

Sicherheit in Rechnernetzen

Mehrseitige Sicherheit in verteilten und durch verteilte Systeme

Folien zur Vorlesung: Einführung in die Datensicherheit

Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden

Hans-Grundig-Str. 25, Raum 120

Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, <http://dud.inf.tu-dresden.de/>

Vertiefungsrichtung technischer Datenschutz

<i>Lehrveranstaltung</i>	<i>Lehrende(r)</i>	<i>SWS</i>
Einführung in die Datensicherheit	Pfitzmann	1/1
Kryptographie	Pfitzmann	2/2
Datensicherheit durch verteilte Systeme	Pfitzmann	1/1
Datensicherheit und Datenschutz national und international	Lazarek	2
Kryptographie und -analyse	Klimant	2
Kanalkodierung	Schönfeld	2/2
Steganographie	Westfeld	1/1
Datensicherheit und Kryptographie	Clauß, Klimant, Kriegelstein	/4
Datenschutzfreundl. Technologien im Internet	Clauß, Kriegelstein, Köpsell	/2
Informatik und Gesellschaft	Pfitzmann	2
Hauptseminar techn. Datenschutz	Pfitzmann et.al.	2

Gliederung (1)

1 Einführung

- 1.1 Was sind Rechnernetze (verteilte offene Systeme)
- 1.2 Was bedeutet Sicherheit?
 - 1.2.1 Was ist zu schützen?
 - 1.2.2 Vor wem ist zu schützen?
 - 1.2.3 Wie und wodurch kann Sicherheit erreicht werden?
 - 1.2.4 Vorausschau auf Schutzmechanismen
 - 1.2.5 Angreifermodell
- 1.3 Was bedeutet Sicherheit in Rechnernetzen?

2 Sicherheit in einzelnen Rechnern und ihre Grenzen

- 2.1 Physische Sicherheitsannahmen
 - 2.1.1 Was kann man bestenfalls erwarten?
 - 2.1.2 Gestaltung von Schutzmaßnahmen
 - 2.1.3 Ein Negativbeispiel: Chipkarten
 - 2.1.4 Sinnvolle physische Sicherheitsannahmen
- 2.2 Schutz isolierter Rechner vor unautorisiertem Zugriff und Computerviren
 - 2.2.1 Identifikation
 - 2.2.2 Zugangskontrolle
 - 2.2.3 Zugriffskontrolle
 - 2.2.4 Beschränkung der Bedrohung "Computer-Viren" auf die durch "transitive Trojanische Pferde"
 - 2.2.5 Restprobleme

Gliederung (2)

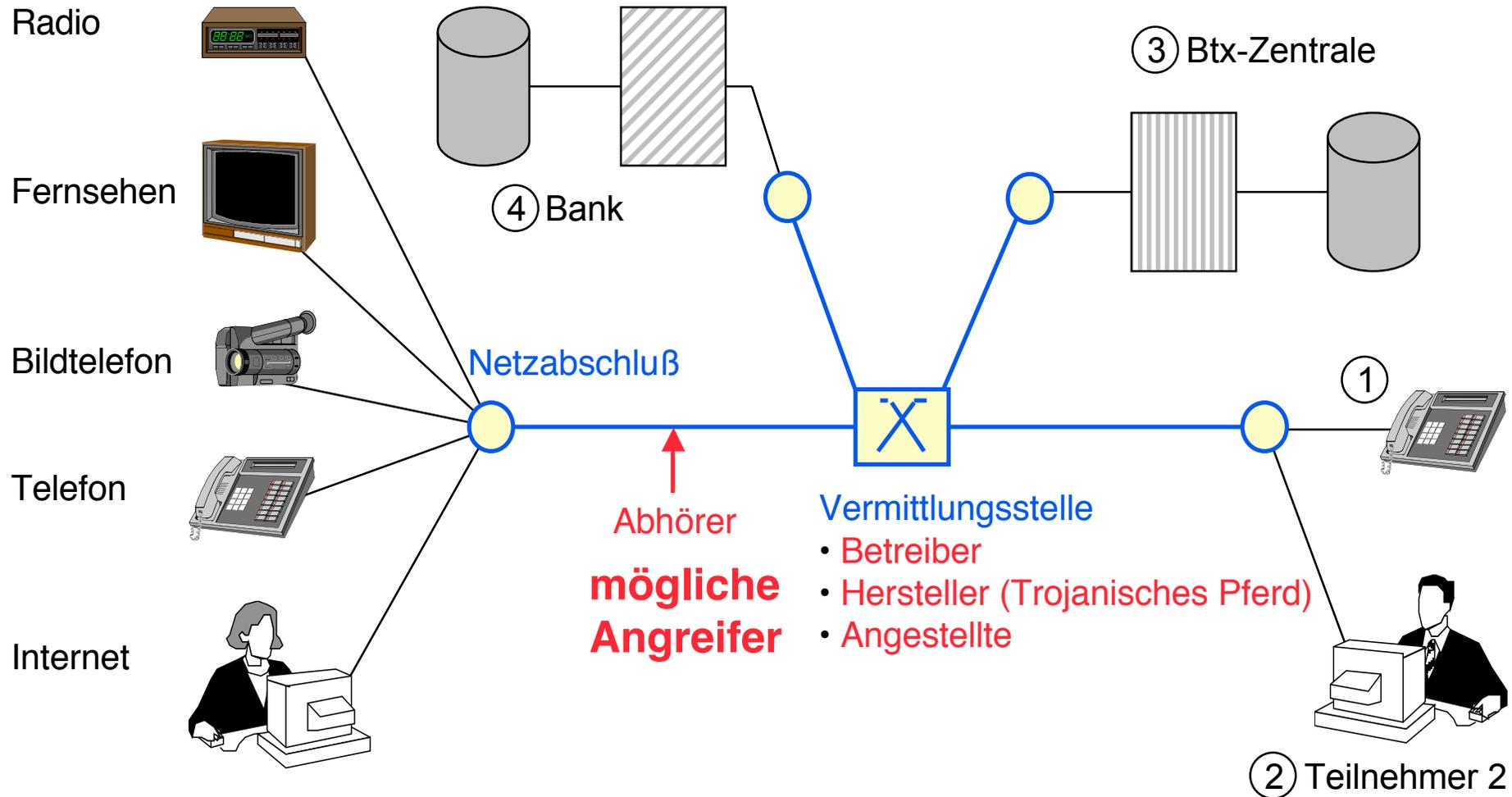
3 Kryptologische Grundlagen

4 Datenschutz garantierende Kommunikationsnetze

5 Digitale Zahlungssysteme und Credentials als Verallgemeinerung

6 Zusammenfassung und Ausblick

Ausschnitt eines Rechnernetzes



Bsp. ⑤ Patientenüberwachung, ⑥ Bewegtbildüberwachung während Operation

Warum reichen juristische Regelungen (für Rechtssicherheit und Datenschutz) nicht aus ?

Geschichte der Rechnernetze (1)

- 1833 erster **elektromagnetischer Telegraph**
- 1858 erste **Kabelverbindung zwischen Europa und Nordamerika**
- 1876 **Fernsprechen** über 8,5 km lange Versuchsstrecke
- 1881 erstes **Fernsprechortsnetz**
- 1900 Beginn der **drahtlosen Telegraphie**
- 1906 Einführung des **Selbstwählferndienstes** in Deutschland, realisiert durch Hebdrehwähler, d.h. erste vollautomatische Vermittlung durch Elektomechanik
- 1928 Fernsprechdienst Deutschland-USA eingeführt (über Funk)
- 1949 erster funktionierender **von-Neumann-Rechner**
- 1956 erstes **Transatlantikkabel für Fernsprechen**
- 1960 erster **Fernmeldesatellit**
- 1967 Beginn des Betriebes des **Datex-Netzes** durch die deutsche Bundespost, d.h. des ersten speziell für Rechnerkommunikation realisierten Kommunikationsnetzes (Rechnernetz erster Art). Die Übertragung erfolgt digital, die Vermittlung durch Rechner (Rechnernetz zweiter Art).
- 1977 Einführung des Elektronischen Wähl-Systems (**EWS**) für Fernsprechen durch die Deutsche Bundespost, d.h. erstmals Vermittlung durch Rechner (Rechnernetz zweiter Art) im Fernsprechnet, aber weiterhin analoge Übertragung

Geschichte der Rechnernetze (2)

- 1981 erster persönlicher Rechner (PC) der Rechnerfamilie (**IBM PC**), die weite Verbreitung auch im privaten Bereich findet
- 1982 Investitionen in die **Übertragungssysteme** des Fernsprechnetzes erfolgen zunehmend in **digitale** Technik
- 1985 Investitionen in die Vermittlungssysteme des Fernsprechnetzes erfolgen zunehmend in rechnergesteuerte Technik, die nunmehr nicht mehr analoge, sondern **digitale Signale vermittelt** (in Deutschland 1998 abgeschlossen)
- 1988 Betriebsbeginn des **ISDN** (Integrated Services Digital Network)
- 1989 erster westentaschengroßer PC: **Atari Portfolio**; damit sind Rechner im engeren Sinne persönlich und mobil
- 1993 **zellulare Funknetze** werden Massendienst
- 1994 **www** Kommerzialisierung des Internet
- 2000 **WAP-fähige Handys** für 77 € ohne Vertragsbindung
- 2003 mit IEEE 802.11b finden **WLAN** (Wireless Local Area Network), mit Bluetooth **WPAN** (Wireless Personal Area Network) massenhafte Verbreitung

Wichtige Begriffe

Rechner verbunden über **Kommunikationsnetz** = **Rechnernetz** (erster Art)

Prozeßrechner im **Kommunikationsnetz** = **Rechnernetz** (zweiter Art)

verteiltes System

räumlich

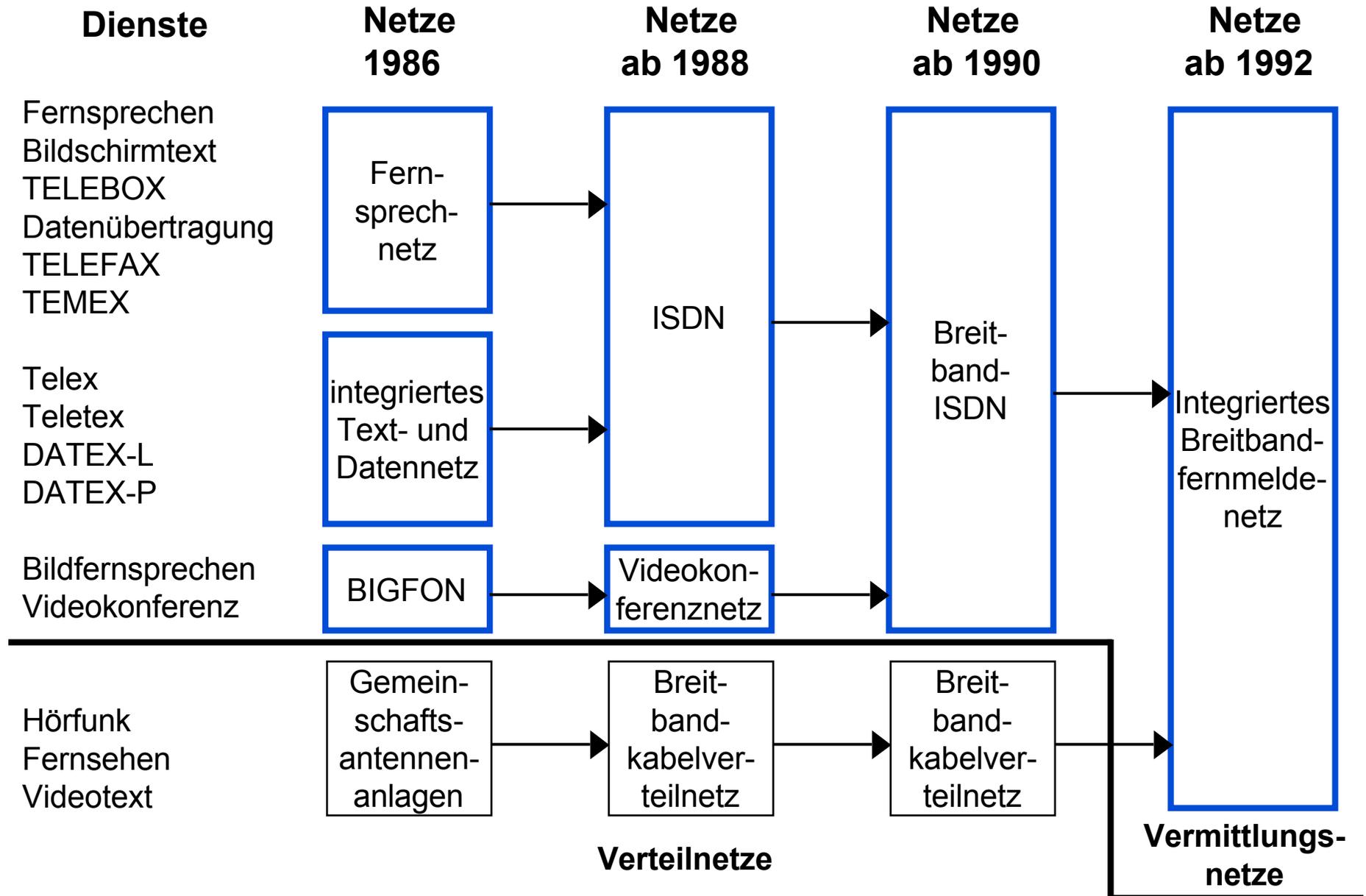
Kontroll- und Implementierungsstruktur

offenes System \neq **öffentliches** System \neq **Open Source** System

diensteintegrierendes System

digitales System

Entwicklung der leitungsgebundenen Kommunikationsnetze der Deutschen Bundespost



Bedrohungen und korrespondierende Schutzziele

Bedrohungen:

