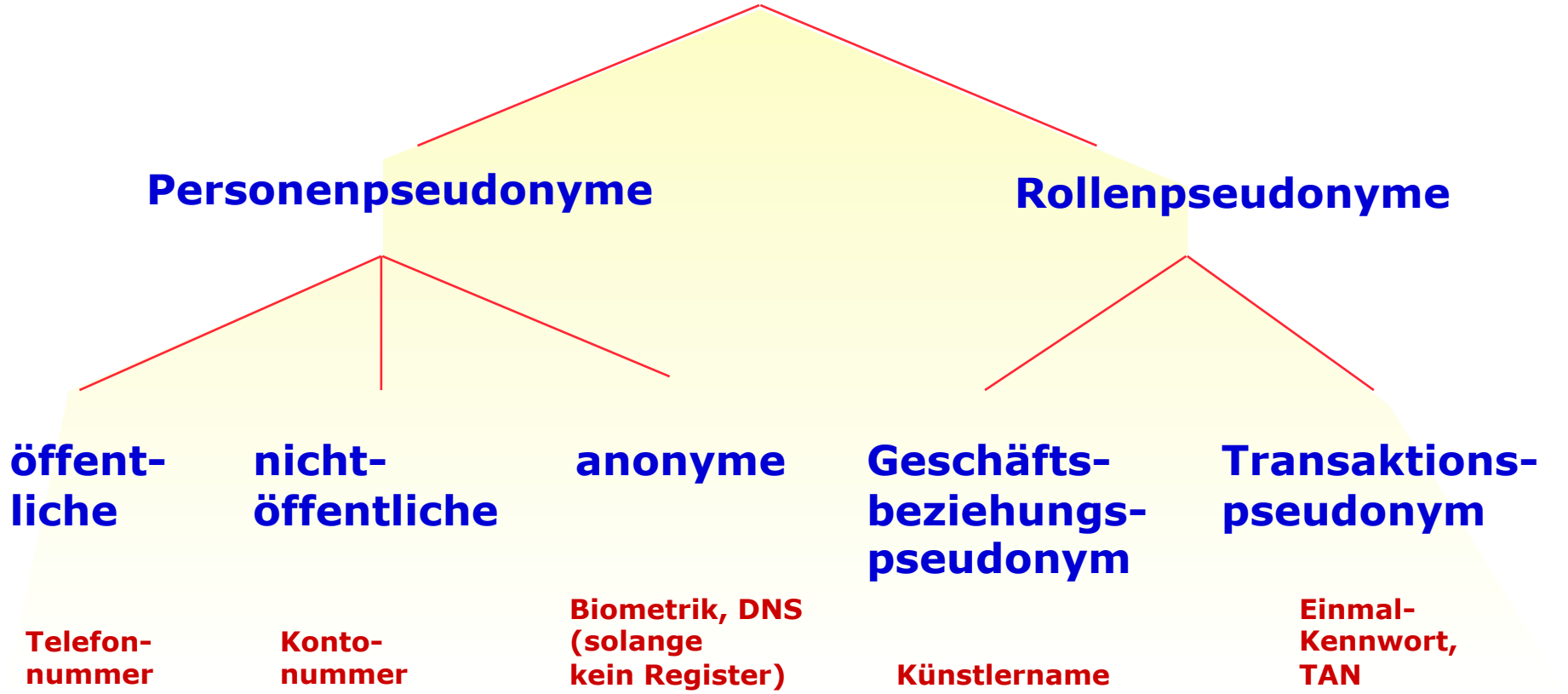
digitales (Integrität, Verfügbarkeit)
Zahlungssystem ist **sicher**, falls

- Benutzer erhaltene Rechte transferieren kann, über Netz, immateriell, digital
- Benutzer ein Recht nur dann verlieren, wenn er hierzu den Willen hat,
- sofern ein zahlungswilliger Benutzer einen anderen Benutzer als Empfänger eindeutig bestimmt, auch nur dieser Empfänger das Recht erhält,
- Benutzer falls notwendig einen vollzogenen Transfer einem Dritten gegenüber nachweisen kann (Quittungsproblem) und
- die Benutzer auch bei Zusammenarbeit ihre Rechte an Geld nicht vermehren können, ohne dass der Täter identifiziert wird.

Problem: Nachrichten sind kopierbar

Lösung: Zeuge akzeptiert nur *erste* Nachricht

Pseudonyme Beispiele



Skalierbarkeit bezüglich des Schutzes

A n o n y m i t ä t

Pseudonyme genauer

Unterscheidung nach:

1. Initialer Personenbezug
2. Verwendungszusammenhang

Pseudonyme: Initialer Personenbezug

Öffentliches Pseudonym:

Bezug zwischen Pseudonym und seinem Inhaber von Beginn an öffentlich bekannt.

Telefonnummer mit Inhaber im Telefon“buch“ gelistet

Initial nicht-öffentliches Pseudonym:

Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn zwar manchen (Identitätstreuhänder), aber nicht allen bekannt.

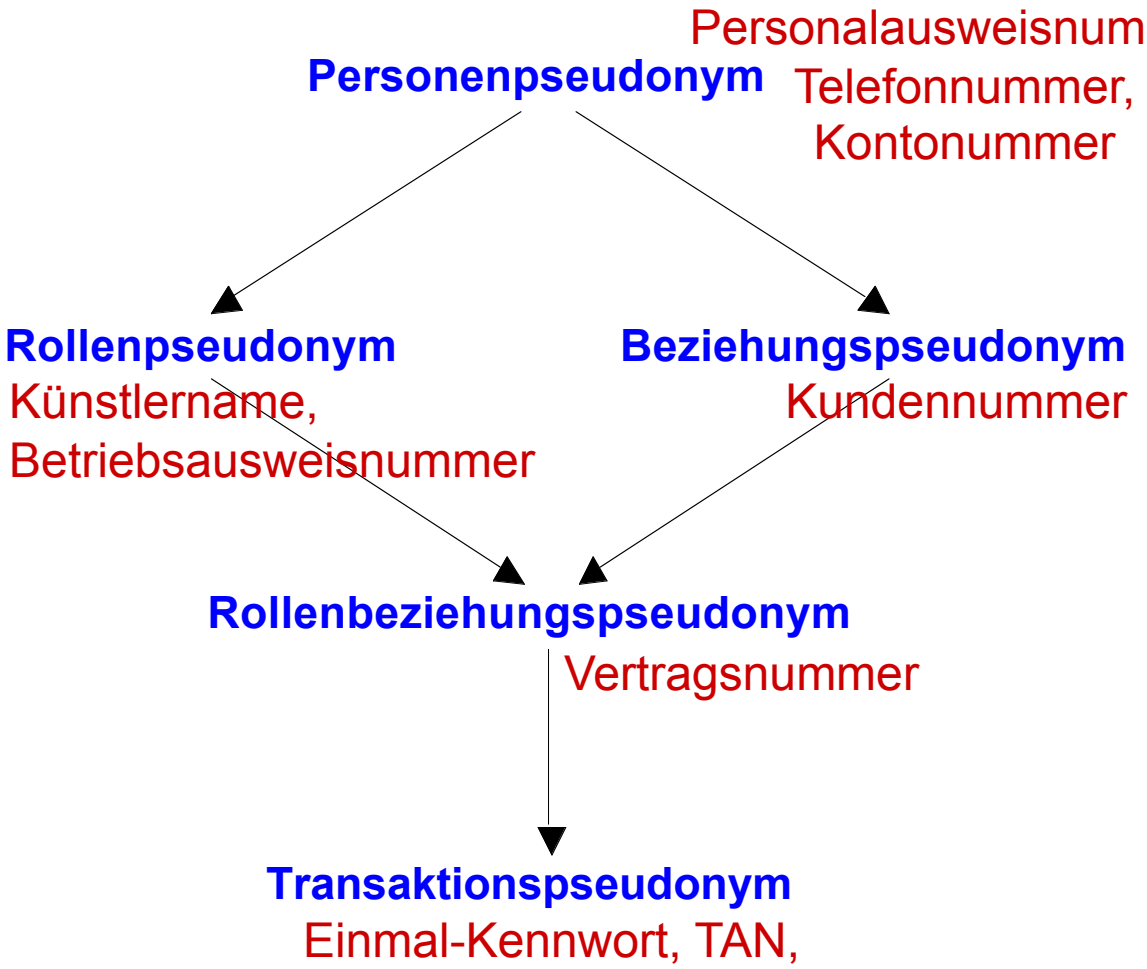
Kontonummer mit Bank als Identitätstreuhänder,
Kreditkartennummer ...

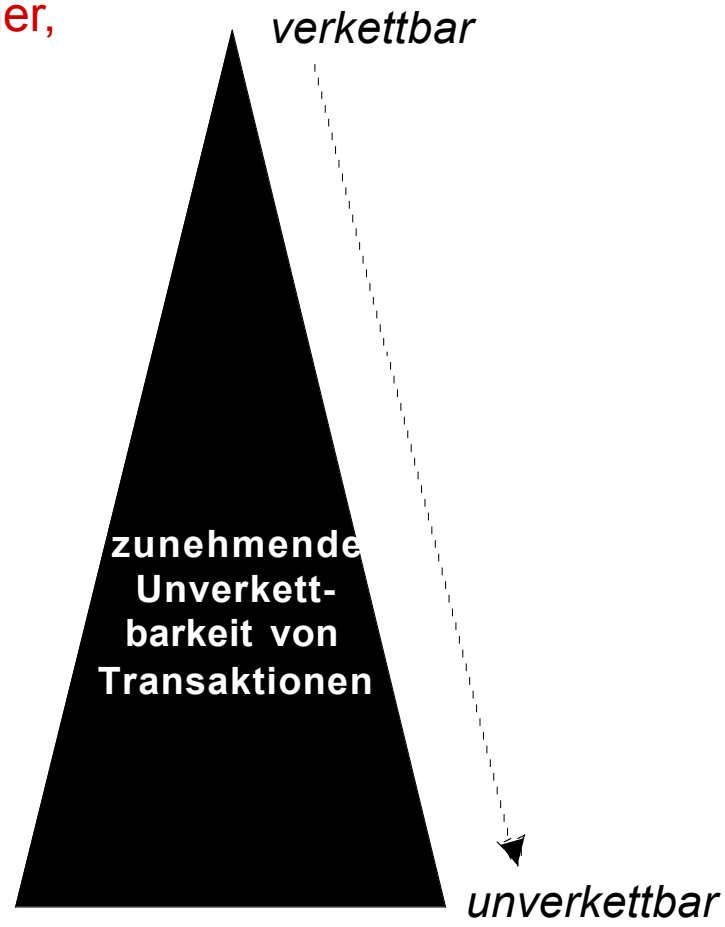
Initial unverkettetes Pseudonym:

Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn nur dem Inhaber bekannt.

Biometrische Merkmale; DNA (solange keinerlei Register)

Pseudonyme: Verwendungszusammenhang => Halbordnung





A → B bedeutet „B ermöglicht stärkere Unverkettbarkeit als A“

Notationen: Übergabe einer signierten Nachricht von X an Y

Funktionale Schreibweise

Signieren der Nachricht N:

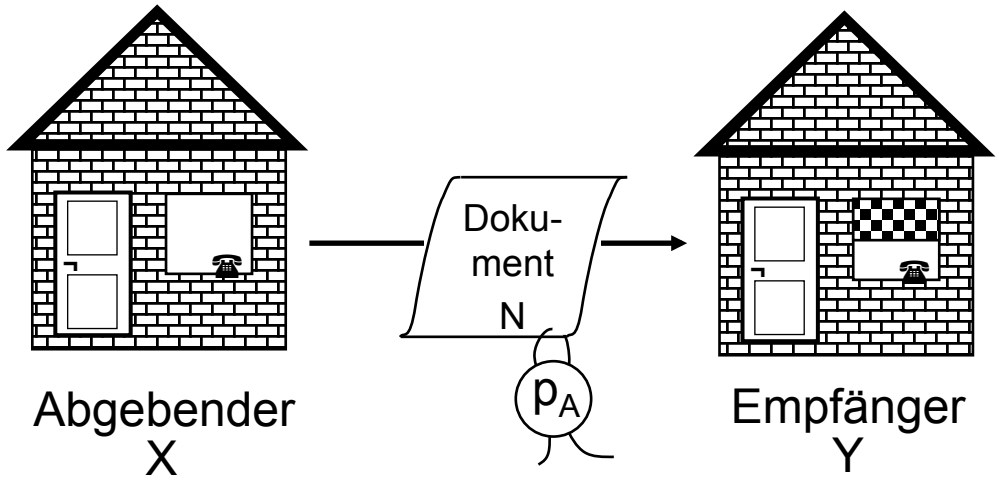
$s_A(N)$

X —— N, $s_A(N)$ ⟶ Y

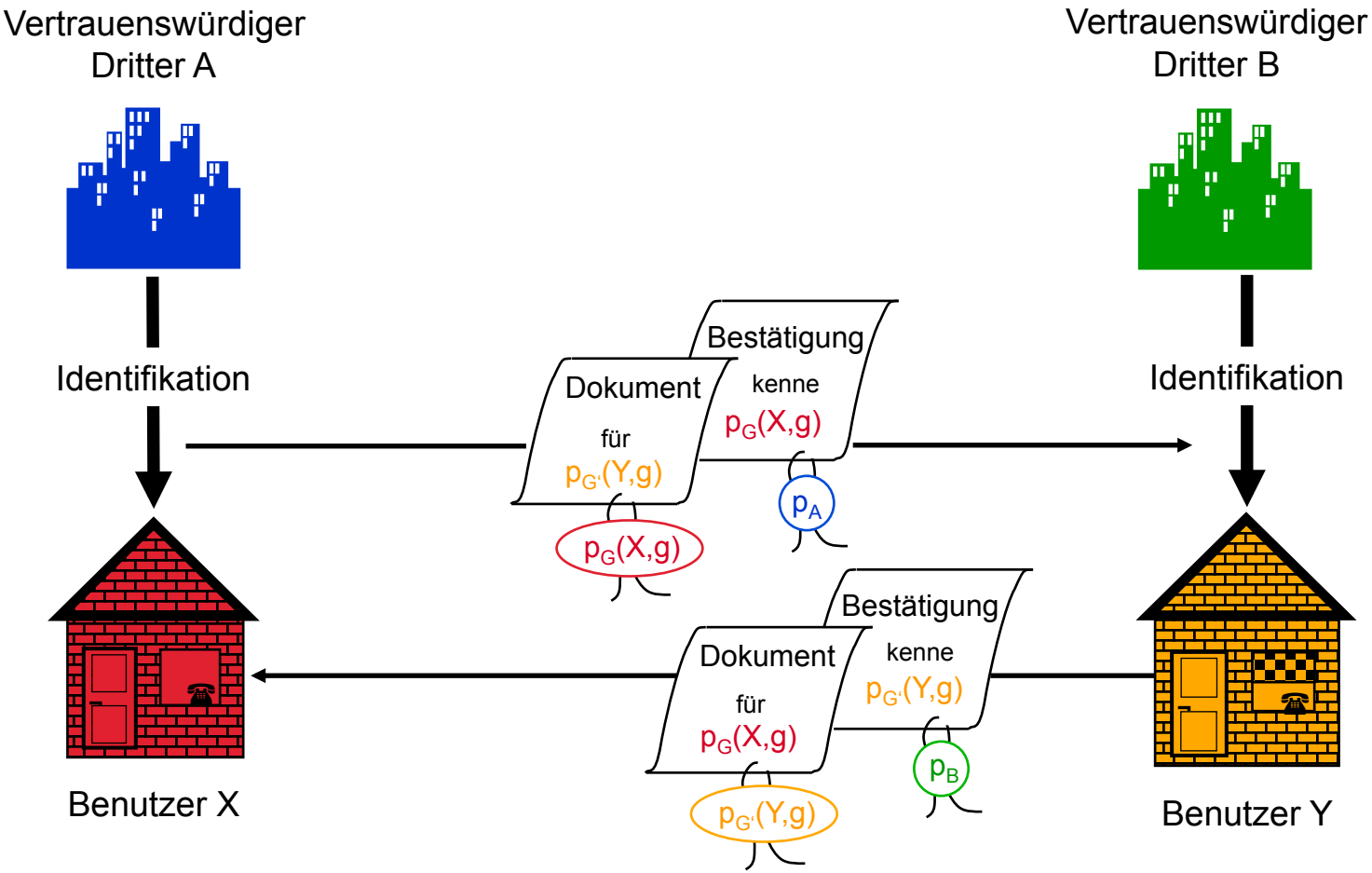
Testen der Signatur:

t_A (N, $s_A(N)$) ?