Bsp.: medizinisches Informationssystem

Schutzziele:

1) Informationsgewinn

Rechnerhersteller erhält Krankengeschichten

Vertraulichkeit

2) Modifikation von Information

unerkannt Dosieranweisungen ändern

3) Beeinträchtigung der Funktionalität

erkennbar ausgefallen

≥ totale
Korrektheit

Integrität

≡ partielle Korrektheit

Verfügbarkeit
für berechnigte
Nutzer

keine Klassifikation, aber pragmatisch sinnvoll

Bsp.: Programm unbefugt modifiziert

1) nicht erkennbar, aber verhinderbar; nicht rückgängig zu machen

2)+3) nicht verhinderbar, aber erkennbar; rückgängig zu machen

Definitionen für die Schutzziele

Vertraulichkeit (confidentiality)

Informationen werden nur Berechtigten bekannt.

Integrität (integrity)

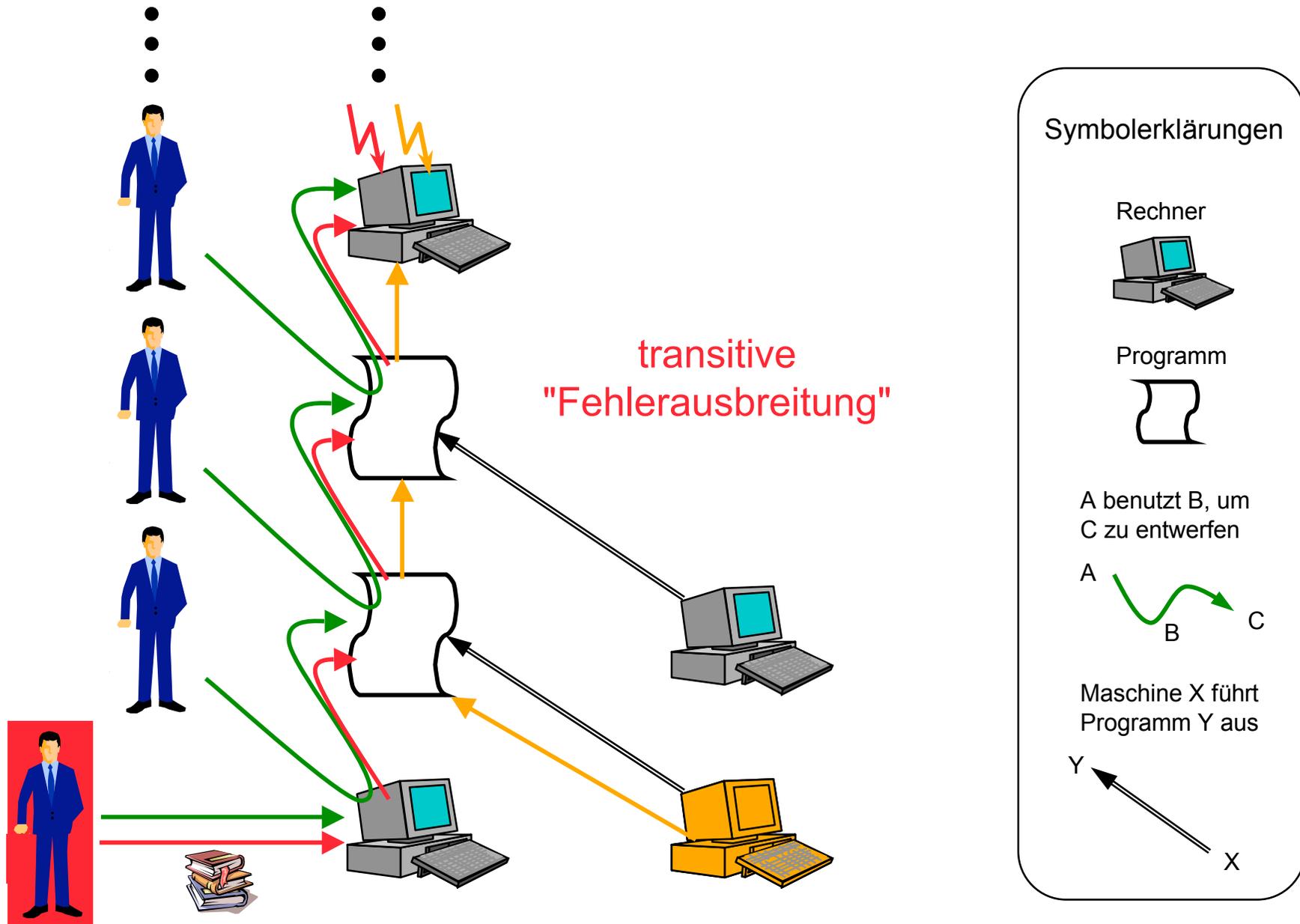
Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Verfügbarkeit (availability)

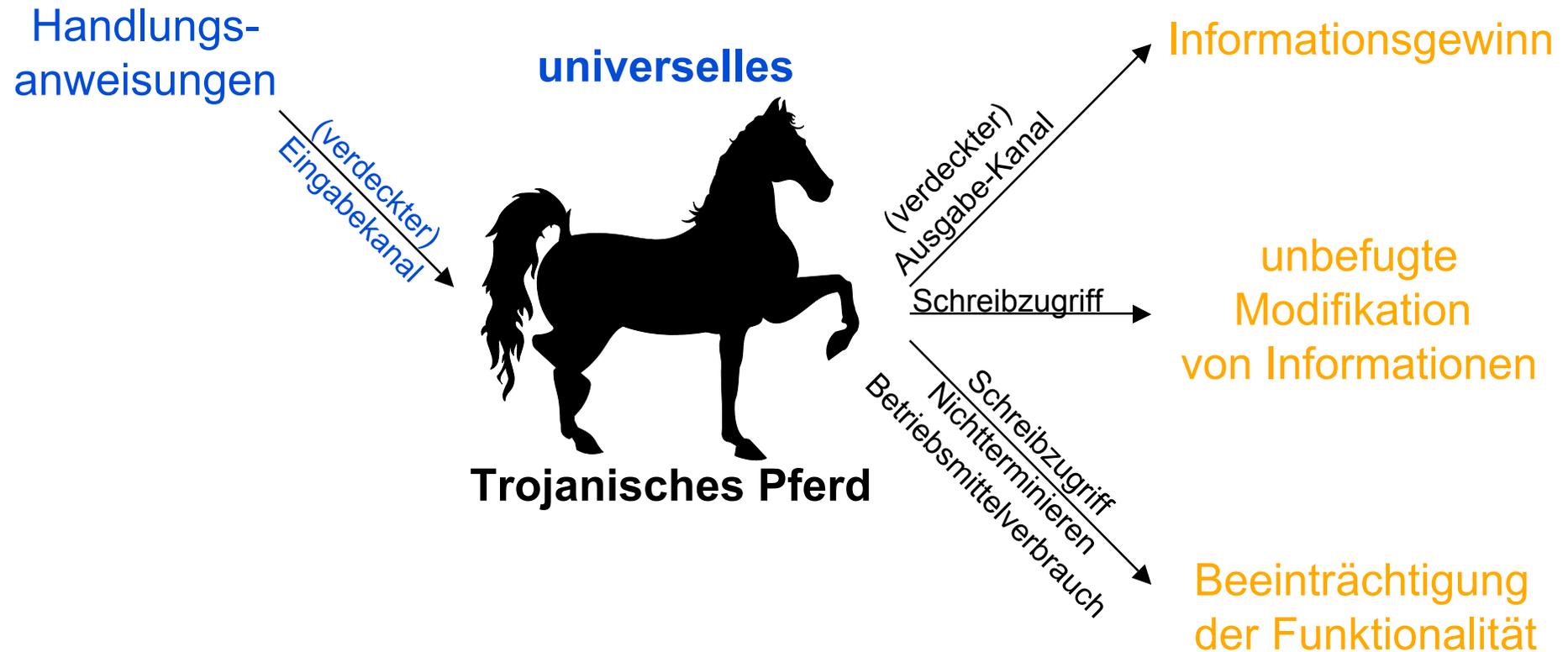
Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- subsumiert: Daten, Programme, Hardwarestrukturen
- es muß geklärt sein, wer in welcher Situation wozu berechtigt ist
- kann sich nur auf das Innere eines Systems beziehen

Transitive Ausbreitung von Fehlern und Angriffen



Universelles Trojanisches Pferd



Vor wem ist zu schützen ?

Naturgesetze und Naturgewalten

- Bauteile altern
- Überspannung (Blitzschlag, EMP)
- Spannungsausfall
- Überschwemmung (Sturmflut, Wasserrohrbruch)
- Temperaturänderungen ...

Fehler-
toleranz

Menschen

- Außenstehende
- Benutzer des Systems
- Betreiber des Systems
- **Wartungsdienst**
- **Produzenten** des Systems
- **Entwerfer** des Systems
- **Produzenten** der Entwurfs- und Produktionshilfsmittel
- **Entwerfer** der Entwurfs- und Produktionshilfsmittel
- **Produzenten** der Entwurfs- und Produktionshilfsmittel der Entwurfs- und Produktionshilfsmittel
- **Entwerfer** ... jeweils auch Benutzer,
Betreiber,
Wartungsdienst ... des verwendeten Systems

Trojanisches Pferd
universell
transitiv

Welche Schutzmaßnahmen gegen welche Angreifer

Schutz bzgl. Schutz vor	Erwünschtes leisten	Unerwünschtes verhindern
Entwerfer und Produzent der Entwurfs- und Produktionshilfsmittel	Zwischensprachen; Zwischenergebnisse, die unabhängig analysiert werden	
Entwerfer des Systems	wie oben + mehrere unabhängige Entwerfer	
Produzenten des Systems	unabhängige Analysen der Produkte	
Wartungsdienst	Kontrolle wie bei neuem Produkt, s. o.	
Betreiber des Systems		physischen Zugriff beschränken, logischen Zugriff beschränken und protokollieren
Benutzer des Systems	physischen und logischen Zugriff beschränken	
Außenstehende	physisch vom System, kryptographisch von den Daten fernhalten	

Schutz bzgl. Schutz vor	Erwünschtes leisten	Unerwünschtes verhindern
Entwerfer und Produzent der Entwurfs- und Produktionshilfsmittel	verständliche Zwischensprachen; Ziele, die nicht durch die Sprache des Anwenders ausgedrückt werden können	
Produktionshilfsmittel	wie oben + Entwurf durch mehrere unabhängige Entwerfer mit unabhängigen Produkten	
Entwerfer des Systems	Produkte mit unabhängigen Werkzeugen analysieren	
Produzenten des Systems		
Wartungsdienst		
		physischen Zugriff durch unmanipulierbare Gehäuse beschränken, logischen Zugriff in ihnen beschränken und
Betreiber des Systems	physischen und logischen Zugriff beschränken	
Benutzer des Systems		
Außenstehende	physisch vom System, kryptographisch von den Daten fernhalten	