Graphische Schreibweise



Authentisierte anonyme Erklärungen zwischen deanonymisierbaren Geschäftspartnern

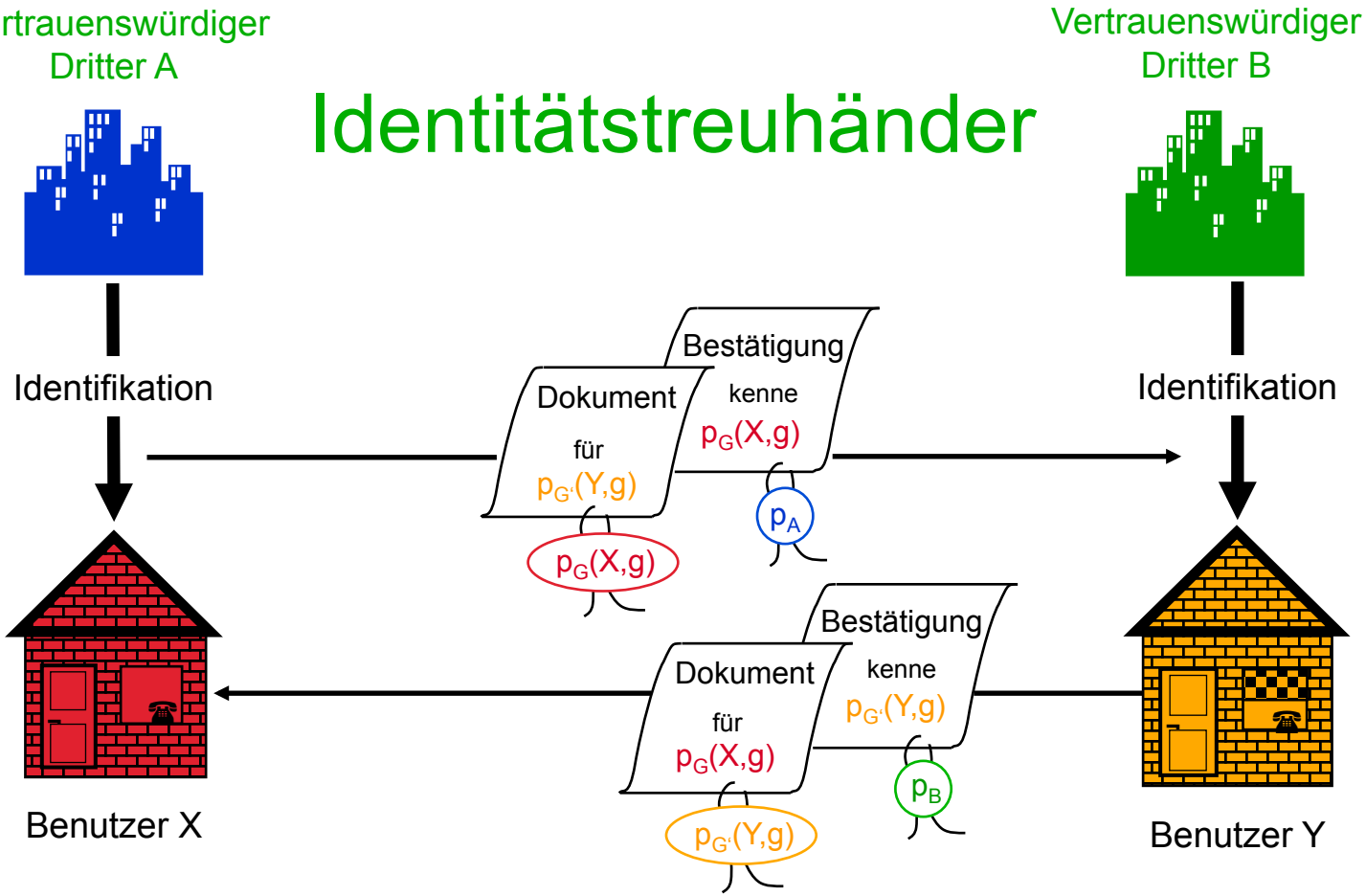


Verallgemeinerung:

$$X \rightarrow B_1 \rightarrow B_2 \rightarrow \ldots \rightarrow B_n \rightarrow Y$$
$$\searrow\ B'_1 \rightarrow B'_2 \rightarrow \ldots \rightarrow B'_m \nearrow$$

Fehler-/ Angriffstoleranz (vgl. MIXe)

Authentisierte anonyme Erklärungen zwischen deanonymisierbaren Geschäftspartnern

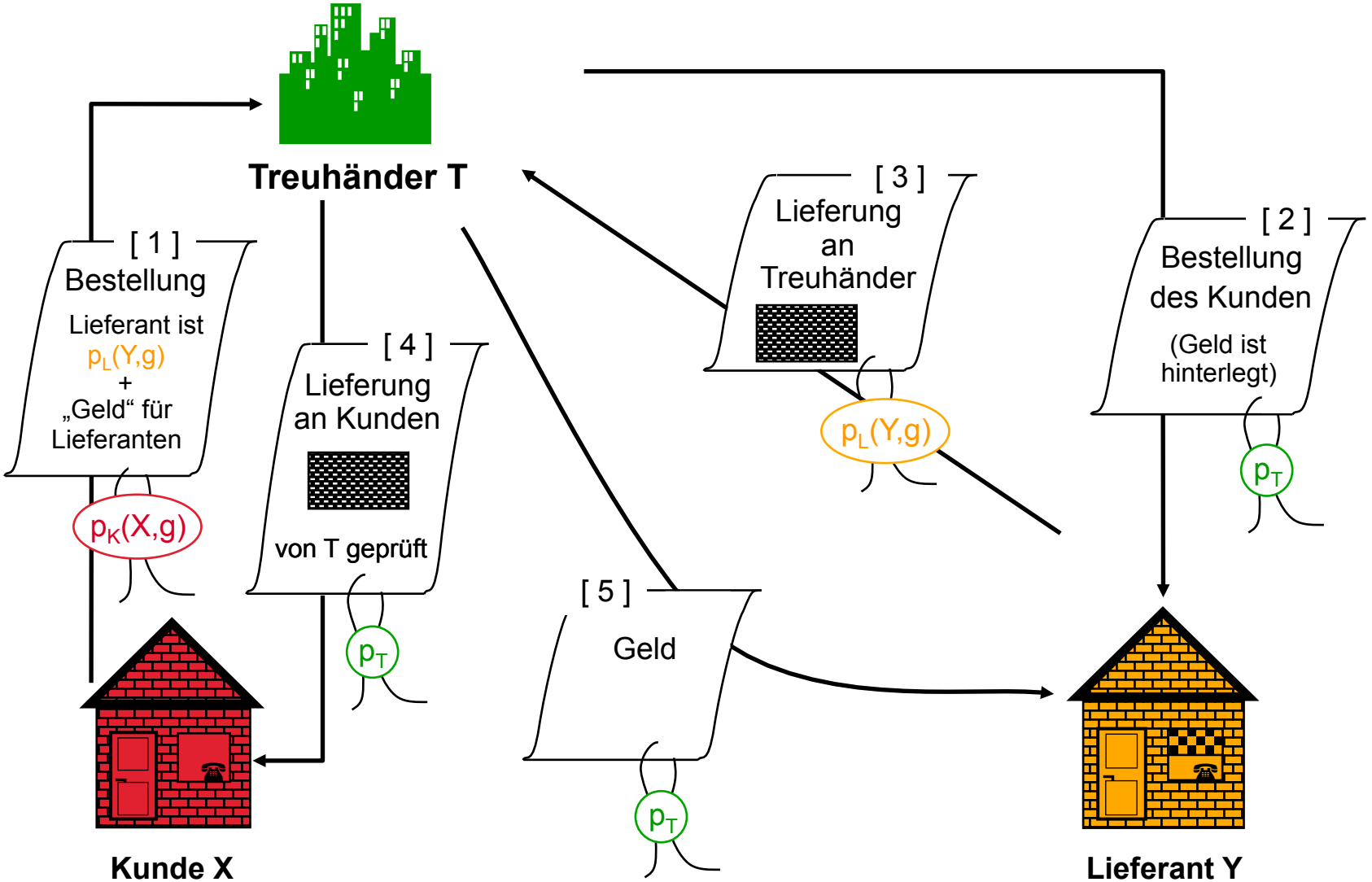


Verallgemeinerung:

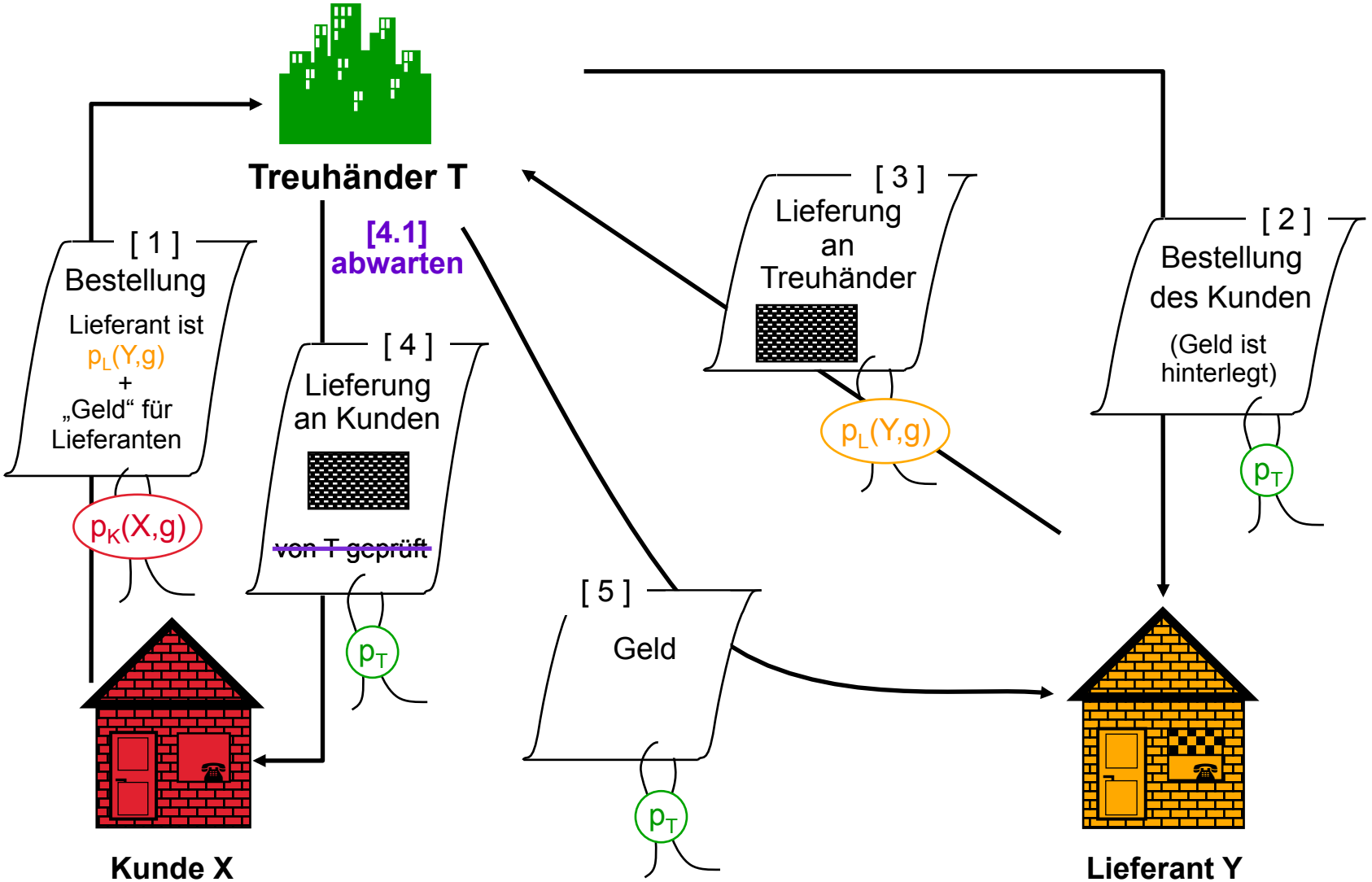
$$X \rightarrow B_1 \rightarrow B_2 \rightarrow \ldots \rightarrow B_n \rightarrow Y$$
$$\searrow\ B'_1 \rightarrow B'_2 \rightarrow \ldots \rightarrow B'_m \nearrow$$

Fehler-/ Angriffstoleranz (vgl. MIXe)

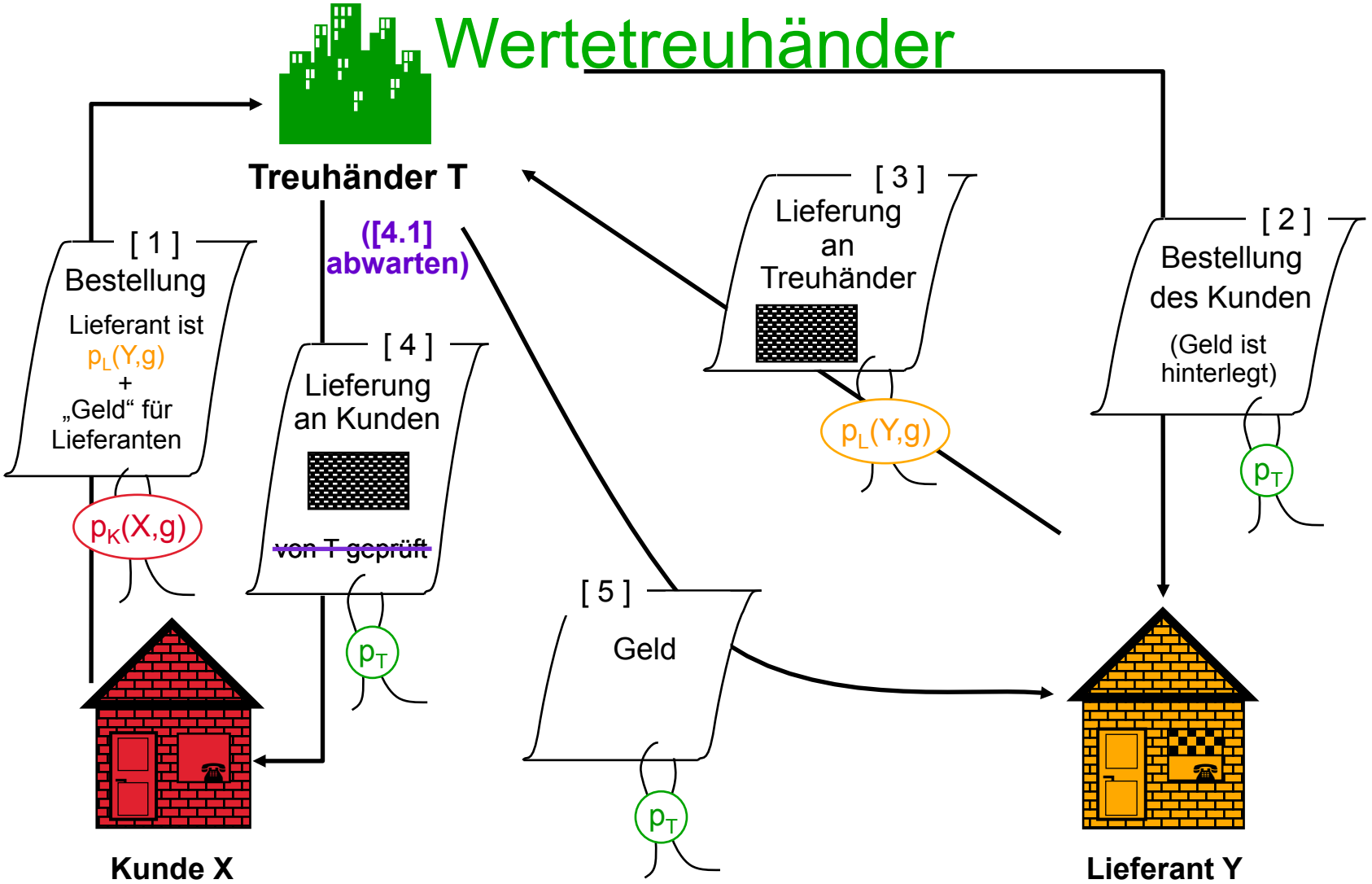
Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware prüfen kann