Welche Schutzmaßnahmen gegen welche Angreifer

Schutz bzgl.	Erwünschtes leisten	Unerwünschtes verhindern
Schutz vor		
Entwerfer und Produzent der Entwurfs- und Produktionshilfsmittel	Zwischensprachen; Zwischenergebnisse, die unabhängig analysiert werden	
Entwerfer des Systems	wie oben + mehrere unabhängige Entwerfer	
Produzenten des Systems	unabhängige Analysen der Produkte	
Wartungsdienst	Kontrolle wie bei neuem Produkt, s. o.	
Betreiber des Systems		physischen Zugriff beschränken, logischen Zugriff beschränken und protokollieren
Benutzer des Systems	physischen und logischen Zugriff beschränken	
Außenstehende	physisch vom System, kryptographisch von den Daten fernhalten	

physische Verteilung und Redundanz

Unbeobachtbarkeit, Anonymität, Unverkettbarkeit:
Erfassungsmöglichkeit "unnötiger Daten" vermeiden

Maximal berücksichtigte Stärke eines Angreifers

Angreifermodell

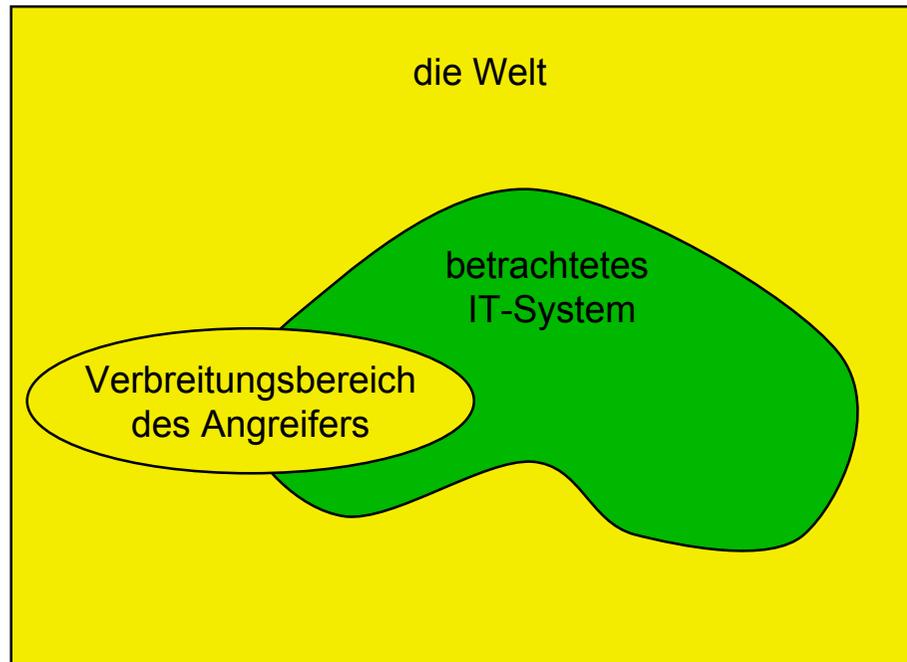
Schutz vor einem allmächtigen Angreifer ist unmöglich.

- Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer ...), *auch kombiniert*
- Verbreitung des Angreifers
- Verhalten des Angreifers
 - passiv / aktiv
 - beobachtend / verändernd (bzgl. seiner erlaubten Handlungen)
- dumm / intelligent
 - Rechenkapazität:
 - unbeschränkt: informationstheoretisch
 - beschränkt: komplexitätstheoretisch

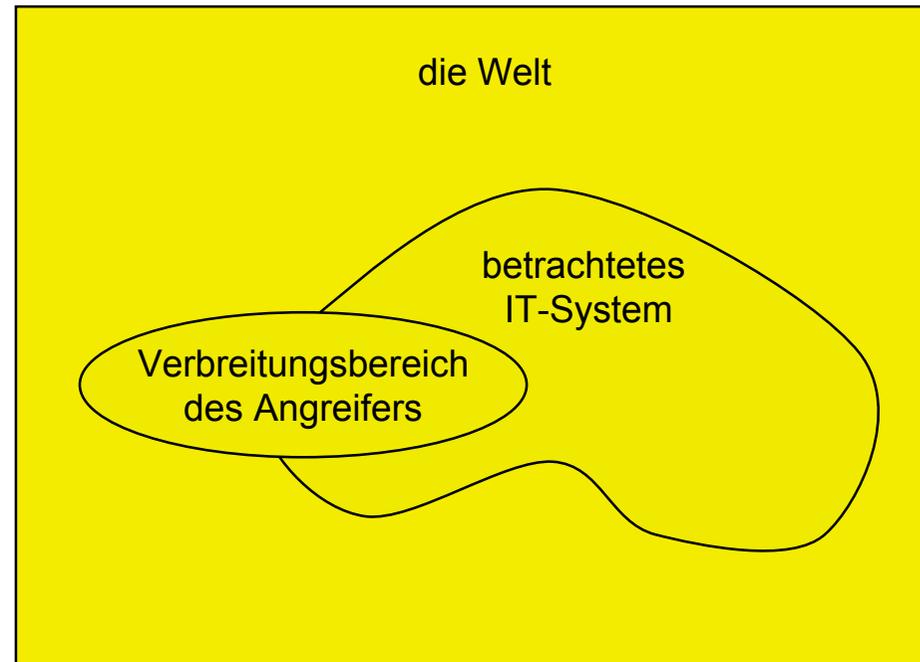
Geld

Zeit

Beobachtender vs. verändernder Angreifer



beobachtender Angreifer



verändernder Angreifer



nur erlaubtes Verhalten



auch verbotenes Verhalten

Sicherheit in Rechnernetzen

Vertraulichkeit

- Nachrichteninhalte vertraulich
- **Ort** • Sender / Empfänger anonym

**Ende-zu-Ende-Verschlüsselung mit
Konzelationssystem**

**Verfahren zum Schutz der
Verkehrsdaten**

Integrität

- Fälschungen erkennen
- Empfänger kann Senden der
Nachricht beweisen
- **Zeit** {
- Absender kann Senden beweis.
- Nutzungsentgelte sichern

**Authentikationssystem (e)
Nachrichten signieren**

**Empfangsquittung
während Dienstleistung mittels
dig. Zahlungssysteme**

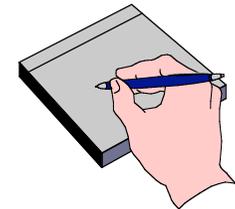
Verfügbarkeit

- Kommunikation ermöglichen

**Diversitäre Netze; faire
Betriebsmittelaufteilung**

Mehrseitige Sicherheit

- Jeder Beteiligte hat **Sicherheitsinteressen**.
- Jeder Beteiligte kann seine Interessen **formulieren**.
- Konflikte werden erkannt und Lösungen **ausgehandelt**.
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.



Sicherheit mit minimalen Annahmen über andere

Schutzziele: Sortierung

	Inhalte	Umfeld
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

Schutzziele: Definitionen

Vertraulichkeit: Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.

Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.

Anonymität: Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.

Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne daß andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

Integrität: Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.

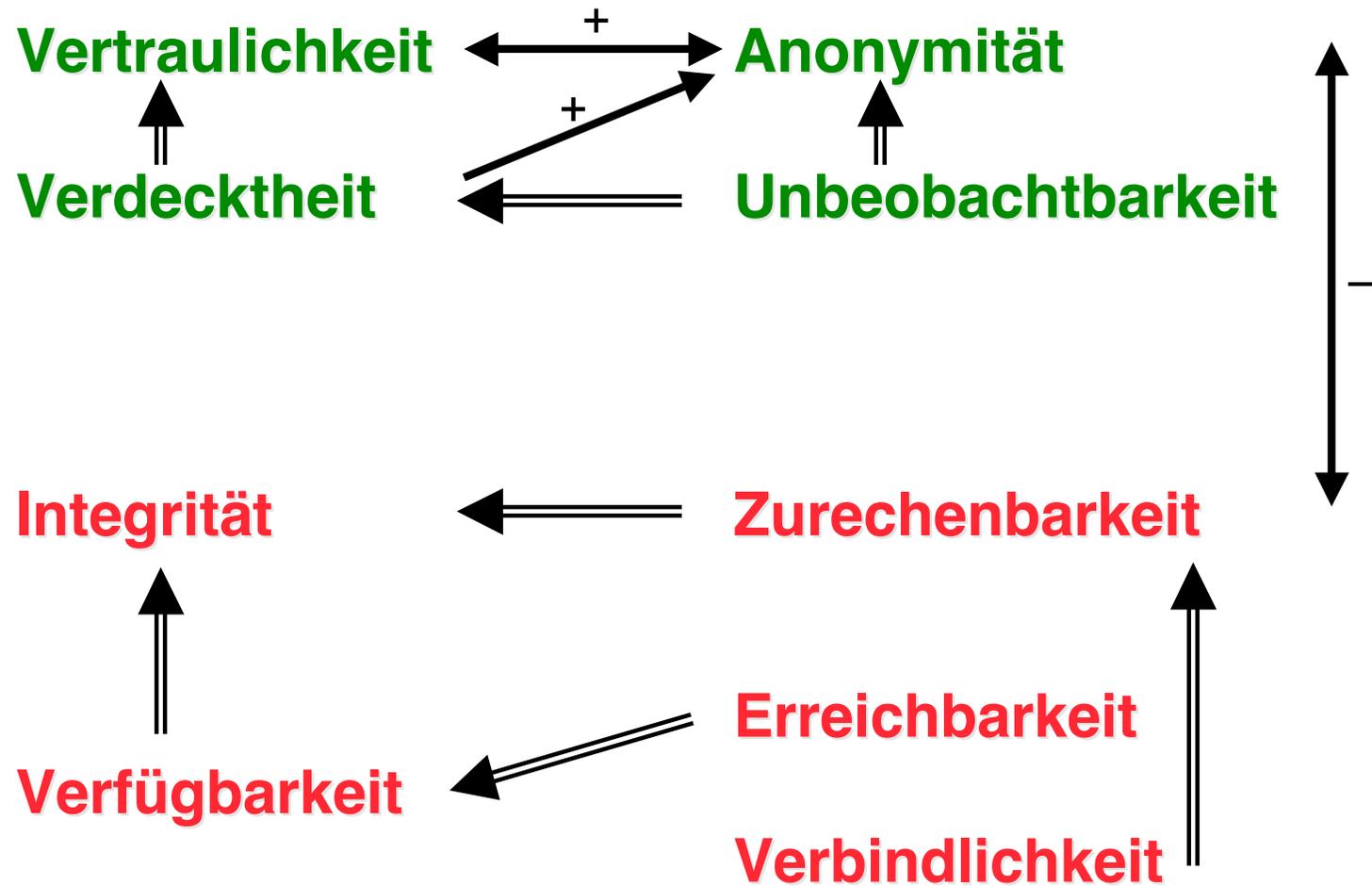
Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

Verfügbarkeit: Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.

Erreichbarkeit: Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.

Verbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

Wechselwirkungen zwischen Schutzzielen



⇒ impliziert

+ → verstärkt

- → schwächt

Physische Sicherheitsannahmen

Alle technischen Schutzmaßnahmen brauchen physische "Verankerung" in einem Systemteil, auf den der Angreifer weder lesenden noch verändernden Zugriff hat.

Spektrum vom "Rechenzentrum X" bis zur "Chipkarte Y"

Was kann man bestenfalls erwarten ?

Verfügbarkeit eines räumlich konzentrierten Systemteils ist gegen durchaus *vorstellbare* Angreifer nicht gewährleistet

→ **physisch verteiltes System**

und hoffen, dass Angreifer nicht an vielen Orten gleichzeitig sein kann.

Verteilung erschwert **Vertraulichkeit** und **Integrität**.

Physische Maßnahmen bzgl. Vertraulichkeit und Integrität jedoch wirkungsvoller: Schutz gegen *alle* derzeit *vorstellbaren* Angreifer scheint erreichbar. Gelingt dies hinreichend, steht physischer Verteilung nichts im Wege.

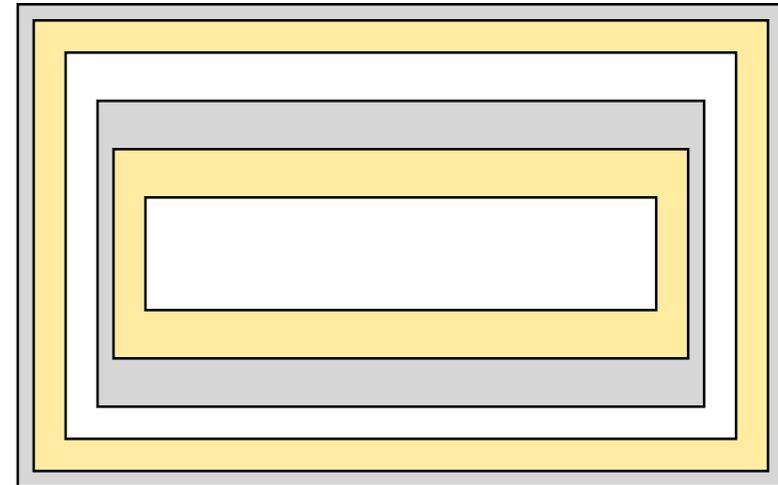
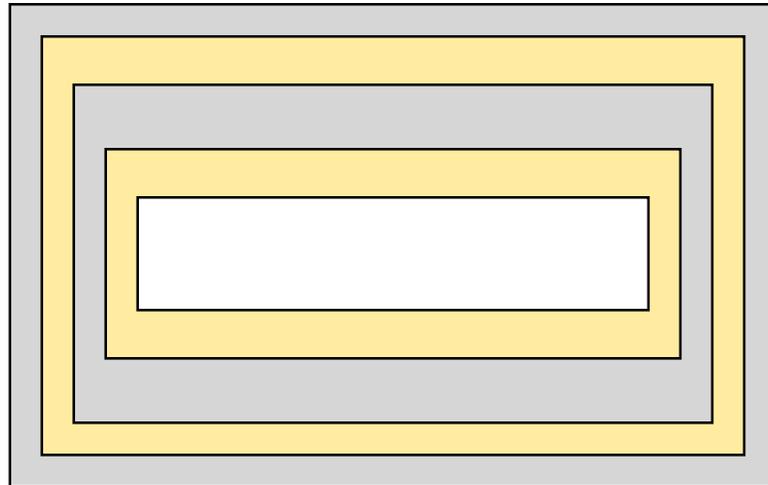
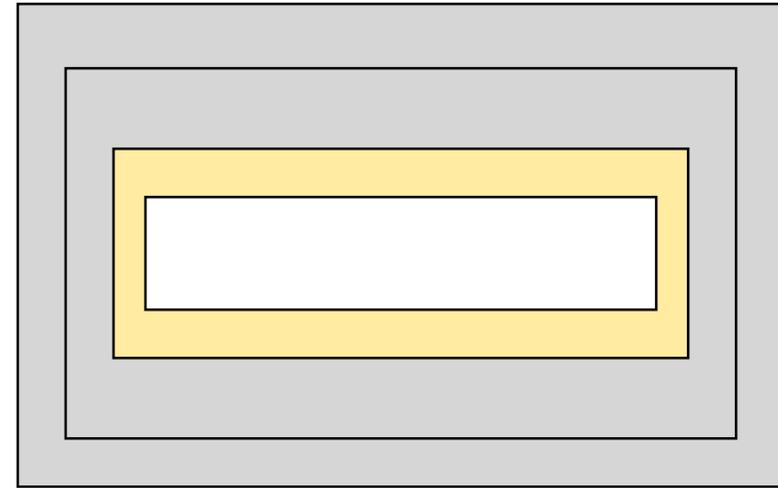
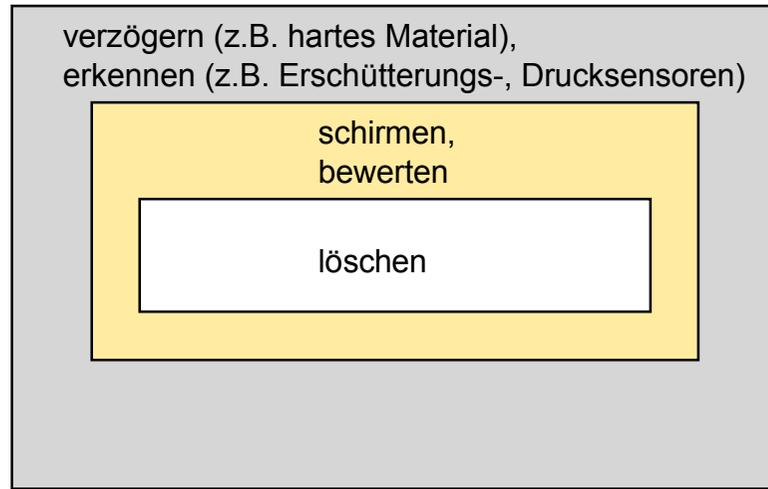
Unmanipulierbare Gehäuse

Eingriff: Erkennen
Bewerten

Angriff: Verzögern
Daten (etc.) löschen

Möglichkeit: mehrere Schichten, Schirmung →

Schalenförmige Anordnung der fünf Grundfunktionen



Unmanipulierbare Gehäuse

Eingriff: Erkennen
Bewerten

Angriff: Verzögern
Daten (etc.) löschen

Möglichkeit: mehrere Schichten, Schirmung

Problem: Validierung ... Glaubwürdigkeit

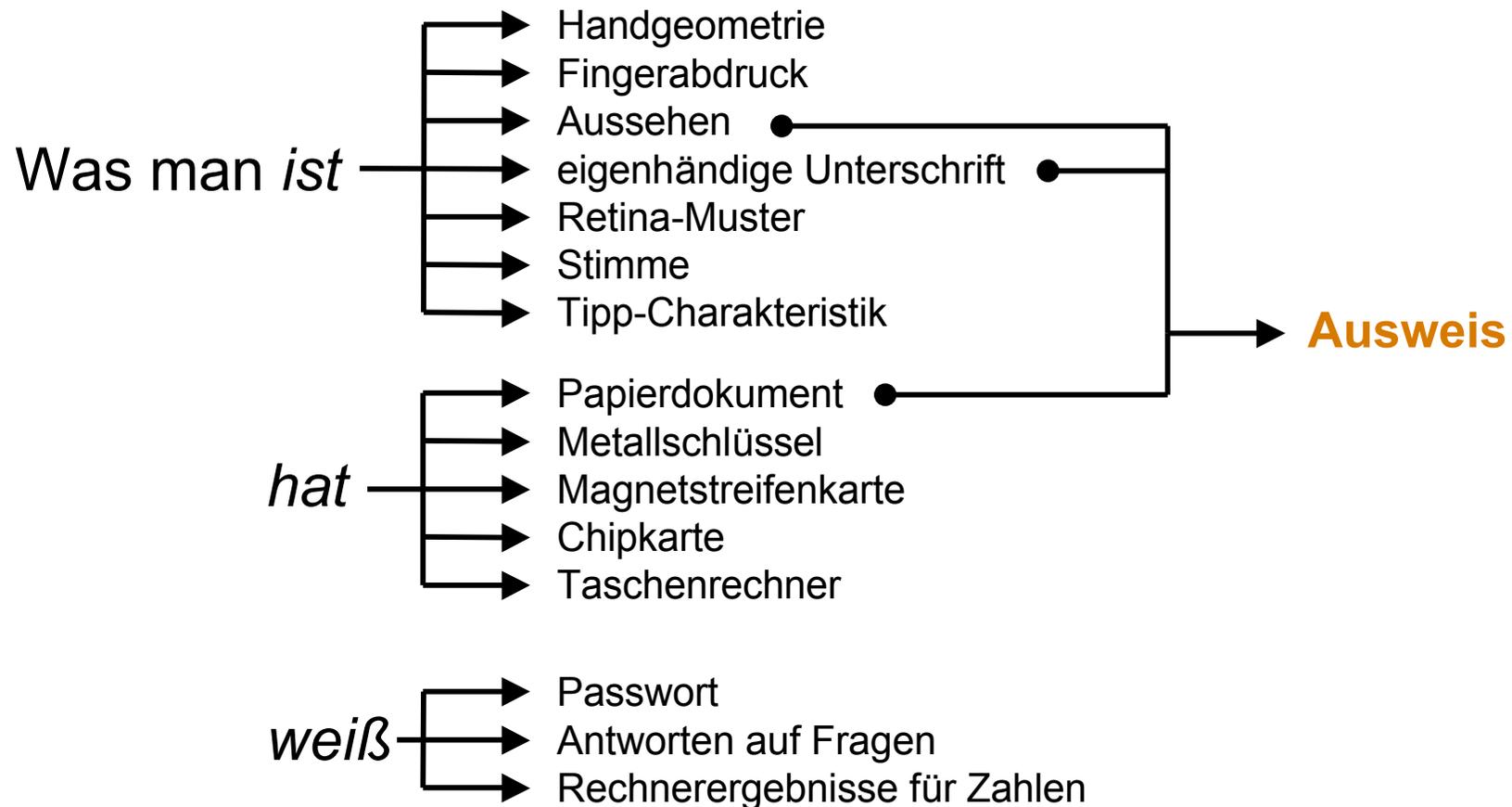
Negativ-Beispiel: Chipkarten

- kein Erkennen (u.a. Batterie fehlt)
- Schirmung schwierig (Karte dünn und biegsam)
- kein Löschen vorgesehen selbst bei Stromversorgung

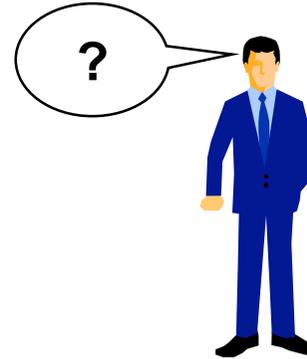
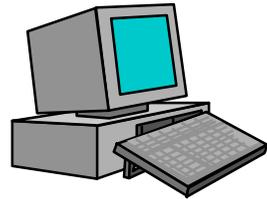
Goldene Regel

Übereinstimmung zwischen organisatorischen
und informationstechnischen Strukturen