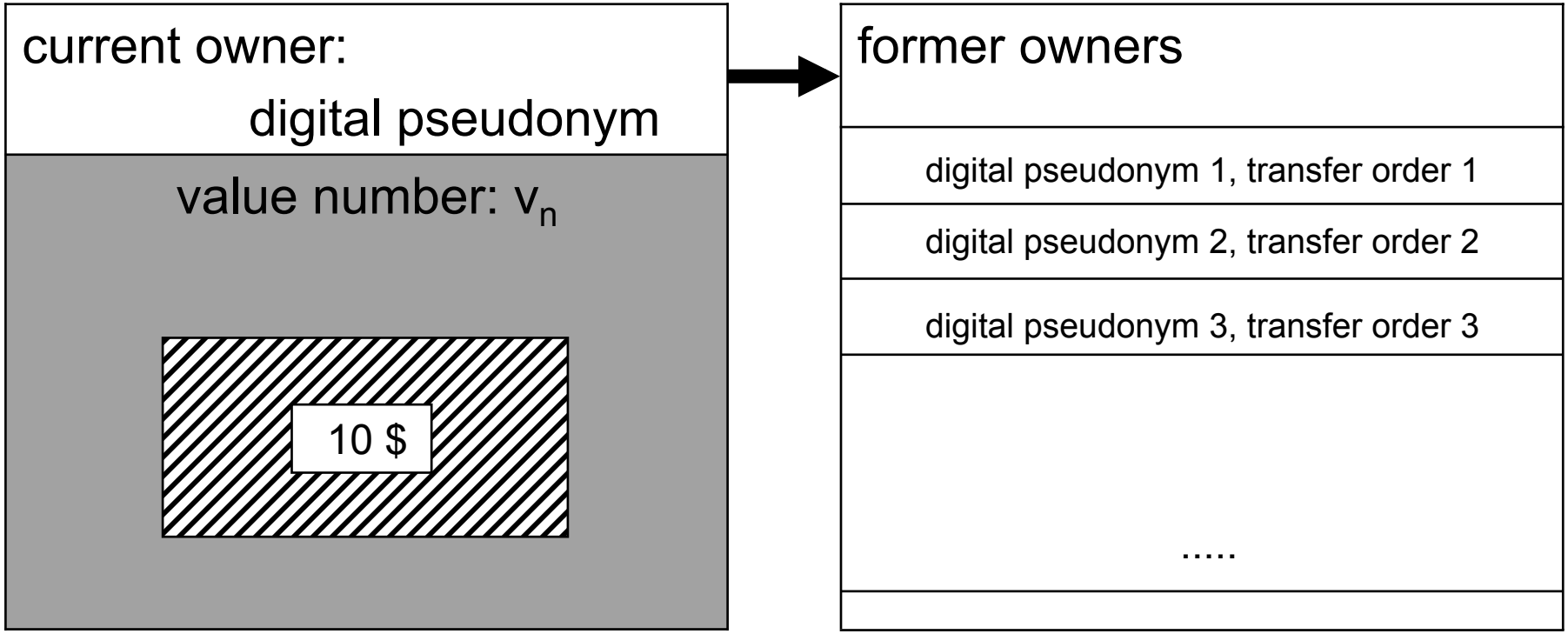
Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware nicht prüfen kann



Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware (nicht) prüfen kann

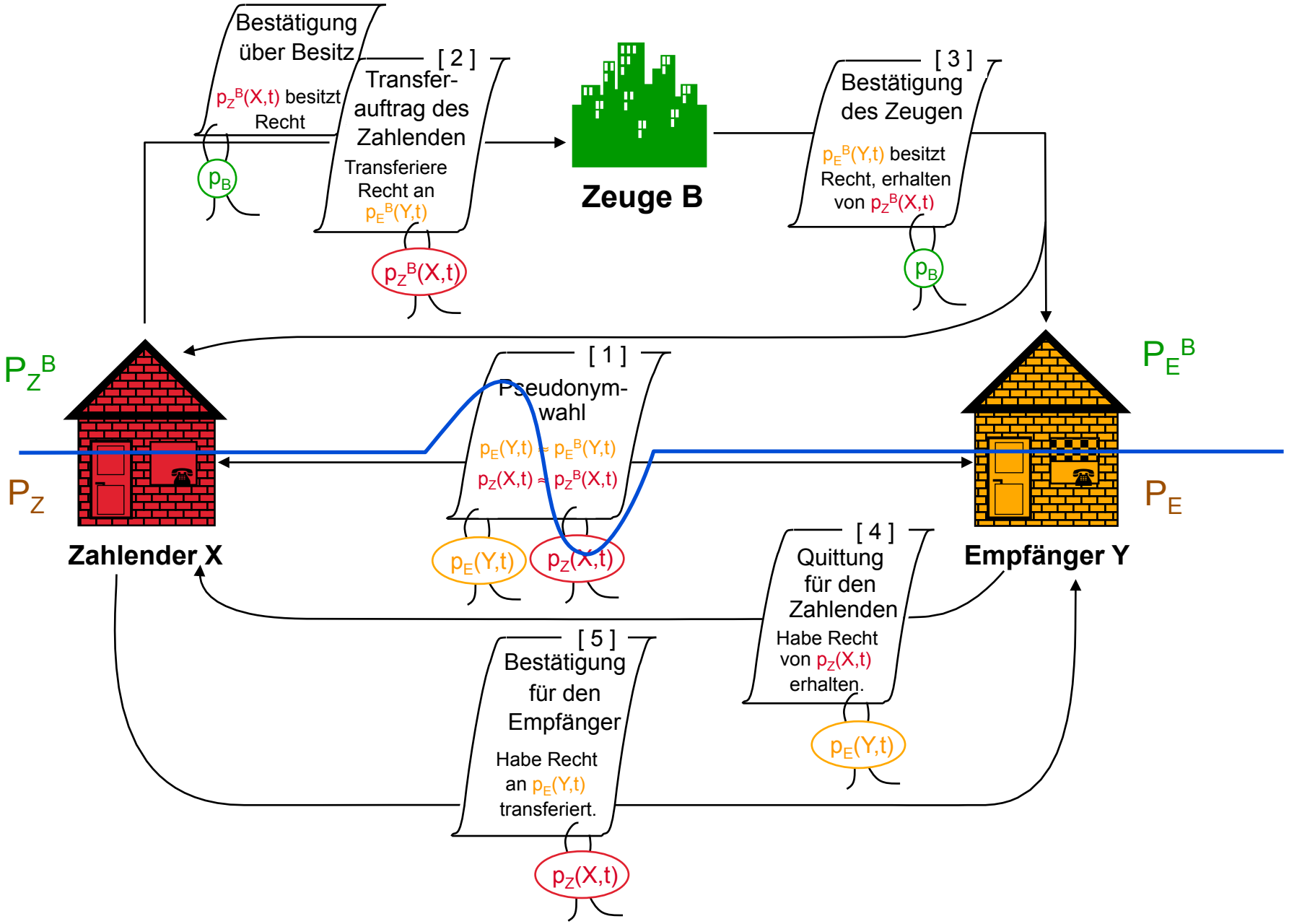


Anonym transferierbare Standardwerte

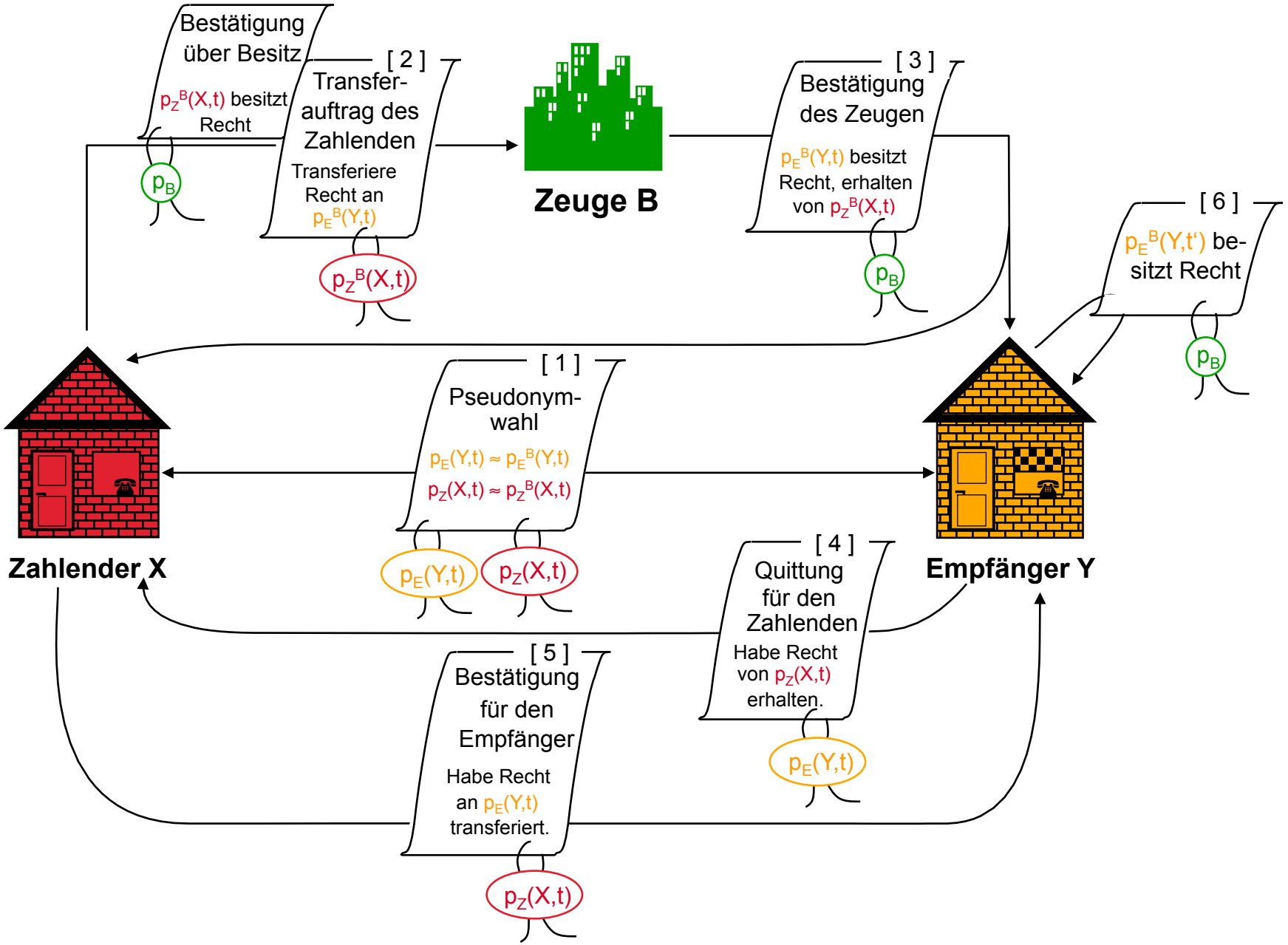


Anonymously transferable standard value

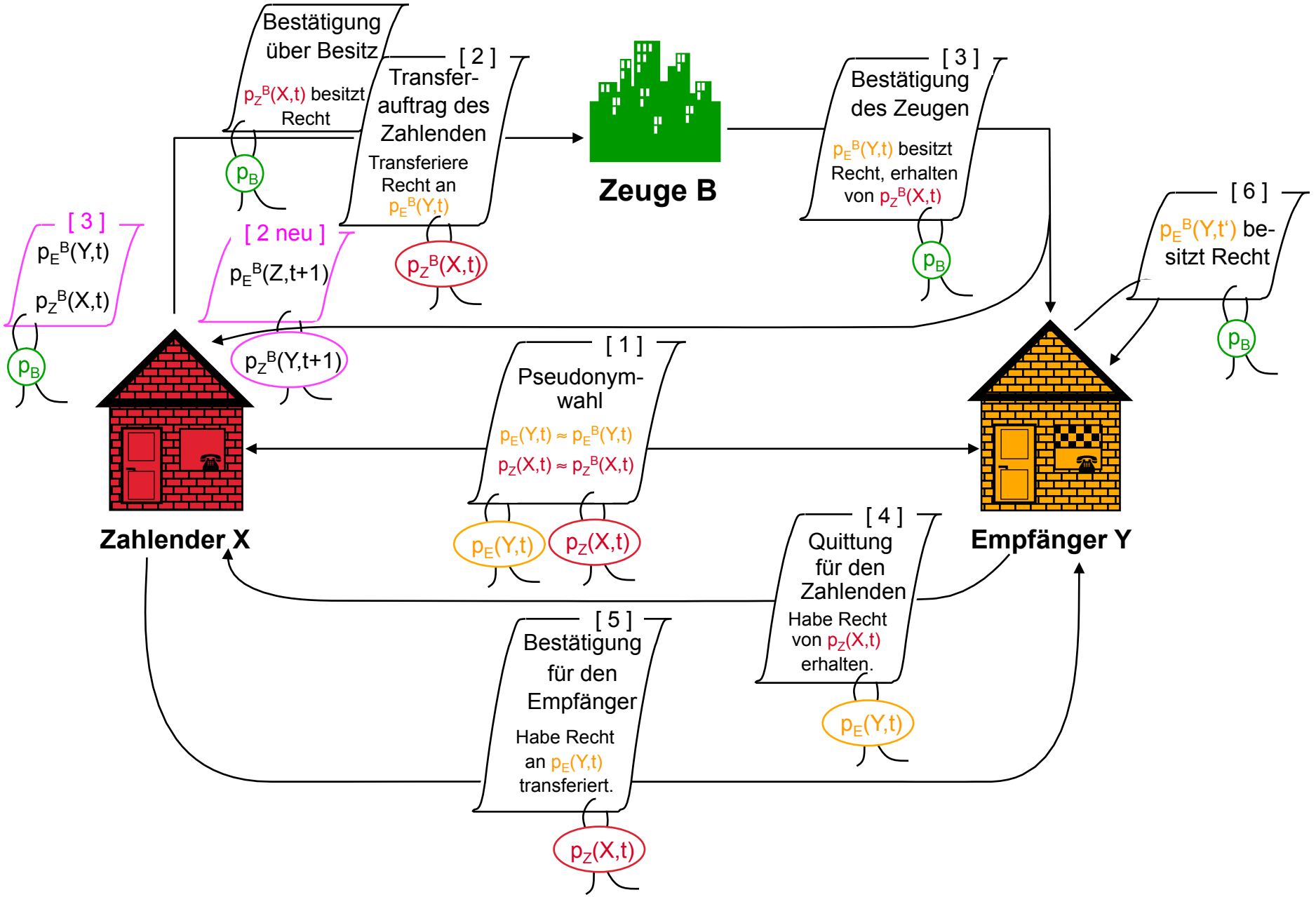
Grundschema eines sicheren und anonymen digitalen Zahlungssystems



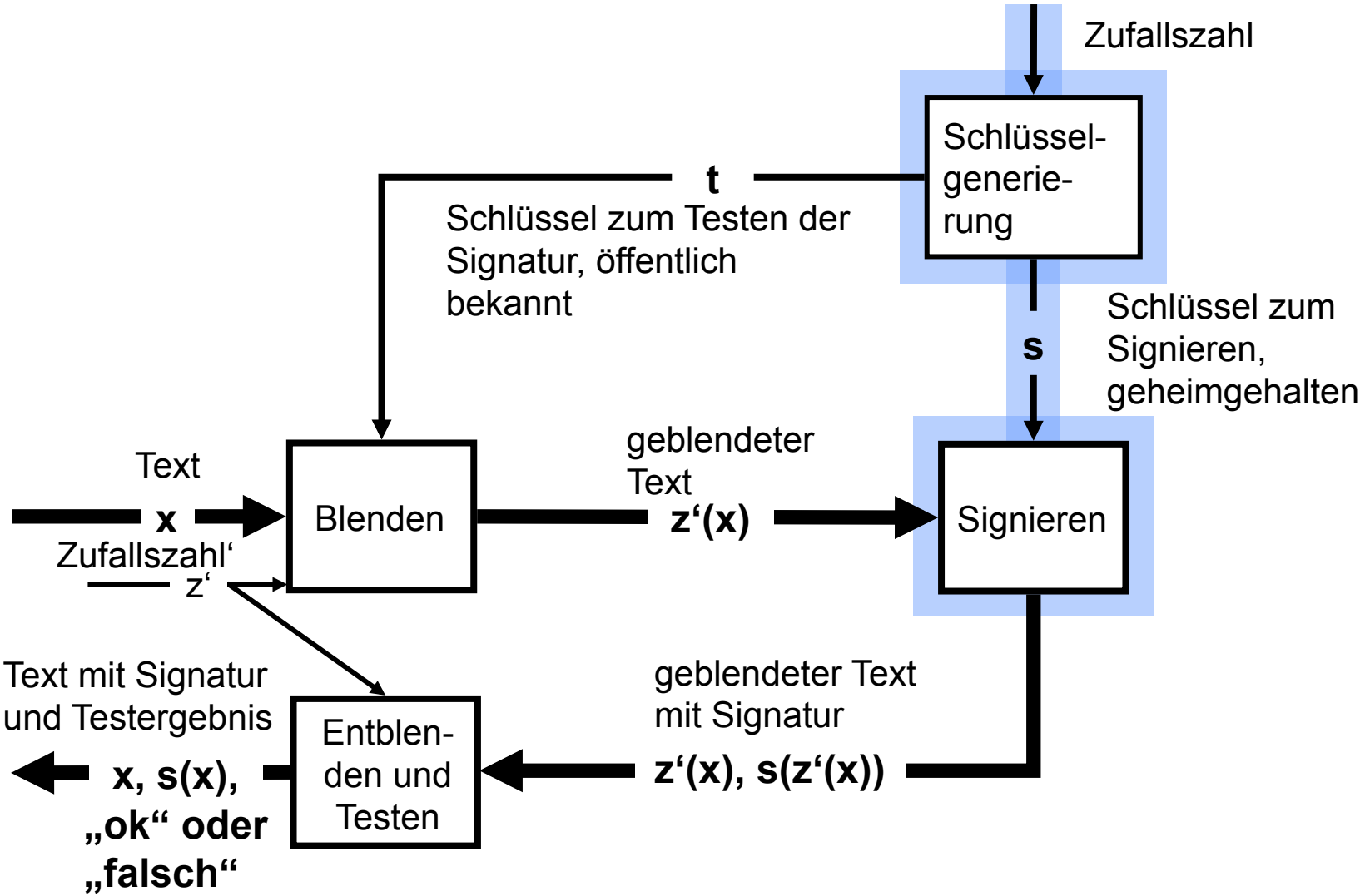
Umformen der Bestätigung des Zeugen



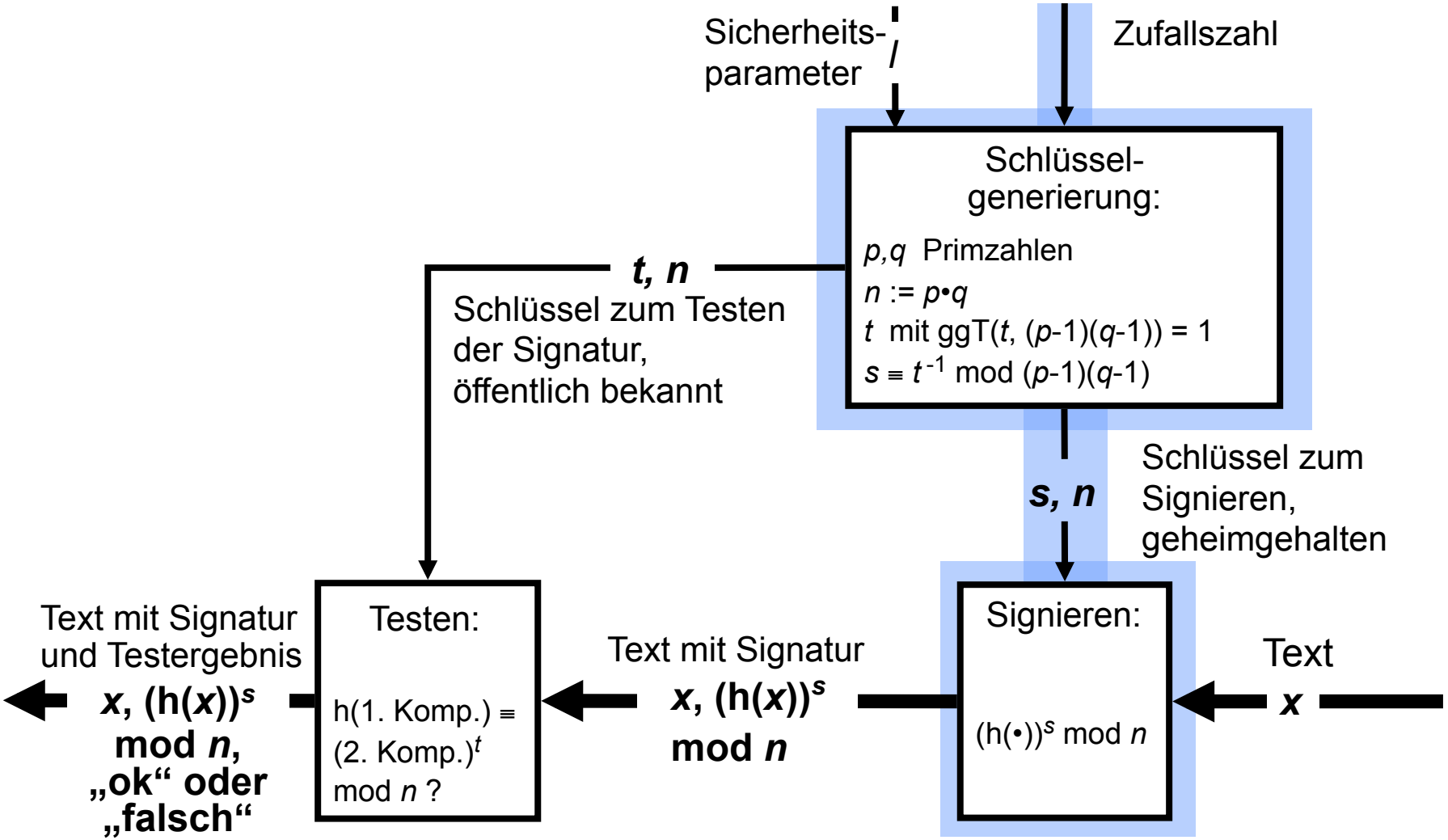
Die nächste Runde: Y in der Rolle Zahlender an Empfänger Z



Signatursystem zum blinden Leisten von Signaturen



RSA als digitales Signatursystem mit kollisionsresistenter Hashfunktion h



Einmal umrechenbare Beglaubigung

Empfänger

Wähle Pseudonym

p

(Testschlüssel eines bel. Sign.-S.)

Kollisionsresistente Hashfunktion **h**

p,h(p)

Wähle $r \in_R Z_n^*$

(p,h(p))•r^t →

← **(p,h(p))^s•r**

Multipliziere mit

r^{-1}

erhalte

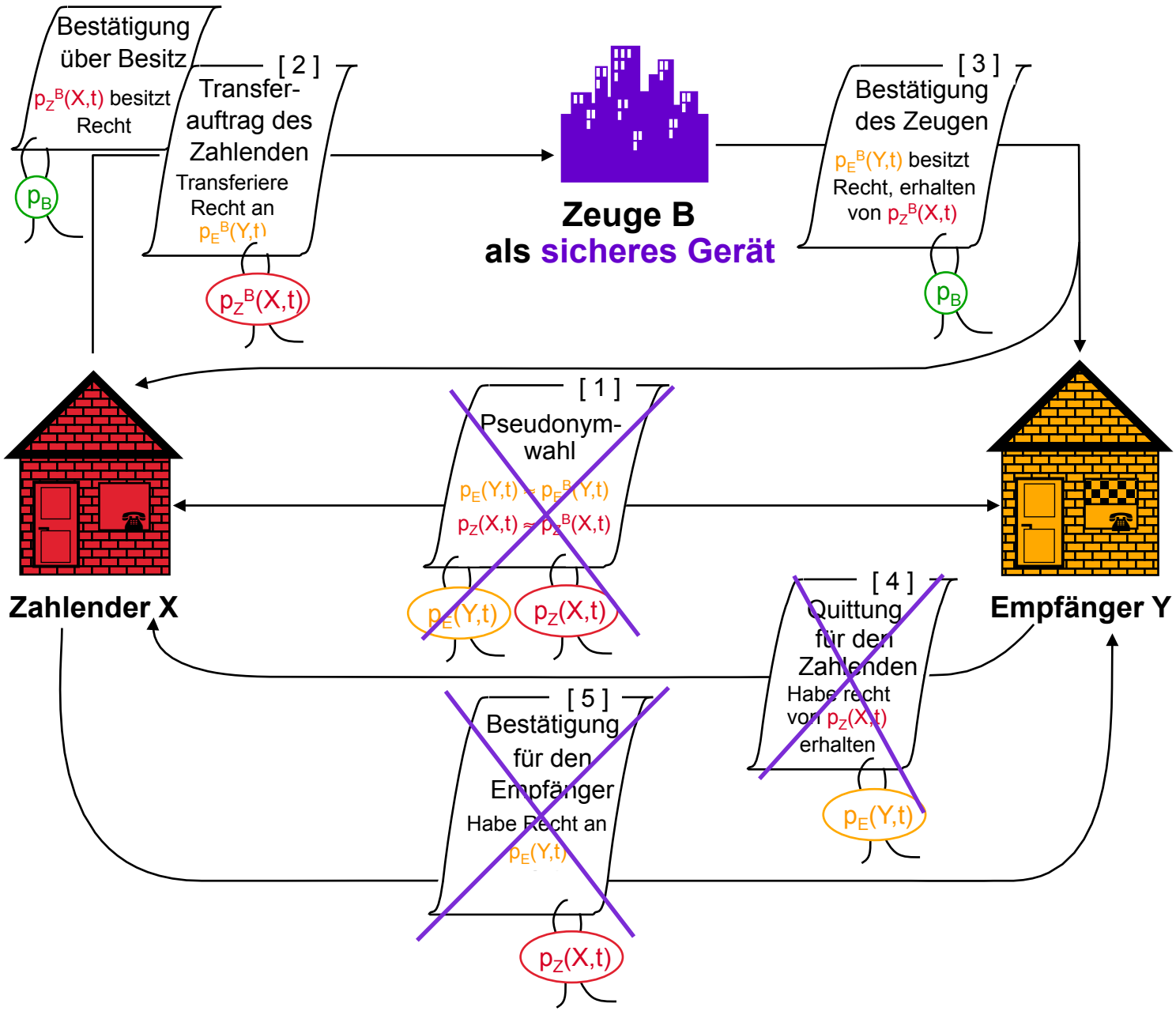
(p,h(p))^s

Aussteller

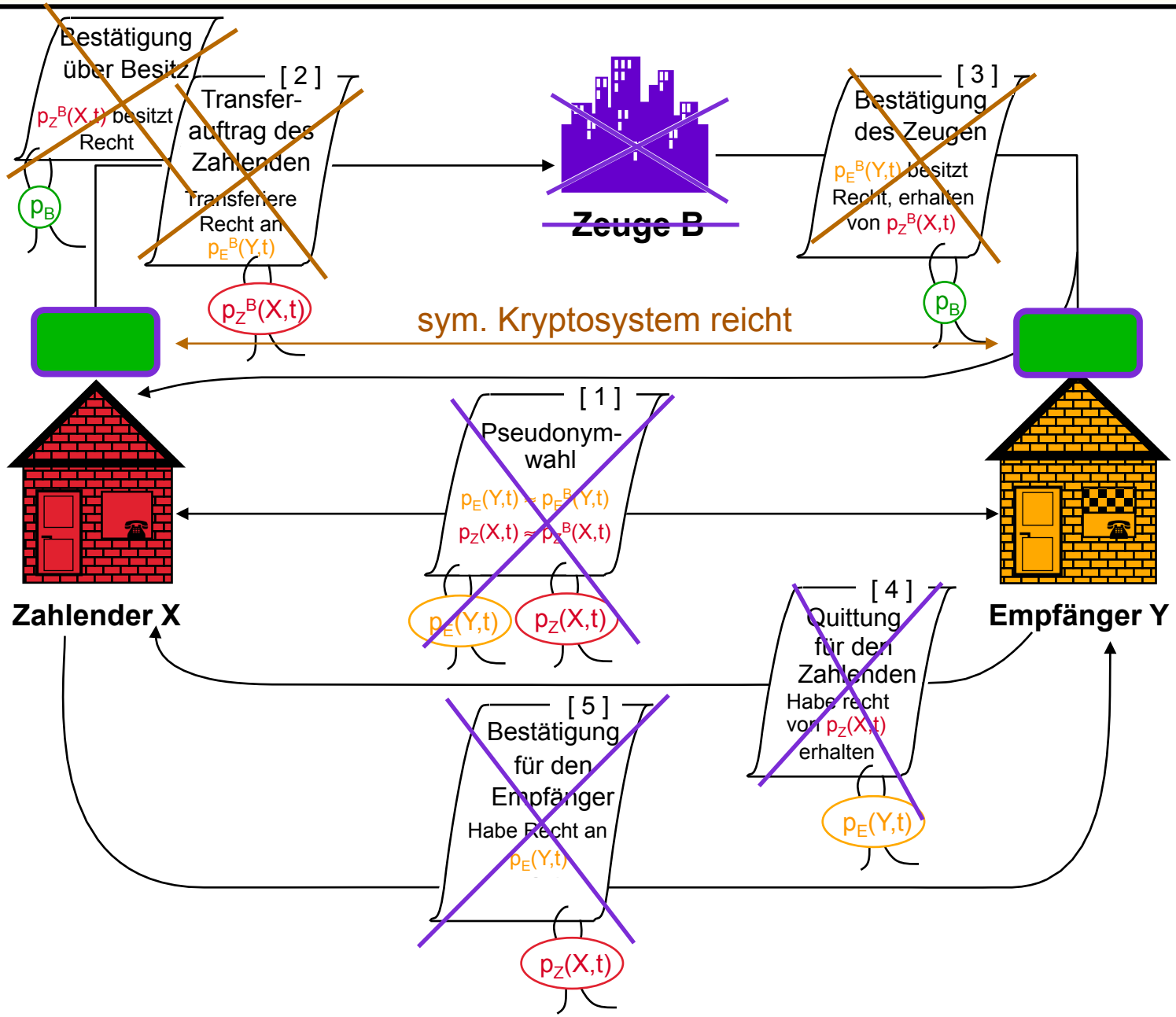
Öffentlicher RSA-Testschlüssel ***t,n***