Identifikation von Menschen durch IT-Systeme



Identifikation von IT-Systemen durch Menschen

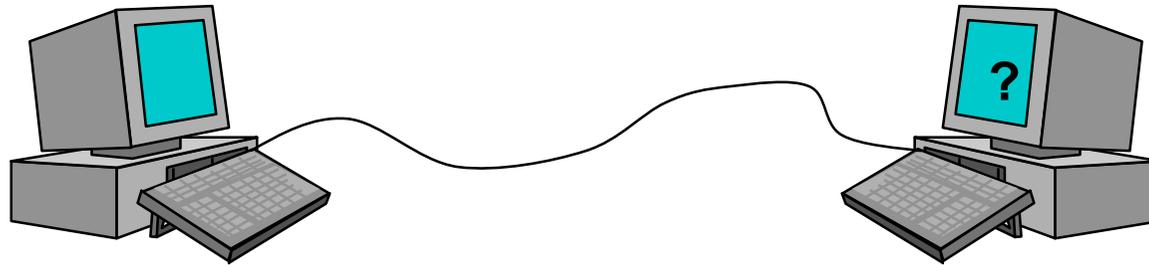


Was es *ist* → Gehäuse
→ Siegel, Hologramm
→ Verschmutzung

weiß → Passwort
→ Antworten auf Fragen
→ Rechnerergebnisse für Zahlen

Wo es *steht*

Identifikation von IT-Systemen durch IT-Systeme



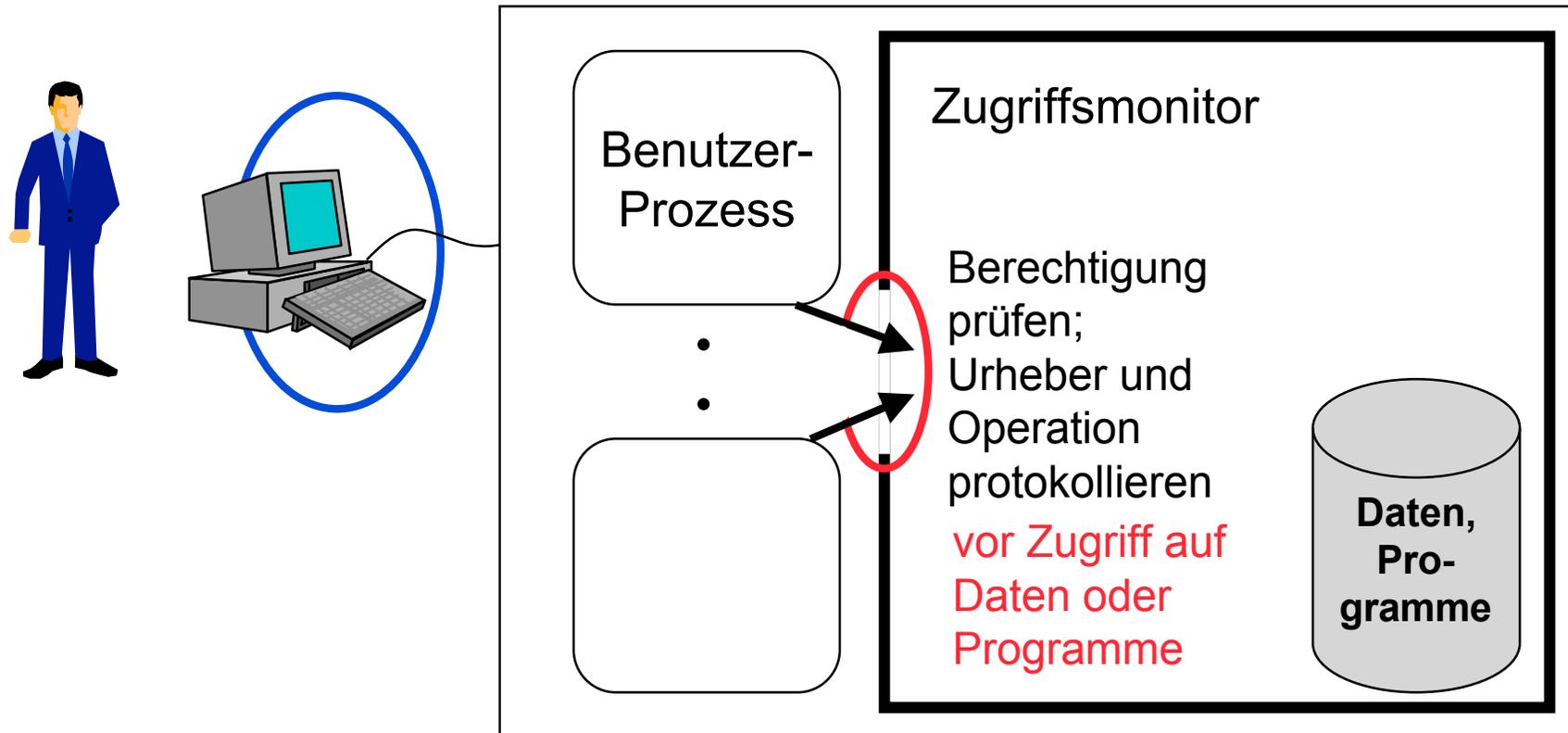
Was es *weiß*

- Passwort
- Antworten auf Fragen
- Rechnerergebnisse für Zahlen
- **Kryptographie**

Leitung *woher*

Zugangs- und Zugriffskontrolle

Zugangskontrolle nur mit berechtigten Partnern kommunizieren



Zugriffskontrolle Subjekt kann Operationen auf Objekt nur ausführen, wenn es ein Recht dazu hat.

Computer-Virus vs. Transitives Trojanisches Pferd

Computer-Virus



transitives Trojanisches Pferd



Zugriffskontrolle

Beschränkung der Angriffsausbreitung durch geringstmögliche Privilegierung:

Keine unnötigen Zugriffsrechte gewähren !

➡ Keine Computer-Viren, nur noch transitive trojanische Pferde !

Grundsätzliches zu Computer-Viren und Troj. Pferden

Andere Maßnahmen versagen:

1. Nicht entscheidbar, ob Programm ein Computer-Virus ist
Beweis (ind.) Annahme decide (•)

```

program Gegenbeispiel
  if decide (Gegenbeispiel) then keine_Virusfkt
                                else Virusfkt
  
```

2. Nicht entscheidbar, ob Programm ein Trojanisches Pferd ist

Also: Besser zu vorsichtig!

3. Selbst bekannte Computer-Viren nicht wirksam erkennbar
Selbstmodifikation  ~~Viren Scanner~~

4. dito Trojanische Pferde

5. Schaden bzgl. Daten hinterher nicht ermittelbar
Schadensfkt. könnte sich selbst modifizieren

Restprobleme

1. Genau spezifizieren, was IT-System tun und *unterlassen* soll.
2. *Totale Korrektheit* der Implementierung nachweisen. **heute**
3. Alle *verdeckten Kanäle* erkannt ?

?

?

?

Goldene Regel

IT-System so als verteiltes System entwerfen und realisieren, dass begrenzt viele angreifende Rechner keinen wesentlichen Schaden anrichten können.

Verteiltes System

Aspekte von Verteiltheit

räumliche Verteiltheit

verteilte Kontroll- und Implementierungsstruktur

verteiltes System:

keine Instanz hat globale Systemsicht

Sicherheit in verteilten Systemen

Vertrauenswürdige Endgeräte

vertrauenswürdig nur für Benutzer
 auch für andere

Kommunikationsfähigkeit

Verfügbarkeit durch Redundanz und Diversität

Kryptographie

Vertraulichkeit durch Verschlüsselung
Integrität durch MACs oder digitale Signaturen

Verfügbarkeit

Infrastruktur mit geringstmöglicher Entwurfskomplexität

Anschluß an vollständig diversitäre Netze

unterschiedliche Frequenzbänder bei Funk

unterschiedliche Leitungsführung bei leitungsgebundenen Netzen

Diversitätsengpässe vermeiden

z.B. Funknetz benötigt gleiche OVSt,

für alle Anschlußleitungen gibt es nur einen Übergangspunkt ins Fernnetz

Kryptologische Grundlagen

erreichbare Schutzziele:

Vertraulichkeit, Konzelation genannt

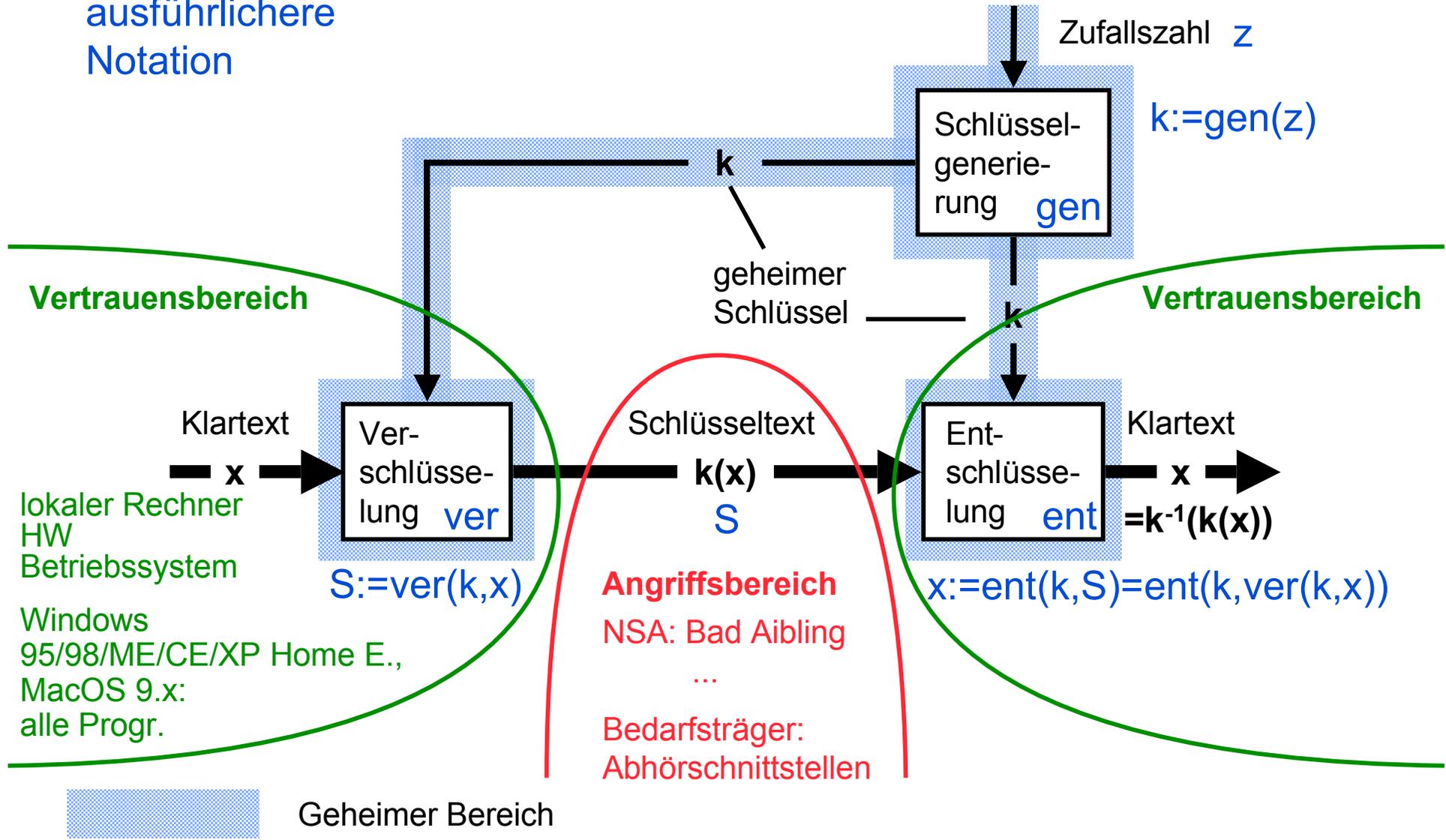
Integrität (= keine *unerkannte* unbefugte Modifikation von Informationen), Authentikation genannt

durch Kryptographie unerreichbar:

Verfügbarkeit – zumindest nicht gegen starke Angreifer

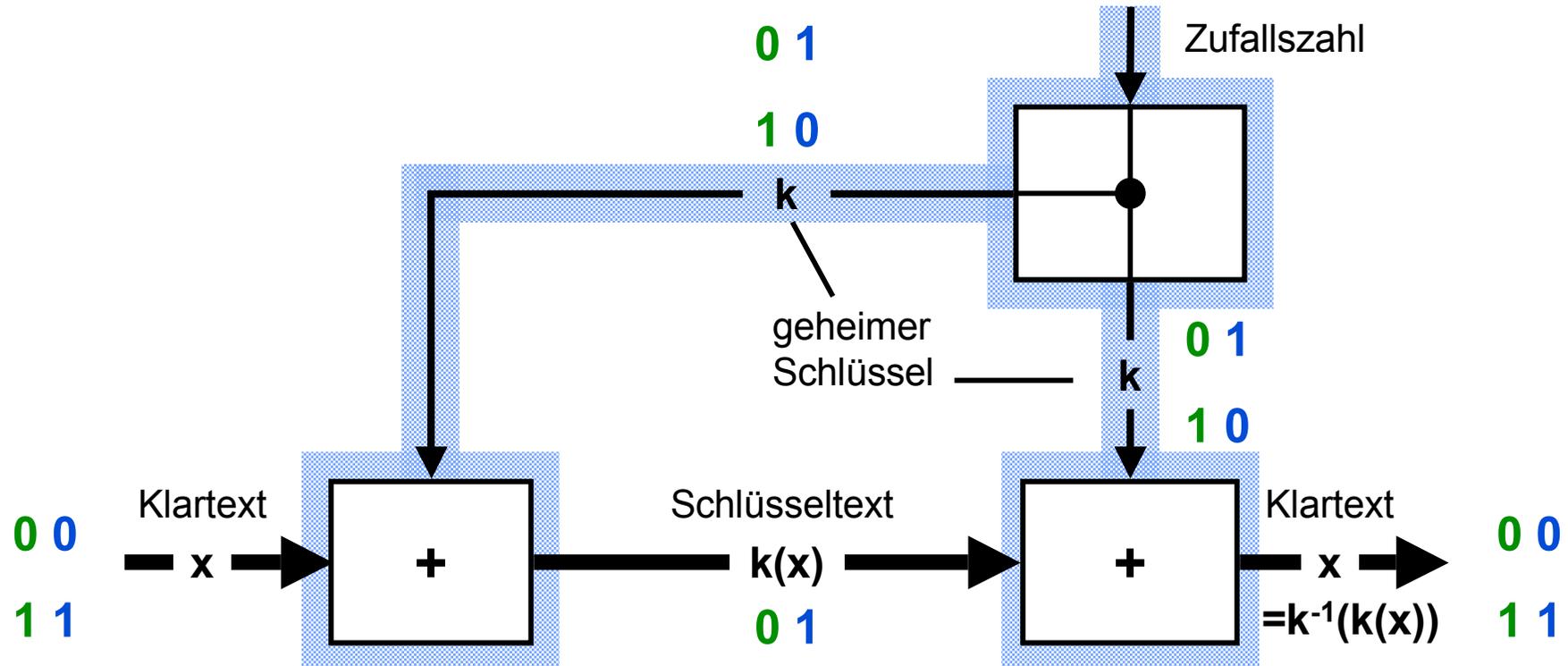
Symmetrisches Konzelationssystem

ausführlichere
Notation



Undurchsichtiger Kasten mit Schloß; 2 gleiche Schlüssel

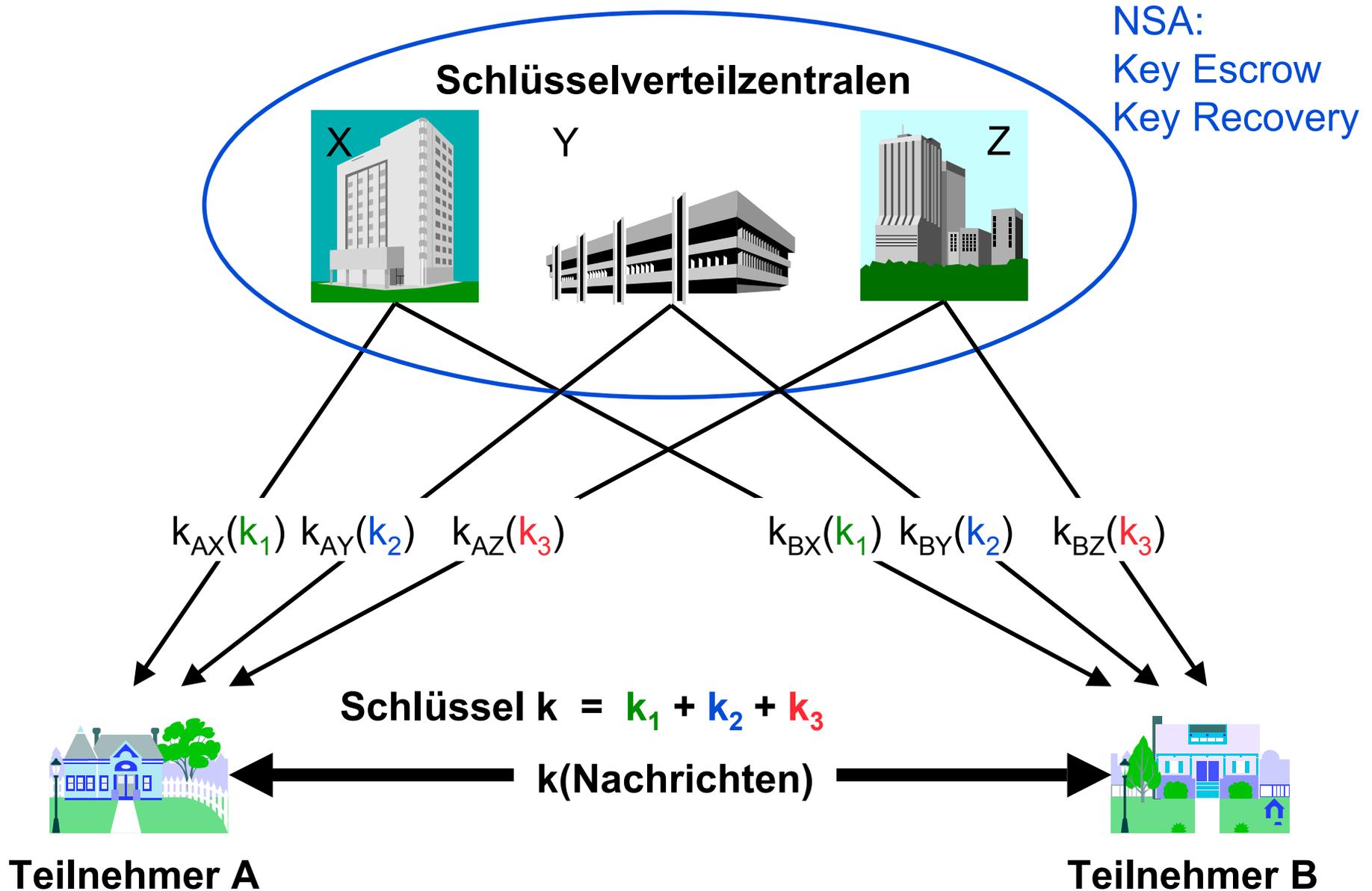
Bsp. Vernam-Chiffre (=one-time-pad)