((p,h(p))•r^t)^s

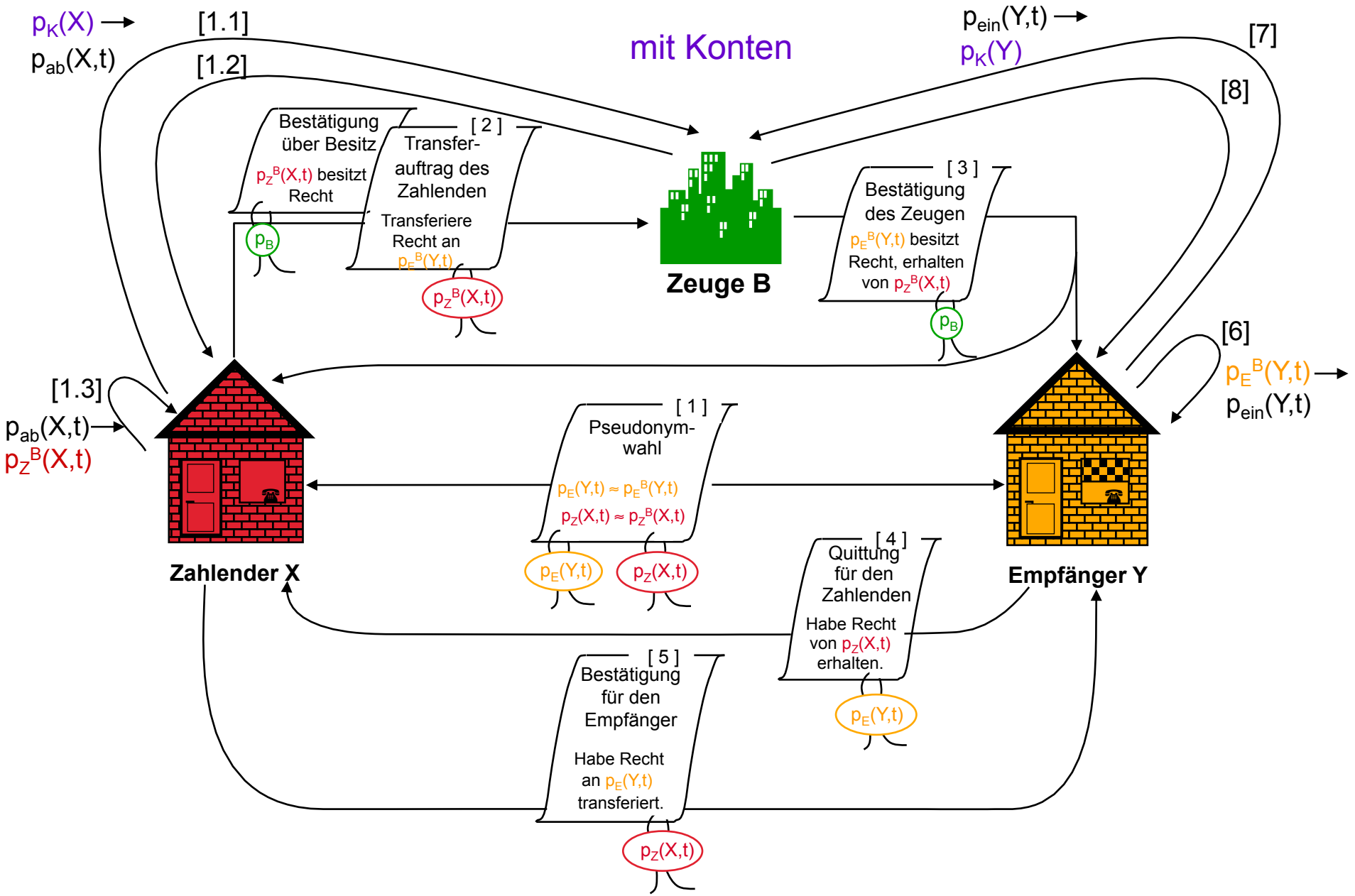
Sicheres Gerät: 1. Möglichkeit



Sicheres Gerät: 2. Möglichkeit



Sicheres und anonymes digit. Zahlungssystem mit Konten



Offline Zahlungssystem

Zahlungssysteme mit Sicherheit durch Deanonymisierbarkeit

k	Sicherheitsparameter
I	Identität des die Banknote Ausgebenden
r_i	zufällig gewählt ($1 \leq i \leq k$)
C	Commitment-Schema mit informationstheoretischer Geheimhaltung

Blind unterschriebene Banknote:

$$s_{Bank}(C(r_1), C(r_1 \oplus I), C(r_2), C(r_2 \oplus I), ..., C(r_k), C(r_k \oplus I)),$$

Empfänger entscheidet, ob er r_i **oder** $r_i \oplus I$ aufdeckt haben will.
(One-time pad bewahrt Anonymität.)

Ausgabe an zwei brave Empfänger:
W'keit ($\exists i$: Bank erfährt r_i und $r_i \oplus I$) $\geq 1-e^{-c \cdot k}$
(Ausgebender identifizierbar)

Ausblick

Rechtssicherheit vs. Haftung

online / offline

Debit / Pay-now / Kredit

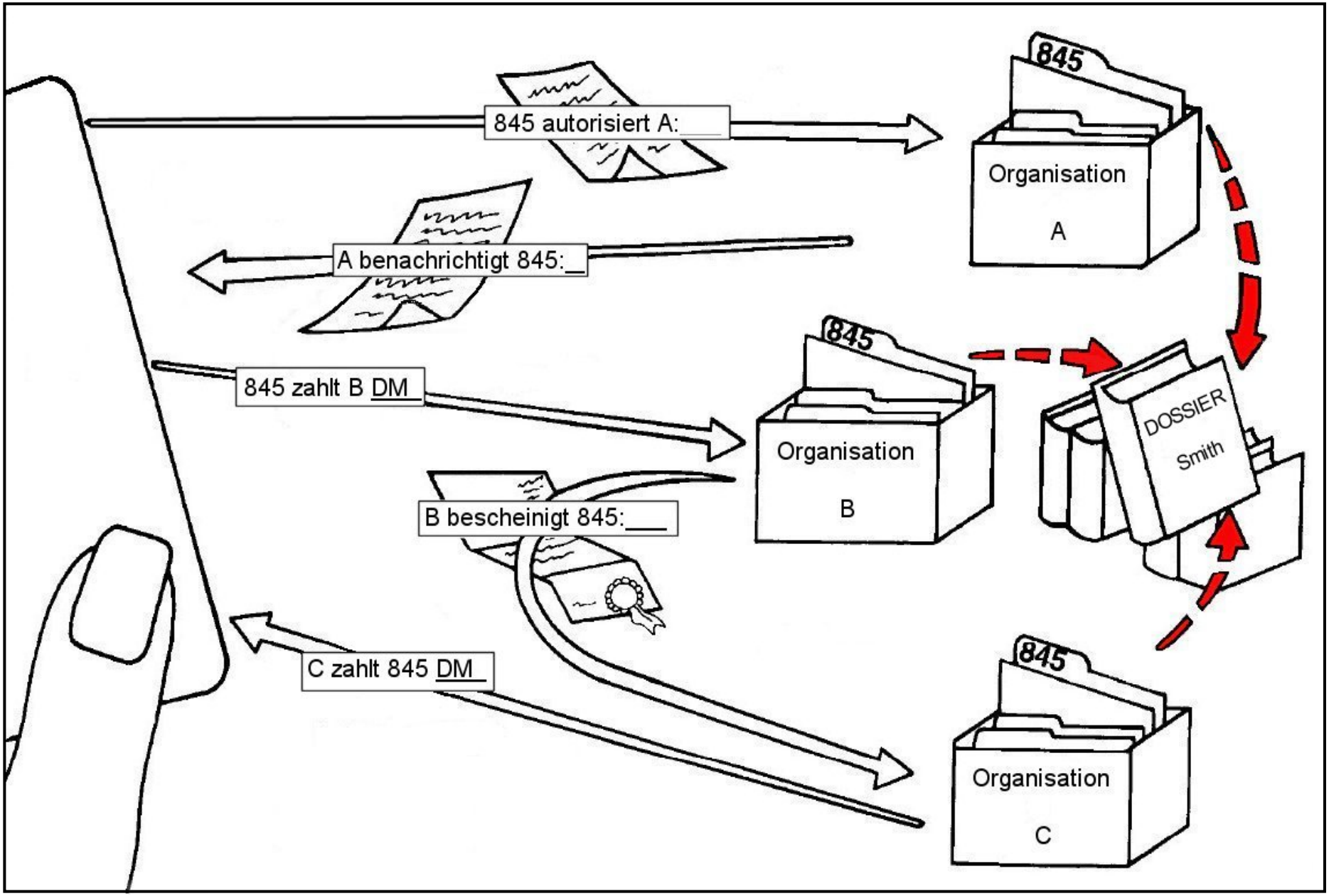
nur spezielle Software oder auch Hardware ?

universelles Zahlungsmittel oder vielfältige Gutscheinsysteme ?

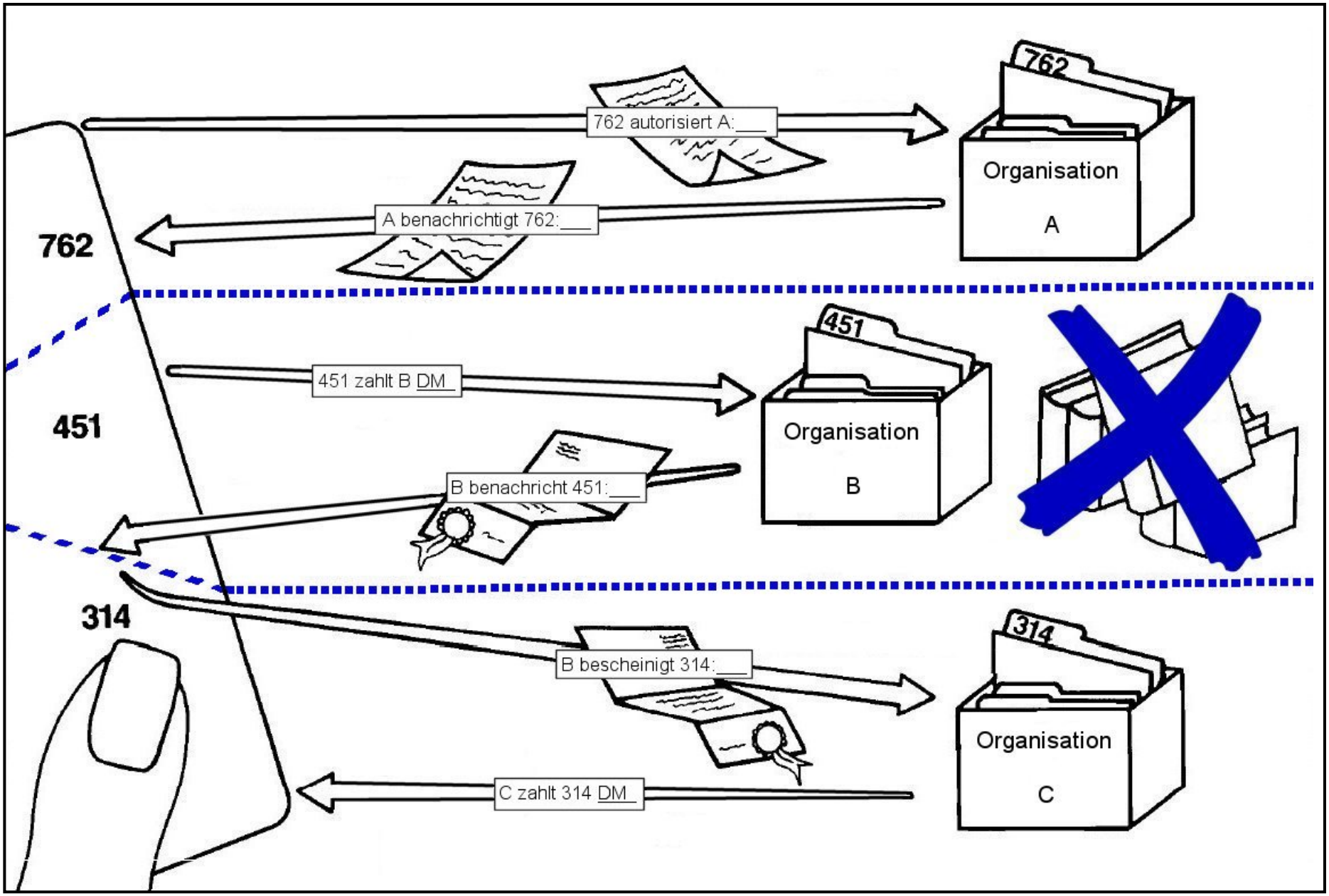
eine oder mehrere Währungen ?

ein oder mehrere Systeme ?

Personenkennzeichen



Rollenpseudonyme
(Geschäftsbeziehungs-, Transaktionspseudonyme)



Mehrseitige Sicherheit bei digitalen Zahlungssystemen

Identifizierung bei anonymen Zahlungssystemen im Betrugsfall

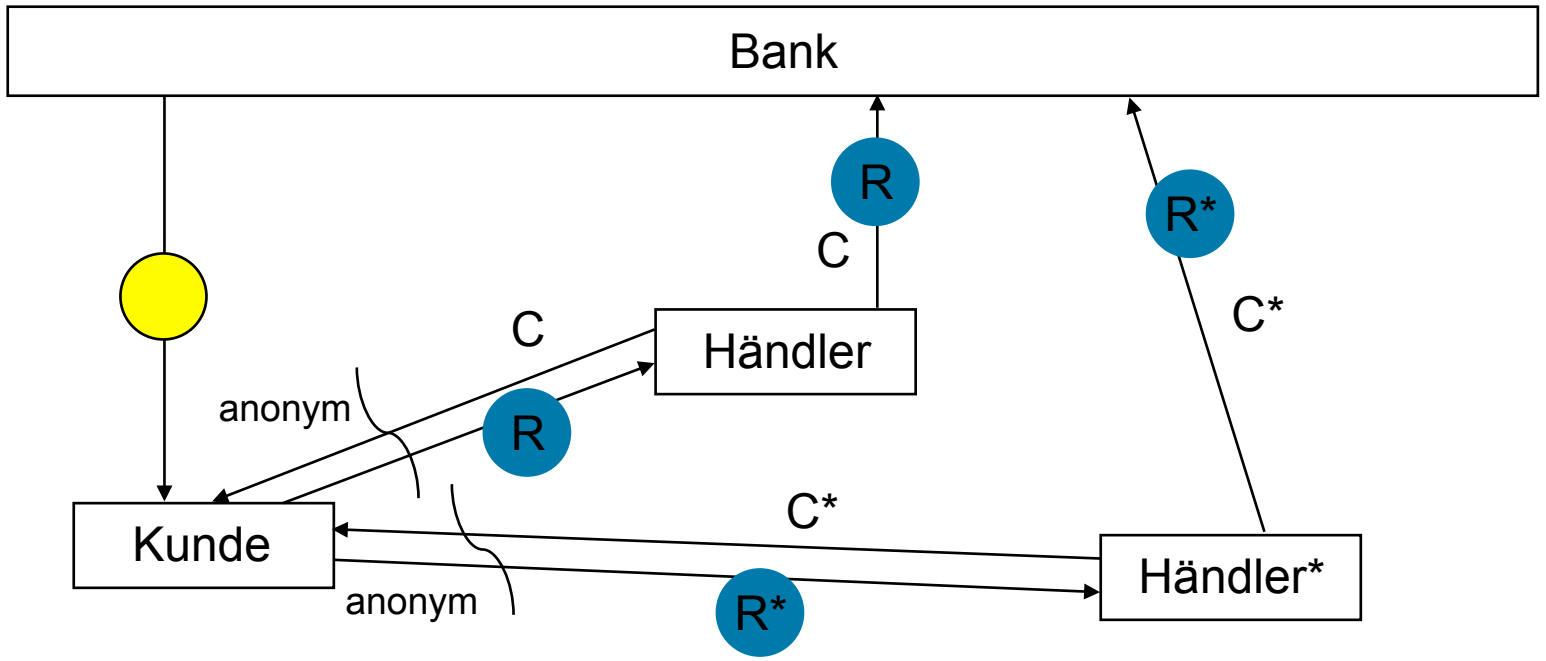


Abb.: Identifizierung im Betrugsfall

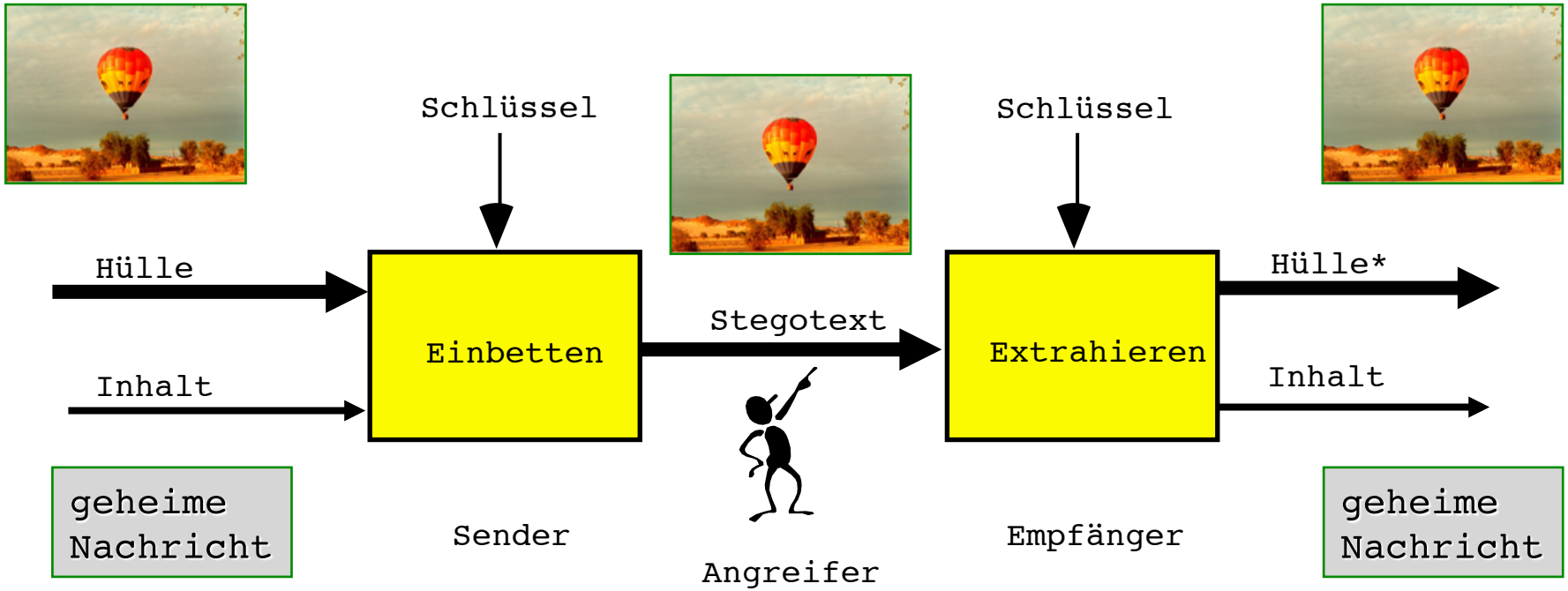
C, C* Challenges (mit Händler-ID)
R, R* Responses

Beweiskräftige Identifizierung des Kunden durch
verschiedene Responses zur gleichen dig. Münze möglich

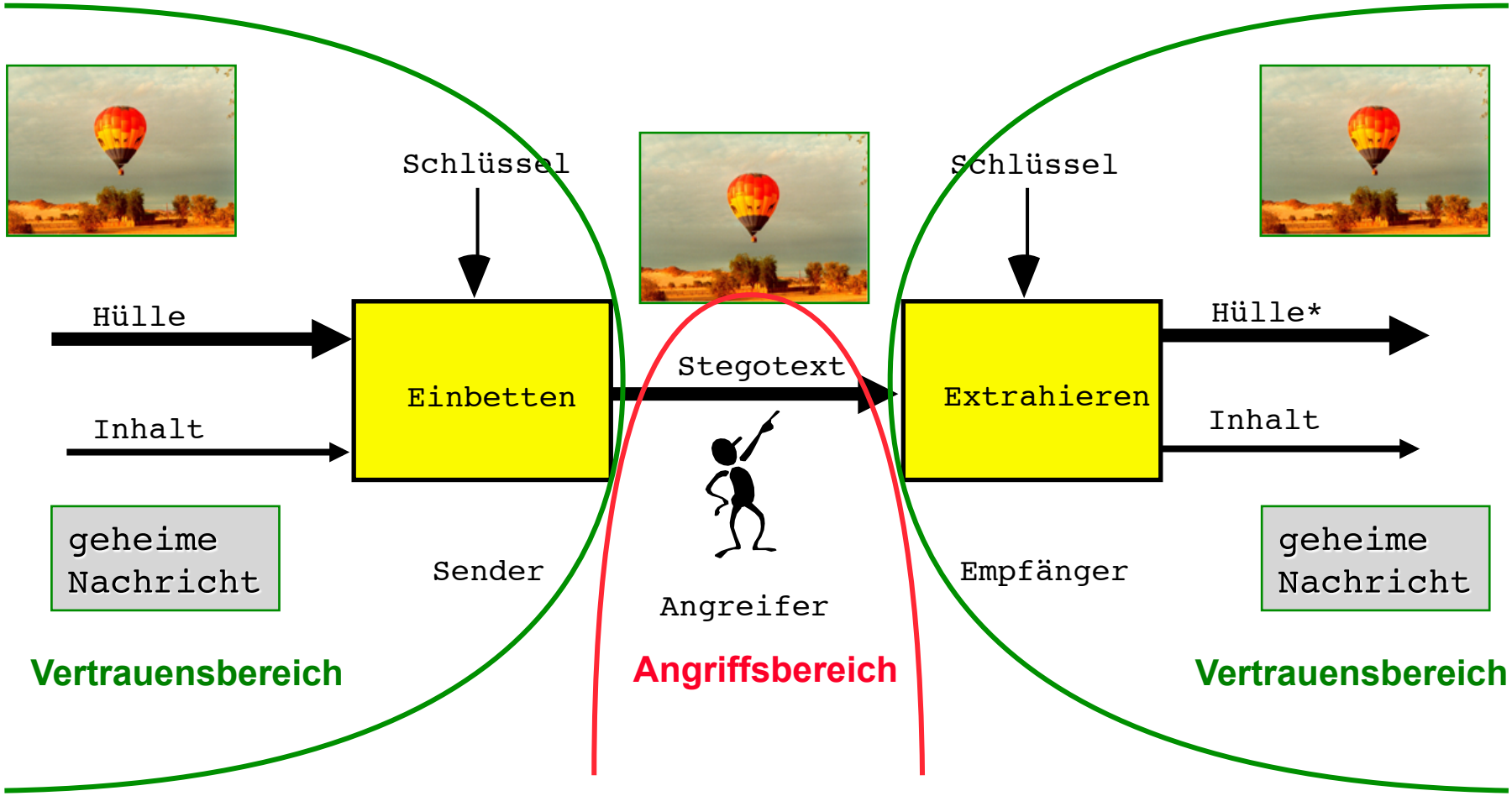
Kryptographie und ihre rechtliche (Un-)Regulierbarkeit

- Kryptosysteme *(kennen Sie bereits)*
- Stegosysteme
- Vorschläge zur Kryptoregulierung
- Technische Randbedingungen jeder Kryptoregulierung
  - Sichere digitale Signaturen → sichere Konzelation
  - Key Escrow Konzelation ohne Dauerüberwachung → Konzelation ohne Key Escrow
  - Symmetrische Authentikation → Konzelation
  - Multimediakommunikation → Steganographie
  - Schlüssel für Kommunikation und geheime Signierschlüssel sind jederzeit ersetzbar → Key Escrow als Schlüsselbackup ist unsinnig
- Vorschläge zur Kryptoregulierung schaden nur den Braven