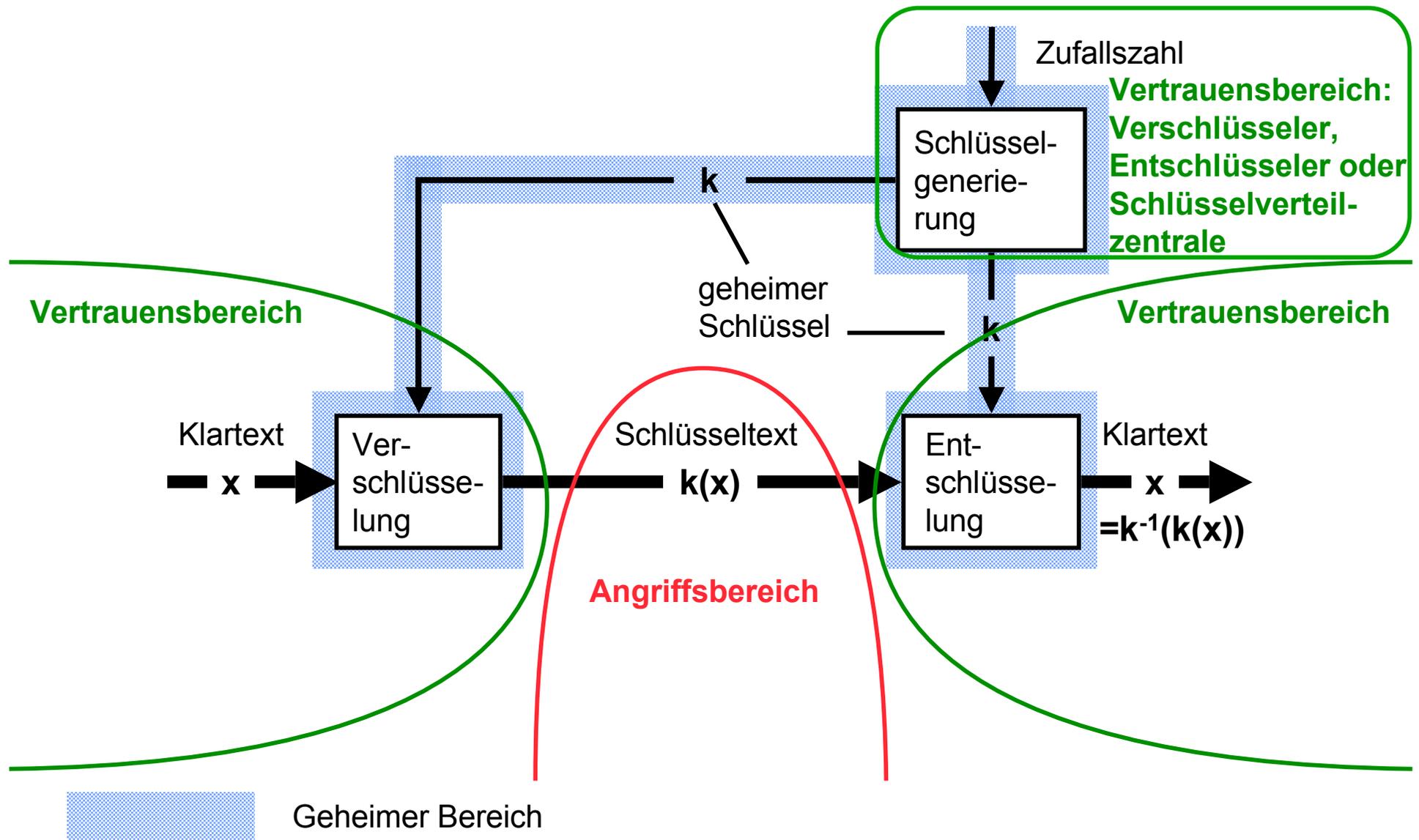
 Geheimer Bereich

Undurchsichtiger Kasten mit Schloß; 2 gleiche Schlüssel

Schlüsselverteilung bei symmetrischem Kryptosystem

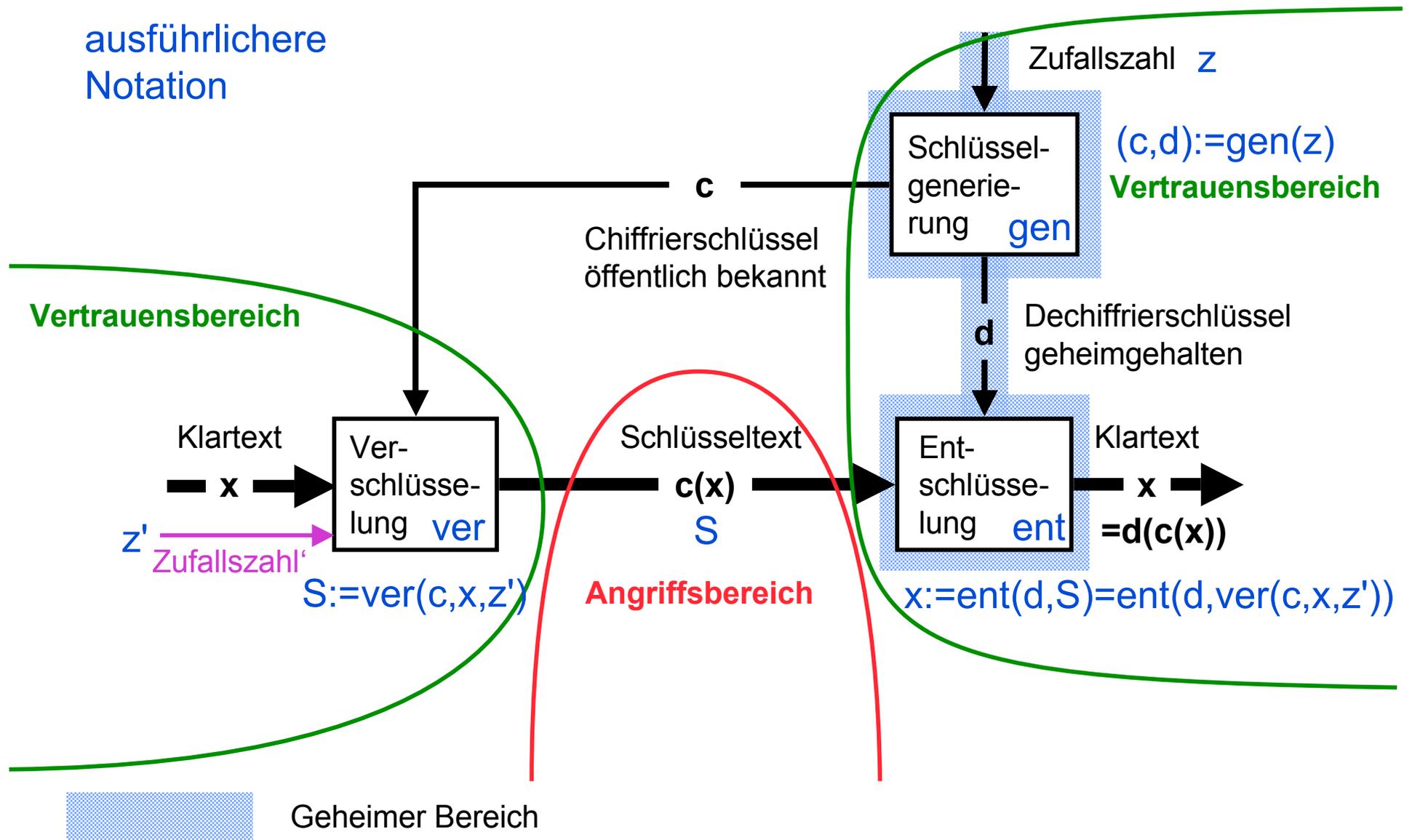


Sym. Konz.system: Vertrauensbereich Schlüsselgenerierung



Asymmetrisches Konzelationssystem

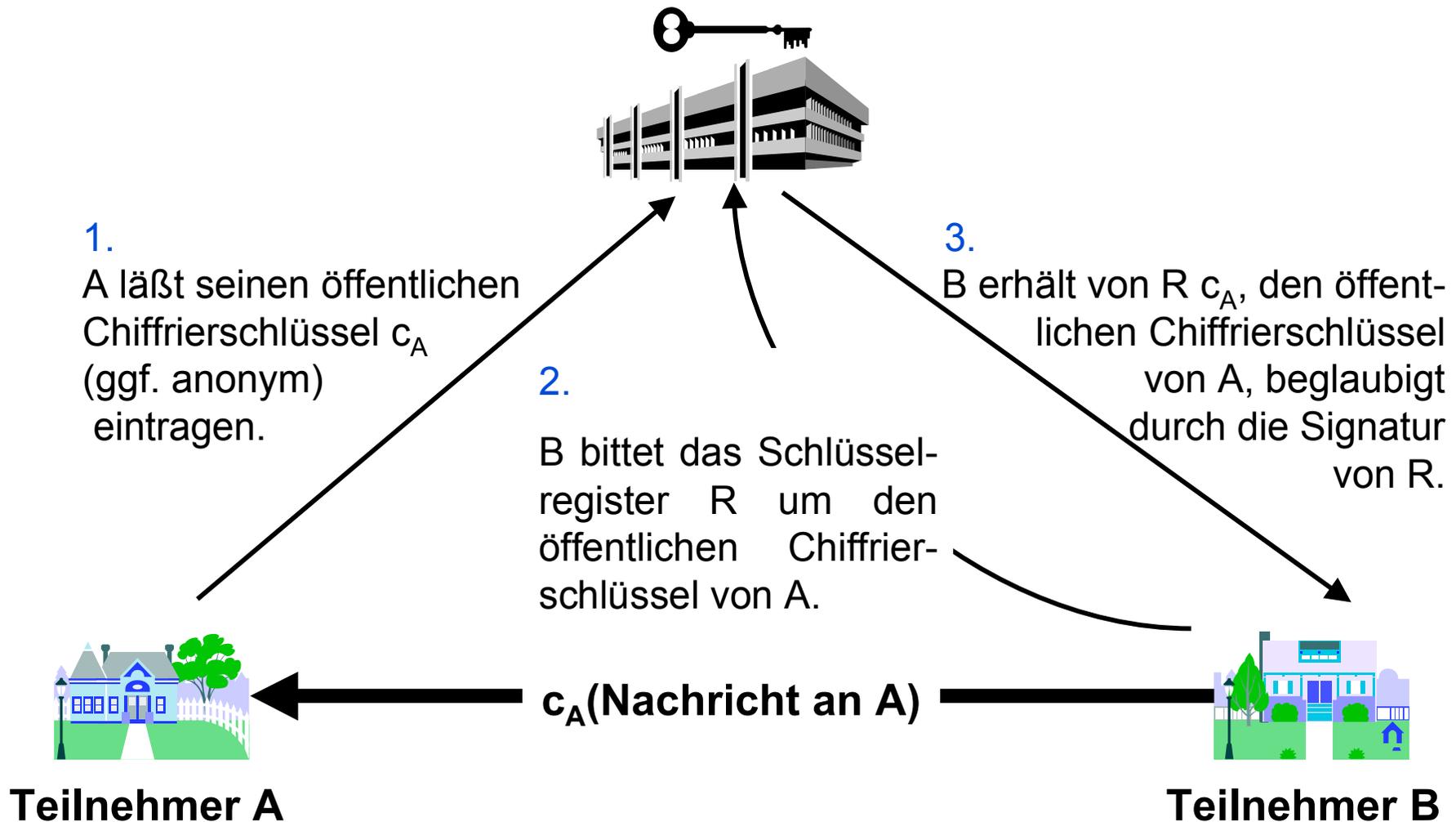
ausführlichere
Notation



Undurchsichtiger Kasten mit Schnappschloß; 1 Schlüssel

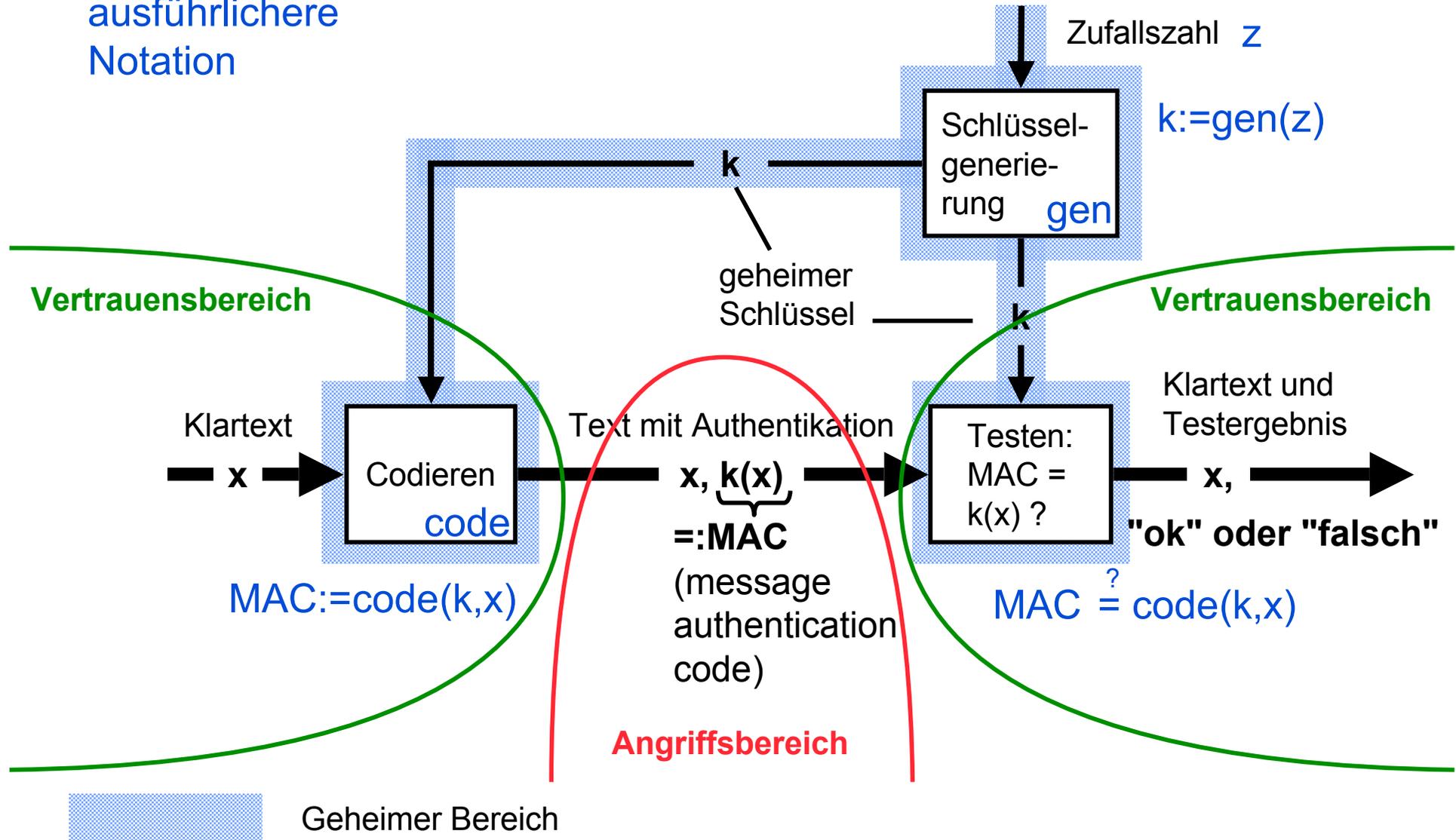
Schlüsselverteilung bei asymmetrischem Konzelationssystem

Öffentliches Schlüsselregister R



Symmetrisches Authentifikationssystem

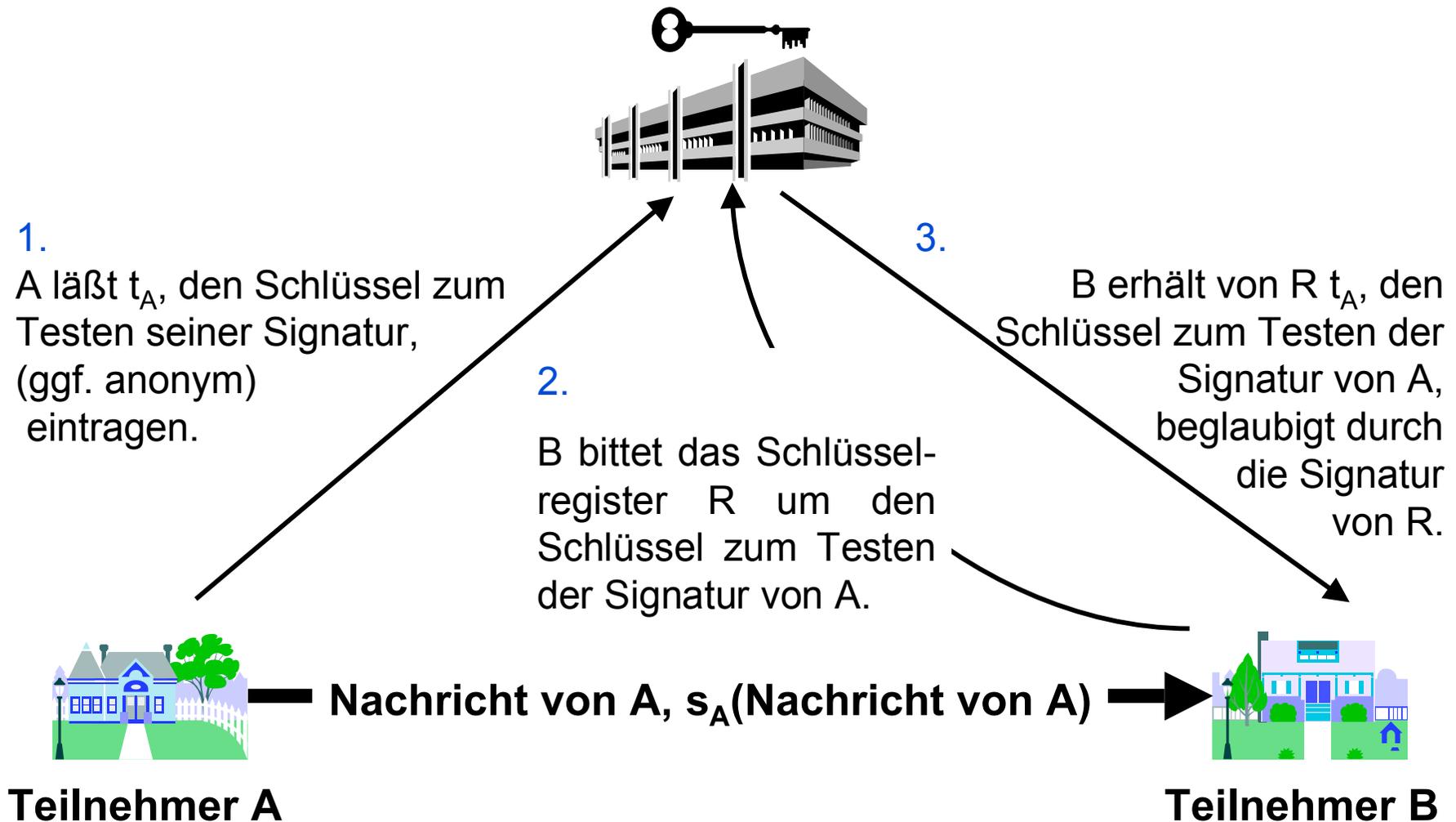
ausführlichere
Notation



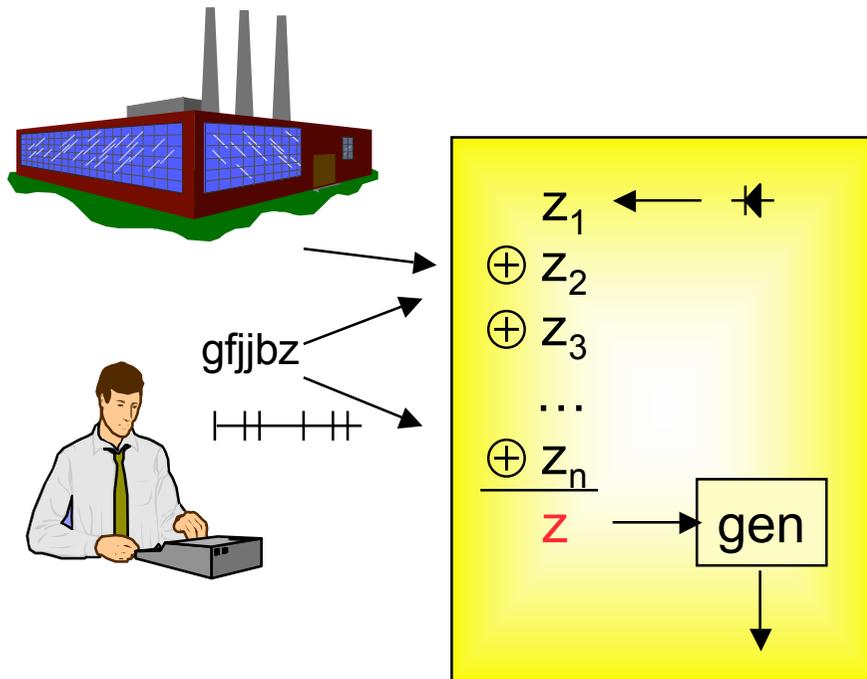
Glasvitrine mit Schloß; 2 gleiche Schlüssel

Schlüsselverteilung bei digitalem Signatursystem

Öffentliches Schlüsselregister R



Schlüsselgenerierung



Erzeugung einer Zufallszahl z für die Schlüsselgenerierung:

XOR aus

- z_1 , einer im Gerät erzeugten,
- z_2 , einer vom Hersteller gelieferten,
- z_3 , einer vom Benutzer gelieferten,
- z_n , einer aus Zeitabständen errechneten.