Steganographie

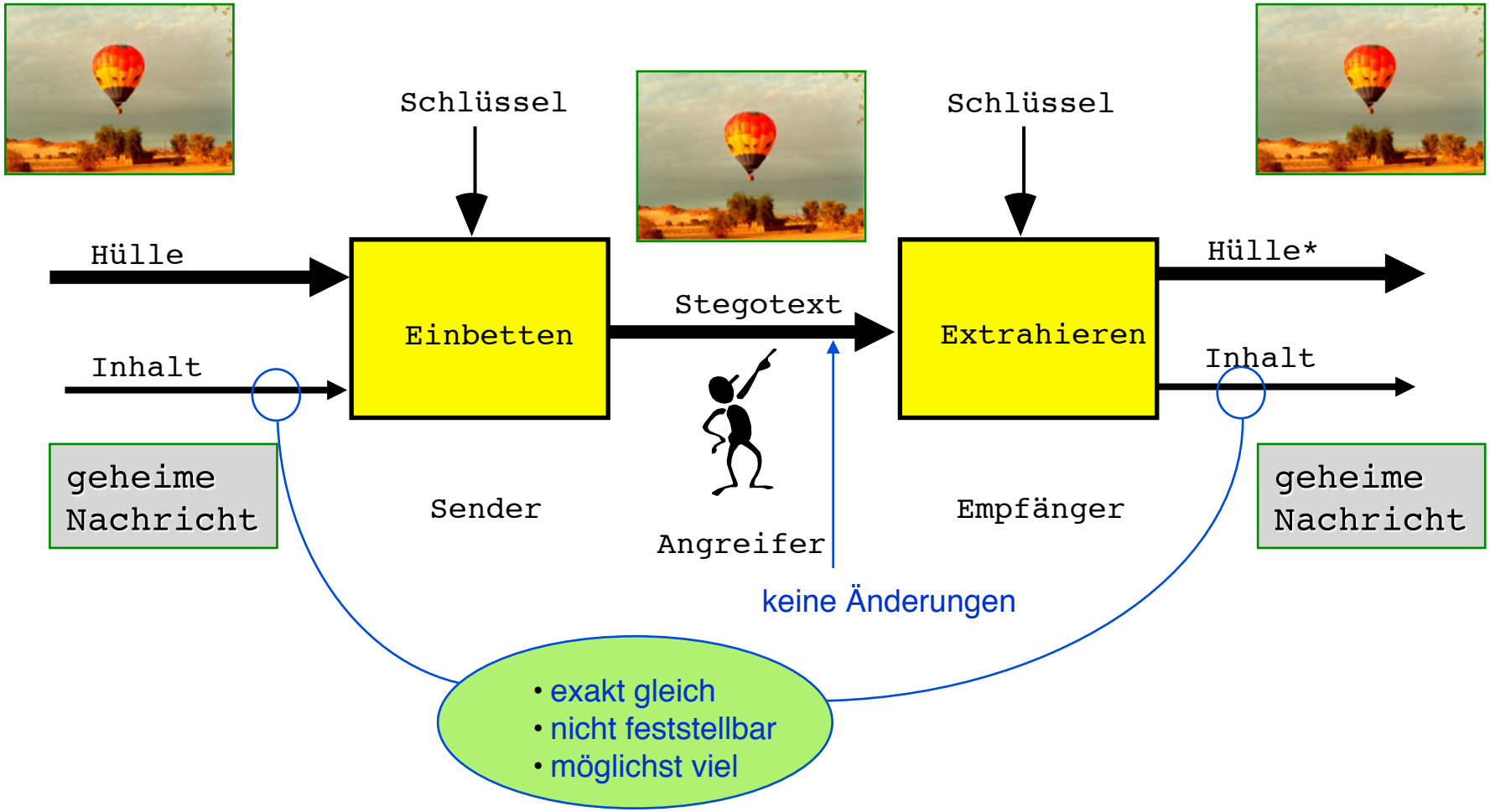


Steganographie



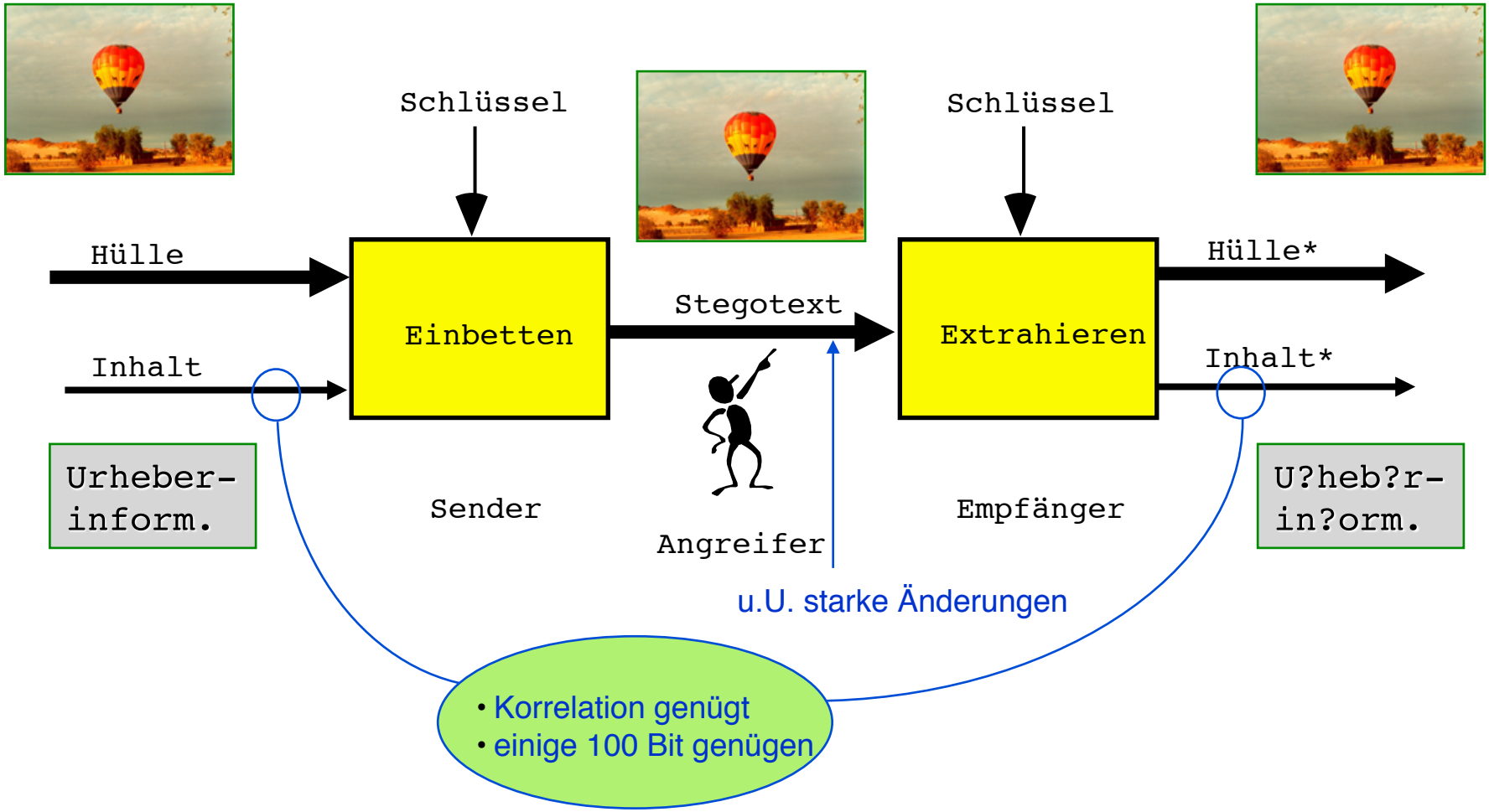
Steganographie

Steganographie: Vertraulichkeit der Vertraulichkeit



Steganographie

Steganographie: Watermarking und Fingerprinting



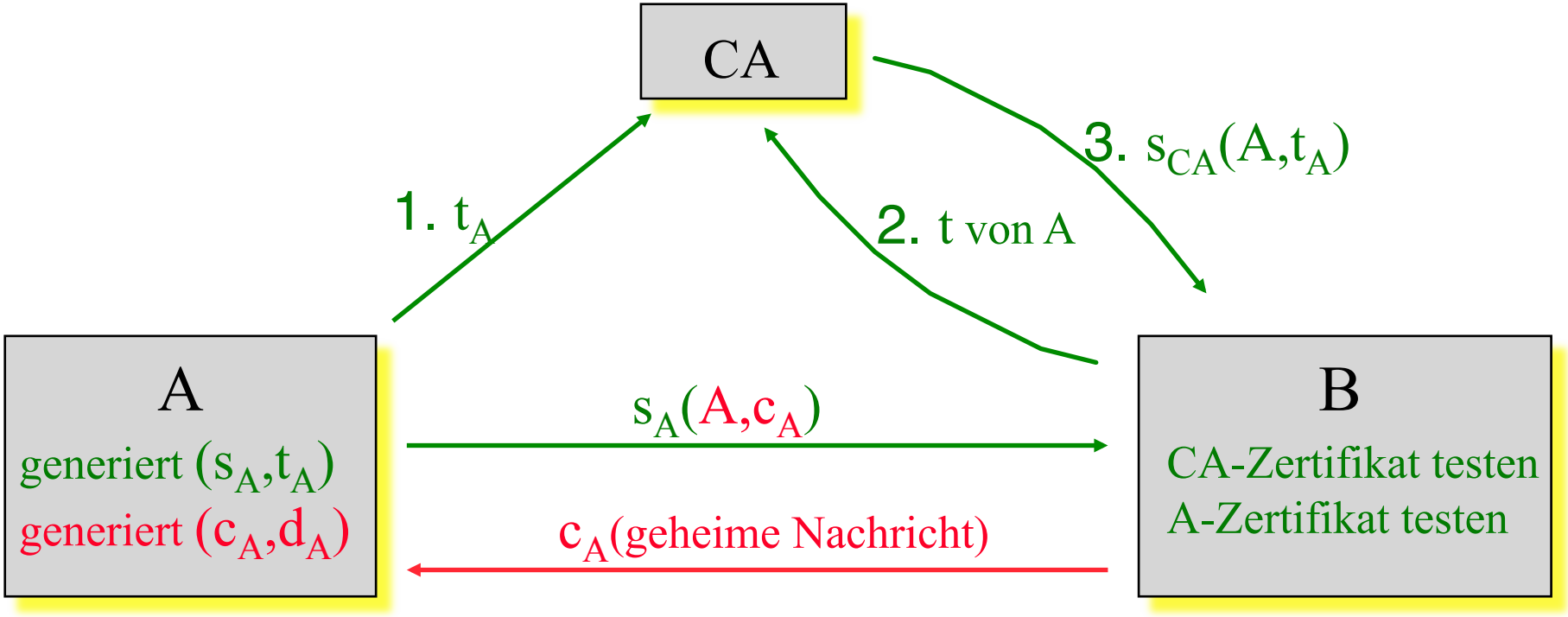
Vorschläge zur Kryptoregulierung ?

- Würden Sie Kryptographie regulieren, um die Verbrechensbekämpfung zu unterstützen ?
- Wenn ja: Wie ?

Vorschläge zur Kryptoregulierung !

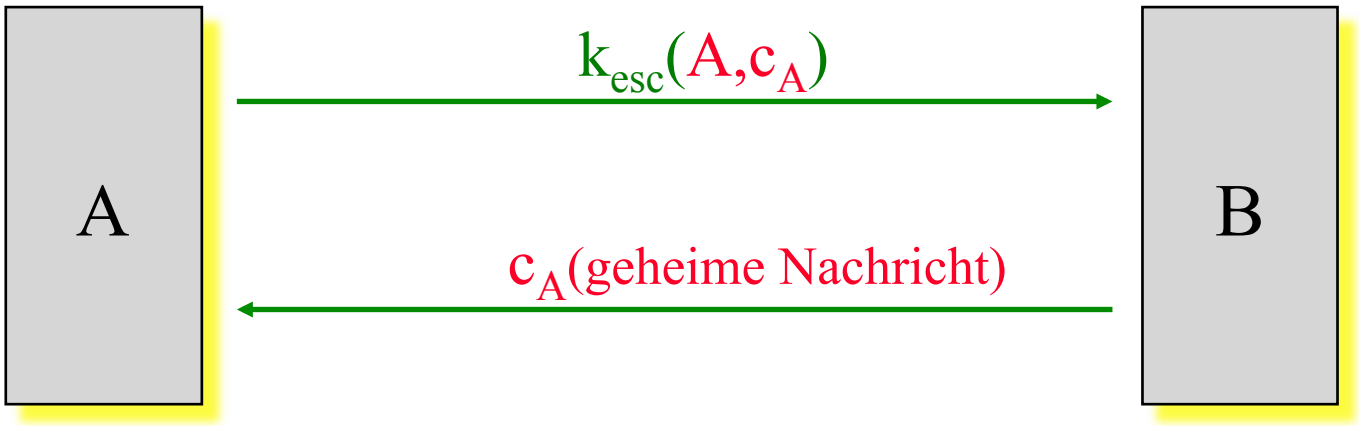
- Kryptographie zur Konzelation verbieten
- Kryptographie zur Konzelation verbieten – außer sehr kurze Schlüssellängen
- Kryptographie zur Konzelation verbieten – außer Key Escrow bzw. Key Recovery Systeme
- Öffentliche Chiffrierschlüssel nur in PKI aufnehmen, wenn geheimer Dechiffrierschlüssel hinterlegt
- Pflicht, bei Strafverfahren Entschlüsselungsschlüssel zu übergeben

Sichere Digitale Signaturen —> sichere Konzelation



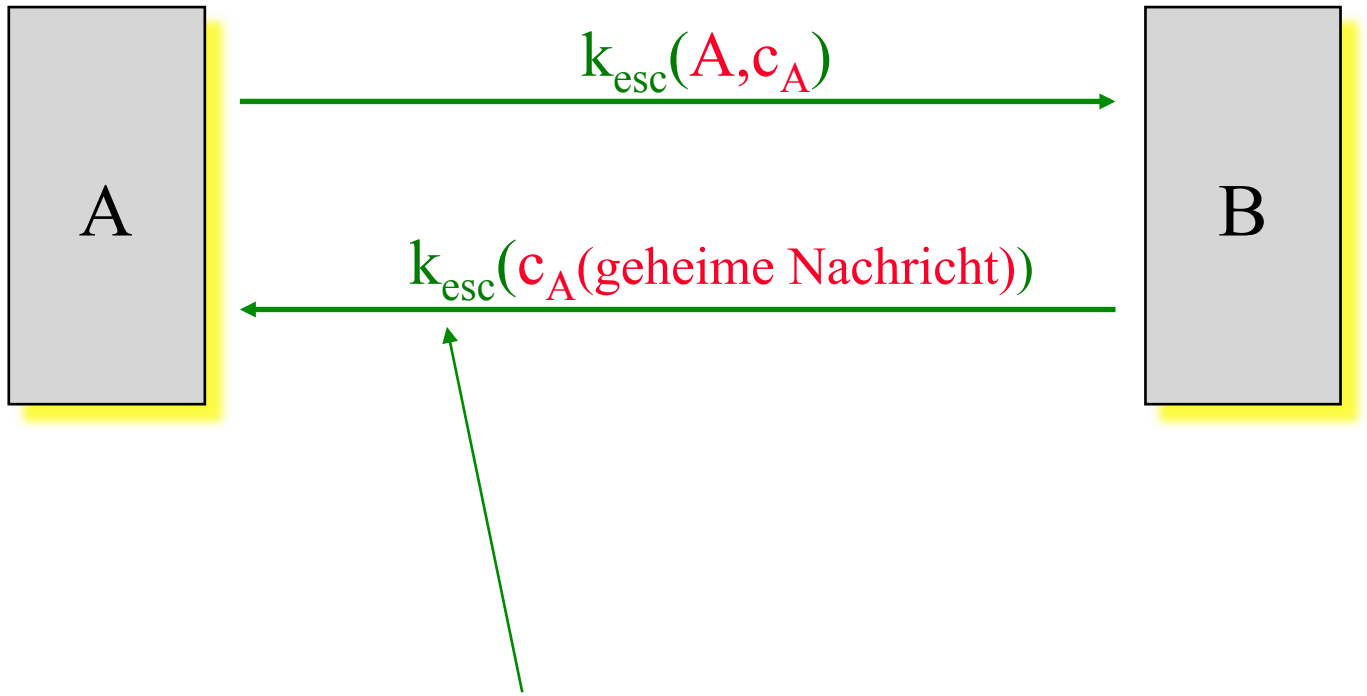
A braucht kein Zertifikat von CA für c_A

Key Escrow Konzelation ohne Dauerüberwachung



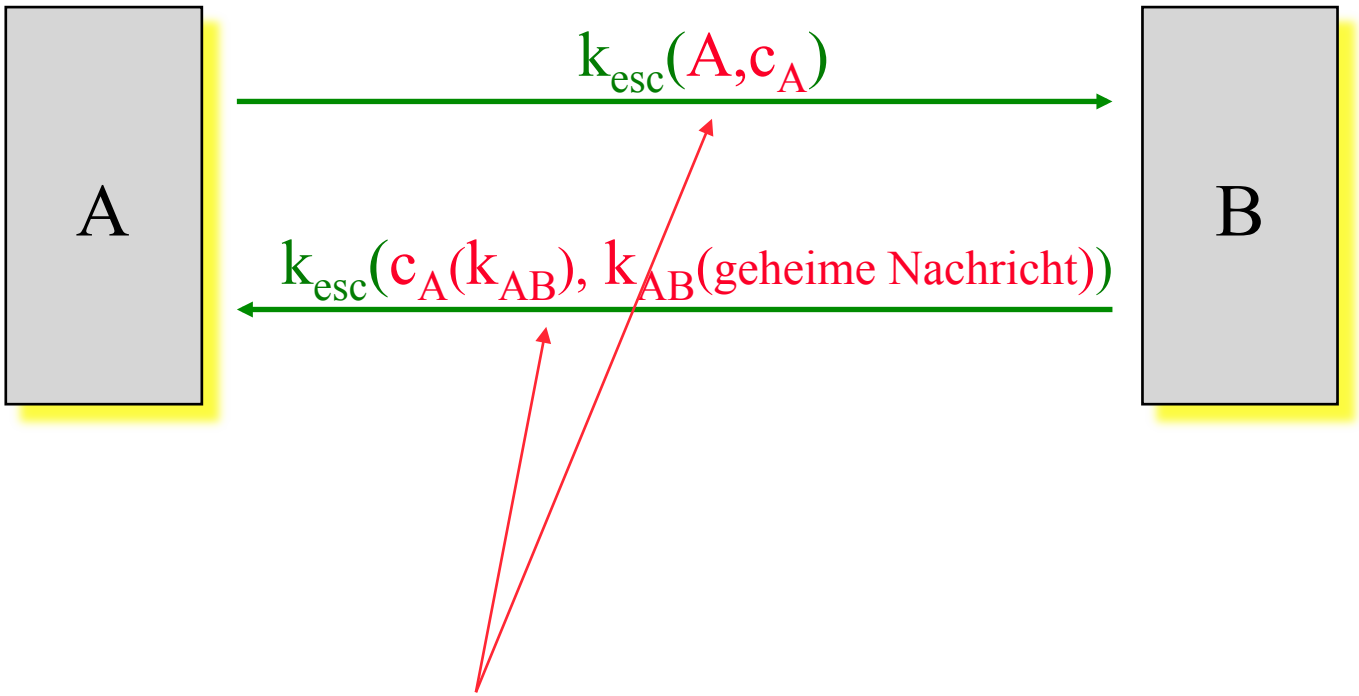
—> Konzelation ohne Key Escrow

Key Escrow Konzelation ohne Dauerüberwachung



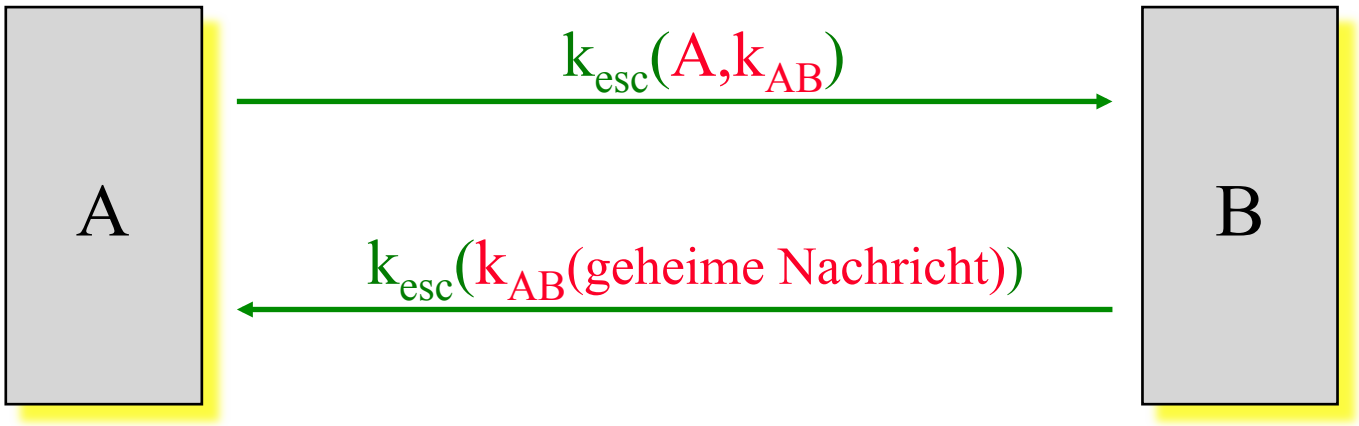
verwende zusätzlich Key Escrow wegen Unverdächtigkeit

Key Escrow Konzelation ohne Dauerüberwachung



auch hybride Kryptosysteme verwendbar

Key Escrow Konzelation ohne Dauerüberwachung



falls nicht rückwirkend überwacht wird bzw. werden kann, genügt allein symmetrisches System

Konzelation mittels symmetrischer Authentikation

Sender *A*

Kennt k_{AB}

Zu übertragen sei Nachricht
$b_1, \ldots b_n$ mit $b_i \in \{0, 1\}$

Berechnet
$\text{MAC}_1 := \text{code}(k_{AB}, b_1) \ldots \text{MAC}_n := \text{code}(k_{AB}, b_n)$

Sei $a_1, \ldots a_n$ die bitweise invertierte Nachricht.

Wählt zufällig $\text{MAC}'_1 \ldots \text{MAC}'_n$ mit
$\text{MAC}'_1 \neq \text{code}(k_{AB}, a_1) \ldots \text{MAC}'_n \neq \text{code}(k_{AB}, a_n)$

bilden

Überträgt (die Mengenklammern bedeuten „zufällige Reihenfolge“)
$\{(b_1, \text{MAC}_1), (a_1, \text{MAC}'_1)\} \ldots$
$\{(b_n, \text{MAC}_n), (a_n, \text{MAC}'_n)\}$

untermischen

Empfänger *B*

Kennt k_{AB}

falsch authentisierte Nachrichten

Probiert, ob
$\{\text{MAC}_1 = \text{code}(k_{AB}, b_1)$ oder
$\text{MAC}'_1 = \text{code}(k_{AB}, a_1)\}$
und empfängt den passenden Wert b_1
...
probiert, ob
$\{\text{MAC}_n = \text{code}(k_{AB}, b_n)$ oder
$\text{MAC}'_n = \text{code}(k_{AB}, a_n)\}$
und empfängt den passenden Wert b_n

entfernen

Ronald L. Rivest: Chaffing and Winnowing: Confidentiality without Encryption; MIT Lab for Computer Science, March 22, 1998; http://theory.lcs.mit.edu/~rivest/chaffing.txt

Konzelation mittels symmetrischer Authentikation

Sender *A*

Kennt k_{AB}

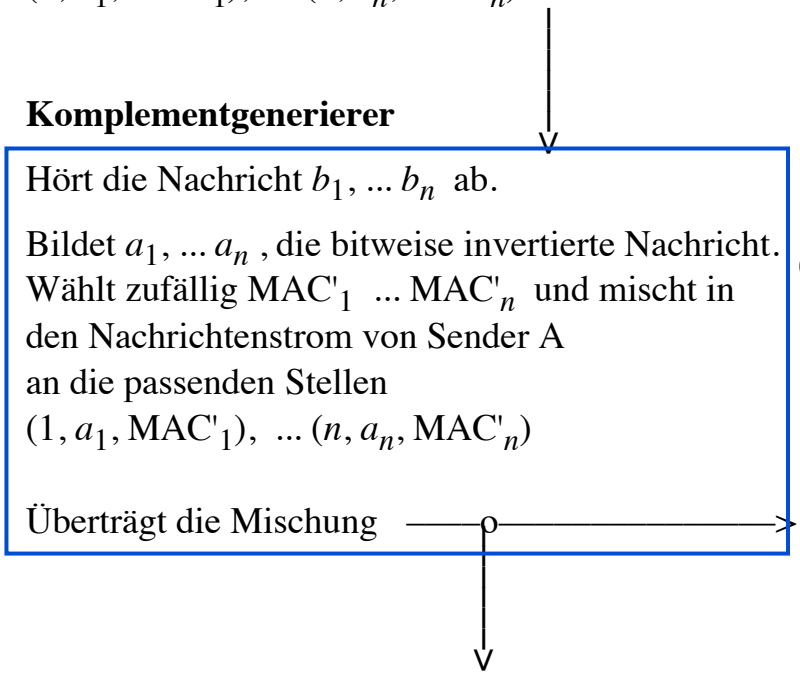
Zu übertragen sei Nachricht
$b_1, \ldots b_n$ mit $b_i \in \{0, 1\}$

Berechnet
$\mathrm{MAC}_1 := \mathrm{code}(k_{AB}, b_1) \ldots \mathrm{MAC}_n := \mathrm{code}(k_{AB}, b_n)$

Überträgt
$(1, b_1, \mathrm{MAC}_1), \ldots (n, b_n, \mathrm{MAC}_n)$

Empfänger *B*

Kennt k_{AB}



Falsch authentisierte Nachrichten

ohne Schlüsselkenntnis
bilden und untermischen

entfernen

normales Authentikationsprotokoll
Ignoriert Nachrichten mit falscher Seque
Ignoriert Nachrichten mit falscher Authe
gibt die übrigbleibenden weiter
empfangen wird mit größter Wahrschein
$b_1, \ldots b_n$

Schlüsselaustausch für Steganographie ?

Schlüsselaustausch außerhalb des Kommunikationsnetzes ist in **kleinen geschlossenen Gruppen** leicht, insbesondere also leicht für Kriminelle und Terroristen.

Große offene Gruppen brauchen für Steganographie eine Technik, die ohne Übertragung verdächtiger Nachrichten im Kommunikationsnetz auskommt – asymmetrische Kryptographie ist hierfür nicht direkt verwendbar.

Die Lösung:

Diffie-Hellman Public-Key-Schlüsselvereinbarung

Verwendet Public Keys eines weitverbreiteten digitalen Signatursystems (DSS, entwickelt und genormt von NSA und NIST, USA)

Schlüsselaustausch ohne Nachrichtenaustausch

Diffie-Hellman Public-Key-Schlüsselvereinbarung

geheim: x y

öffentlich: g^x g^y

$$(g^y)^x = g^{yx} = g^{xy} = (g^x)^y$$

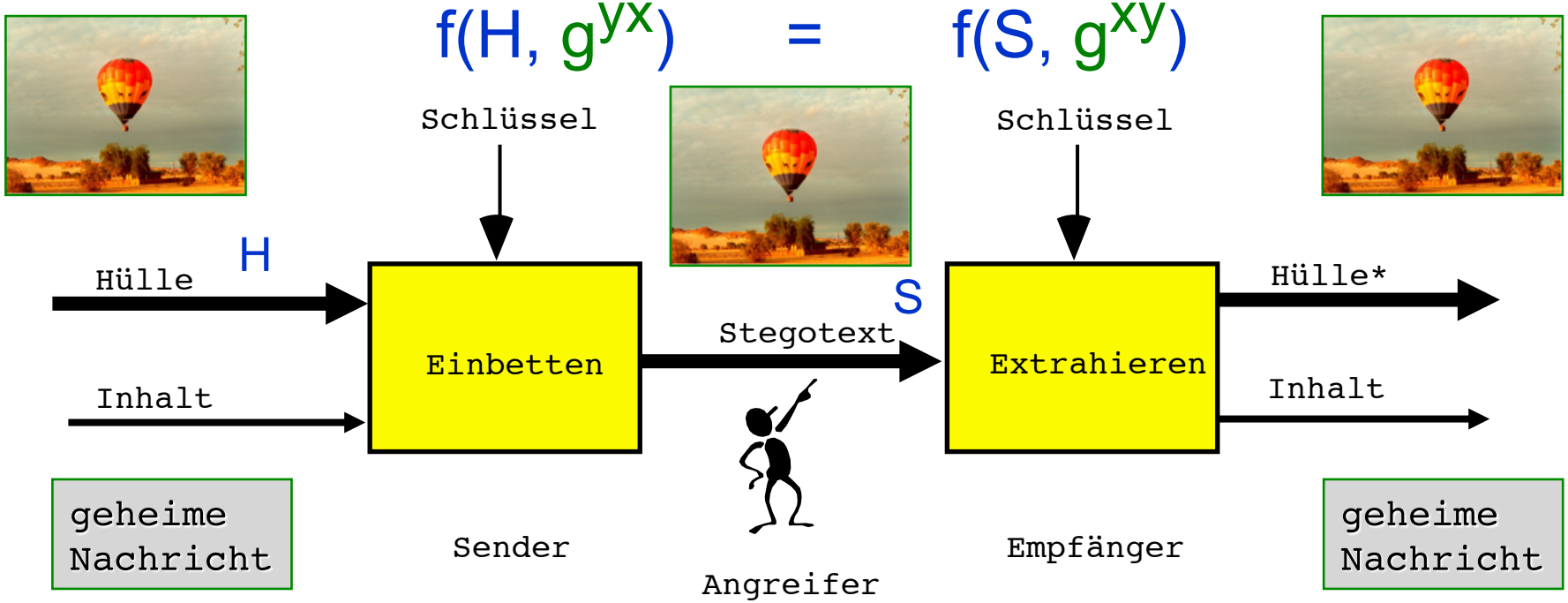
Schlüsselaustausch für Steganographie !

Diffie-Hellman Public-Key-Schlüsselvereinbarung

geheim: x y

öffentlich: g^x g^y

$$(g^y)^x = g^{yx} = g^{xy} = (g^x)^y$$

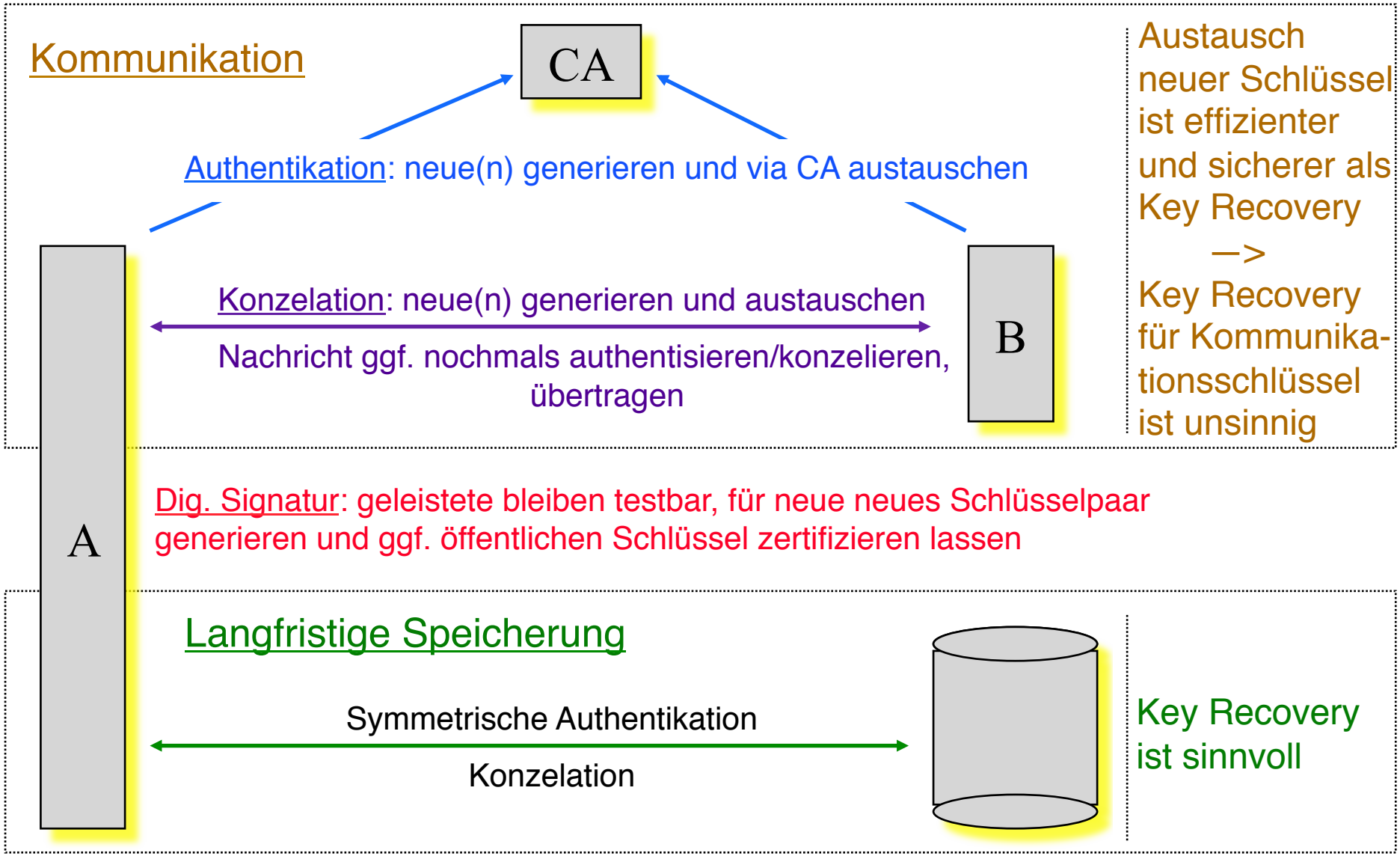


Zusammenfassung

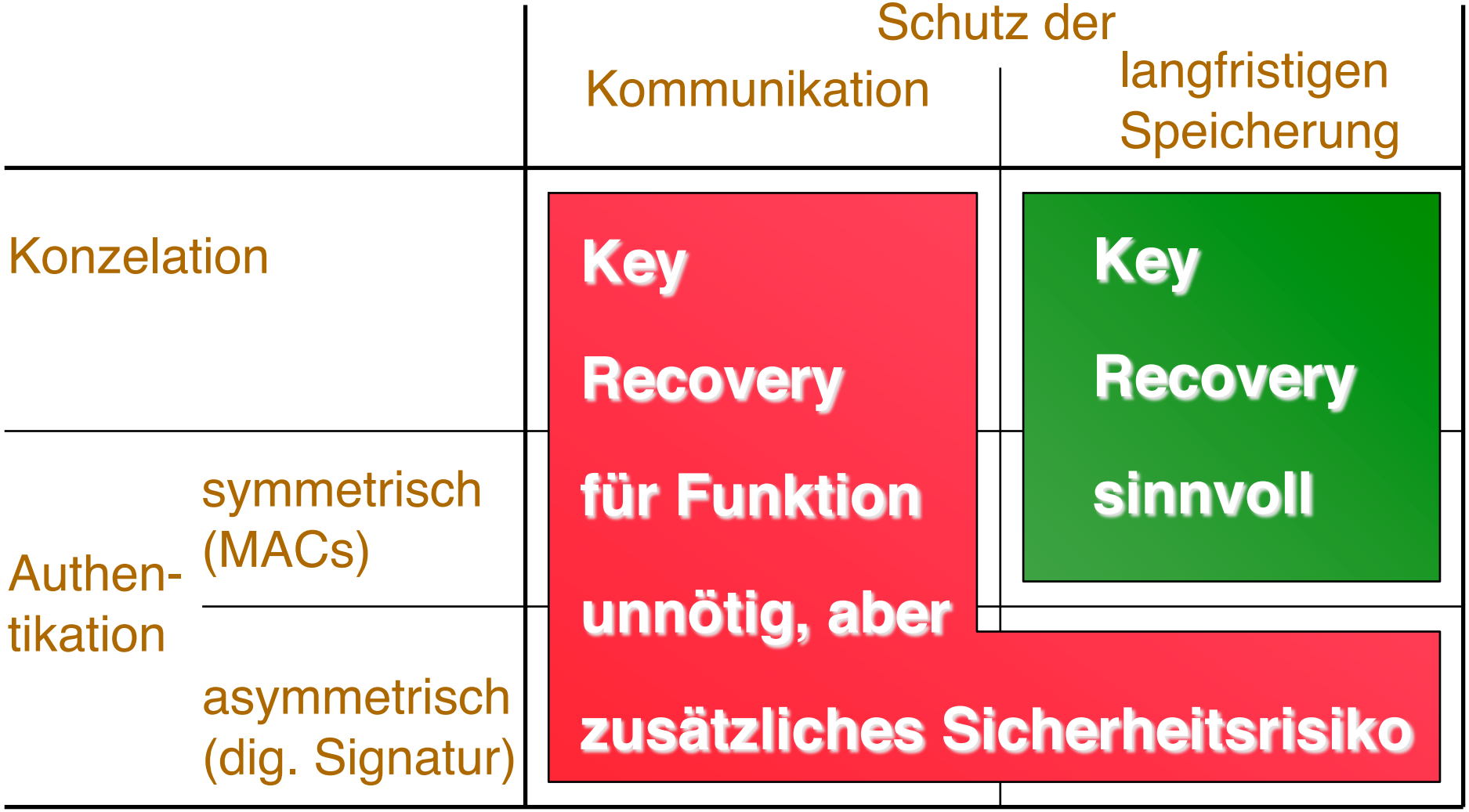
Digitale Signaturen	→	Konzelation
Key Escrow ohne Dauerüberwachung	→	Schlüsselaustausch, Mehrfachverschlüsselung
Multimediakommunikation	→	Steganographie

Kryptoregulierung ignoriert die technischen Randbedingungen

Verlust geheimer Schlüssel



Wo Key Recovery ?



Vorschläge zur Kryptoregulierung schaden nur den Braven

- Kryptographie zur Konzelation verbieten
- Kryptographie zur Konzelation verbieten – außer sehr kurze Schlüssellängen
- Kryptographie zur Konzelation verbieten – außer Key Escrow bzw. Key Recovery Systemen
- Öffentliche Chiffrierschlüssel nur in PKI aufnehmen, wenn geheimer Dechiffrierschlüssel hinterlegt
- Pflicht, bei Strafverfahren Entschlüsselungsschlüssel zu übergeben

- ➢ Steganographie
- ➢ Zusätzlich Steganographie
- ➢ Key Escrow bzw. Key Recovery System für Bootstrap verwenden
- ➢ PKI für öffentliche Chiffrierschlüssel selbst realisieren
- ➢ One-time-pad passend bilden

(Un-)Regulierbarkeit anonymer/pseudonymer Kommunikation

- Explizite Techniken *(die Theorie kennen Sie bereits)*
- Ausweichtechniken

(Un)Regulierbarkeit anonymer/pseudonymer Kommunikation

Anon-Proxies

MIXe

- **Kaskade: AN.ON**
- **P2P: TOR**

All dies gibt es auch im Ausland ohne Regulierung – solange noch keine Weltinnenpolitik

(Un)Regulierbarkeit anonymer/pseudonymer Kommunikation

Selbst im Inland:

- **Öffentliche Telefone,**
- **Prepaid Telefone,**
- **offene WLANs,**
- **unsichere Bluetooth-Mobilfunkgeräte,**
- **...**

Vorratsdatenspeicherung ist weitestgehend sinnlos, da „Kriminelle“ dann ausweichen, s.o.