Anmerkungen zum Schlüsselaustausch

Wem werden Schlüssel zugeordnet?

1. einzelnen Teilnehmern **asymmetrische Systeme**
2. Paarbeziehungen **symmetrische Systeme**
3. Gruppen **—**

Wieviele Schlüssel müssen ausgetauscht werden?

n Teilnehmer

asymmetrische Systeme je System n

symmetrische Systeme $n \cdot (n-1)$

Wann Schlüssel generieren und austauschen?

**Sicherheit des Schlüsselaustauschs begrenzt
kryptographisch erreichbare Sicherheit:**

Mehrere Ur-Schlüsselaustausche durchführen

Angriffsziel/ -erfolg



a) Schlüssel (total break)

b) zum Schlüssel äquivalentes Verfahren (universal break)

c) einzelne Nachrichten,

z.B. speziell für Authentikationssysteme

c1) eine gewählte Nachricht (selective break)

c2) irgendeine Nachricht (existential break)

Angriffstypen

a) passiv

a1) reiner Schlüsseltext-Angriff (ciphertext-only attack)

a2) Klartext-Schlüsseltext-Angriff (known-plaintext attack)

b) aktiv

(je nach Kryptosystem; asym.: eins von beiden: b1 oder b2;
 sym.: ggf. beides: auch b1 und b2)

b1) **Signaturssystem**: Klartext → Schlüsseltext
 (chosen-plaintext attack)

b2) **Konzelationss.**: Schlüsseltext → Klartext
 (chosen-ciphertext attack)

Adaptivität

nicht adaptiv

adaptiv

Kriterium: Handlung

passiver Angreifer

aktiver Angreifer

Erlaubnis

beobachtender Angreifer

verändernder Angreifer

≠

≠

Grundsätzliches über „kryptographisch stark“

Falls keine informationstheoretische Sicherheit:

1) Verwendung von Schlüssel der festen Länge \mathcal{L} :

- Angreiferalgorithmus kann immer alle $2^{\mathcal{L}}$ Schlüssel durchprobieren (bricht asym. Kryptosysteme und sym. bei Klartext-Schlüsseltext-Angriff).
- erfordert exponentiell viele Operationen (ist also für $\mathcal{L} > 100$ zu aufwendig).

→ das Beste, was der Kryptosystementwerfer erhoffen kann.

2) Komplexitätstheorie:

- liefert hauptsächlich asymptotische Resultate
 - behandelt hauptsächlich "worst-case"-Komplexität
- für Sicherheit unbrauchbar, ebenso "average-case"-Komplexität.

Wunsch: Problem soll fast überall, d.h. bis auf einen verschwindenden Bruchteil der Fälle, schwer sein.

- Sicherheitsparameter \mathcal{L} (allgemeiner als Schlüssellänge; praktisch nützlich)
- Wenn $\underbrace{\mathcal{L} \rightarrow \infty}$, dann $\underbrace{\text{Brechwahrscheinlichkeit} \rightarrow 0}$.
- Hoffnung: langsam schnell

Grundsätzliches über „kryptographisch stark“ (Forts.)

3) 2 Komplexitätsklassen:

Ver-/Entschlüsseln: leicht = polynomiell in \mathcal{L}

Brechen: schwer = nicht polynomiell in $\mathcal{L} \approx$ exponentiell in \mathcal{L}

Warum?

a) Schwerer als exponentiell geht nicht, siehe 1).

b) Abgeschlossen: Einsetzen von Polynomen in Polynome ergibt Polynome.

c) Vernünftige Berechnungsmodelle (Turing-, RAM-Maschine) sind polynomiell äquivalent.

Für die Praxis würde Polynom von hohem Grad für Laufzeit des Angreiferalgorithmus auf RAM-Maschine reichen.

4) Warum Komplexitätstheoretische Annahmen? z.B. Faktorisierung schwer
Komplexitätstheorie kann bisher keine brauchbaren unteren Schranken beweisen. Kompakte, languntersuchte Annahmen!

5) Was, wenn sich Annahme als falsch herausstellt?

a) Andere Annahmen treffen.

b) Genauere Analyse, z.B. Berechnungsmodell genau fixieren und dann untersuchen, ob Polynom von genügend hohem Grad.

6) Beweisziel: Wenn der Angreiferalgorithmus das Kryptosystem brechen kann, dann kann er auch das als schwer angenommene Problem lösen.

Sicherheitsklassen kryptographischer Systeme

Sicherheit



1. informationstheoretisch sicher
2. kryptographisch stark
3. wohluntersucht
4. wenig untersucht
5. geheim gehalten

Überblick über kryptographische Systeme

Systemtyp		Konzeleation		Authentifikation	
		sym.	asym.	sym.	asym.
Sicherheit		sym. Konzeleations system	asym. Konzeleations system	sym. Authentika- tionssystem	asym. digitales Signatur- system
	informationstheoretisch	Vernam- Chiffre (one- time pad)	1	Authentika- tionscodes	2
kryptogra- phisch stark gegen...	aktiver Angriff	Pseudo-one- time-pad mit s^2 -mod- n - Generator	3 CS ?	4	GMR
	passiver Angriff	5	System mit mit s^2 -mod- n -Generator	6	7
wohlunter- sucht	Mathematik	8	RSA	9	RSA
	Chaos	DES	10	DES	11

Hybride Kryptosysteme (1)

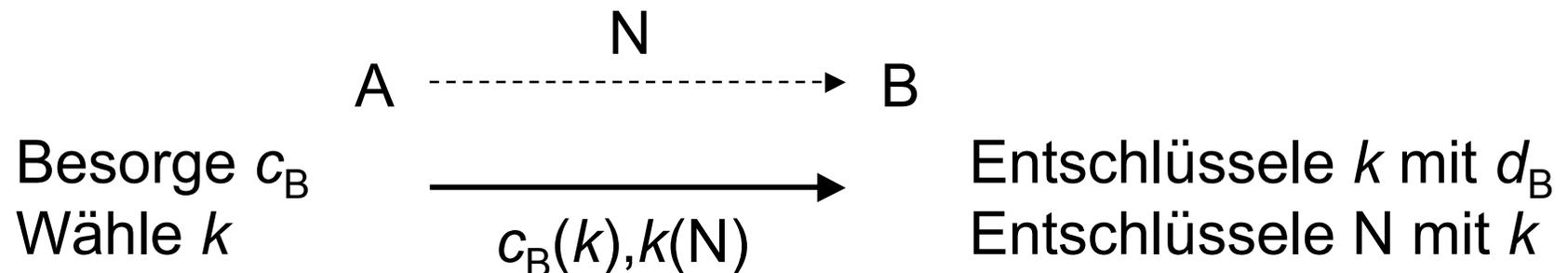
Kombiniere:

- von asymmetrischen: Einfache Schlüsselverteilung
- von symmetrischen: Effizienz (Faktor 100 bis 10000, SW und HW)

Wie?

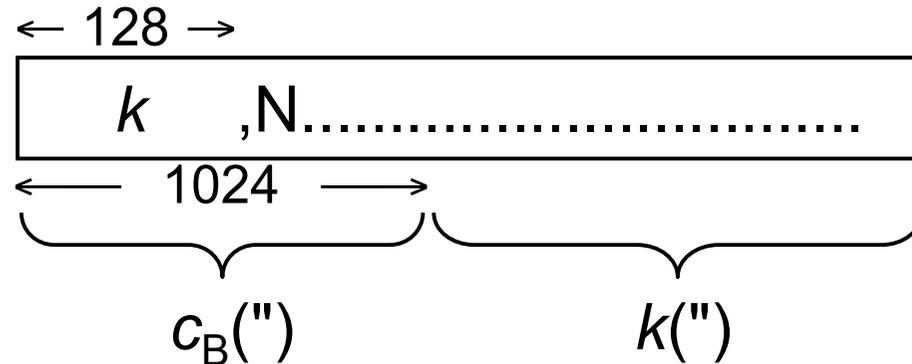
Asymmetrisches System nur, um Schlüssel für symmetrisches auszutauschen

Konzeption:



Hybride Kryptosysteme (2)

Noch effizienter: Teil von N in 1. Block



Wenn B auch k benutzen soll: $s_A(B,k)$ dazulegen

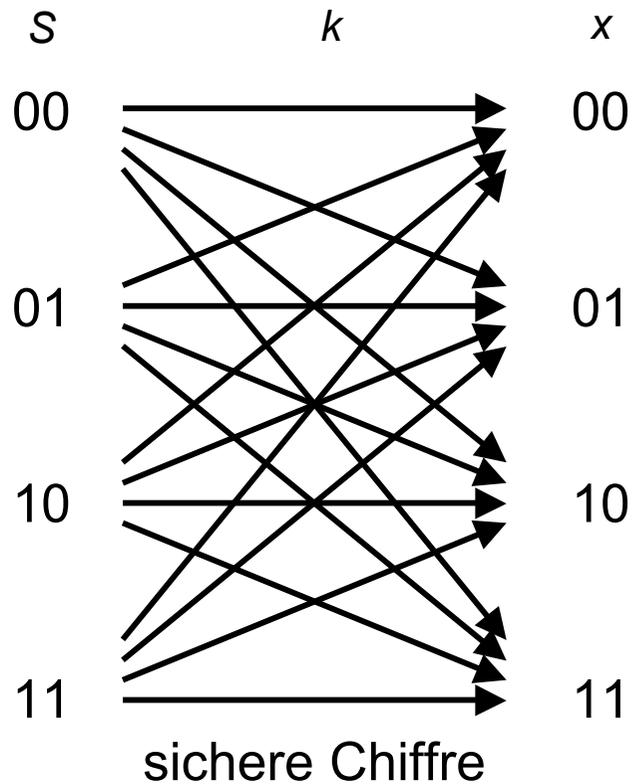
Authentikation: k authentisieren und geheimhalten

Besorge c_B Wähle k	$\xrightarrow{\quad}$	Besorge t_A Entschlüssele $c_B(B,k,s_A(B,k))$ Teste B,k mit t_A Teste N mit k
	$N, k(N), c_B(B, k, s_A(B, k))$	
	$\underbrace{\hspace{10em}}_{\text{MAC}}$	

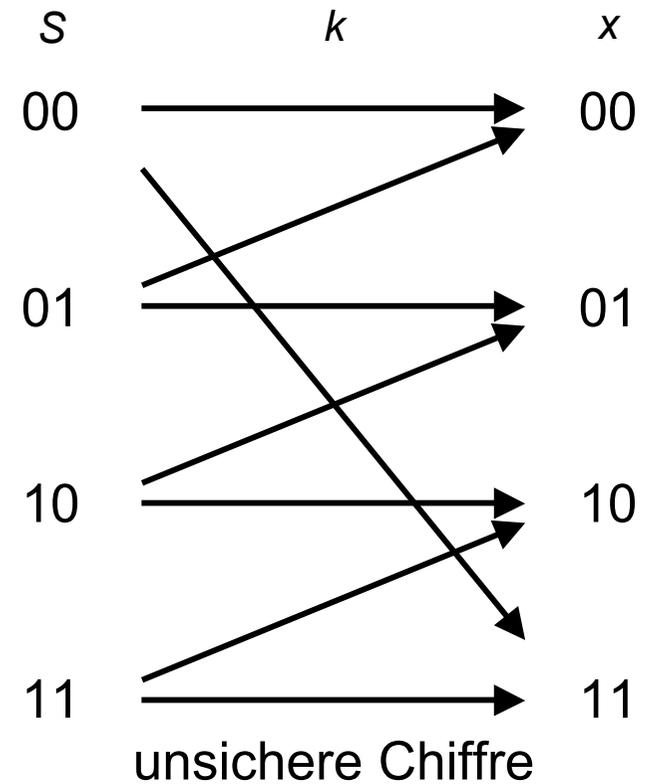
Informationstheoretisch sichere Konzelation

"Hinter jedem Schlüsseltext S kann sich jeder Klartext gleich gut verbergen"

Schlüsseltext Schlüssel Klartext



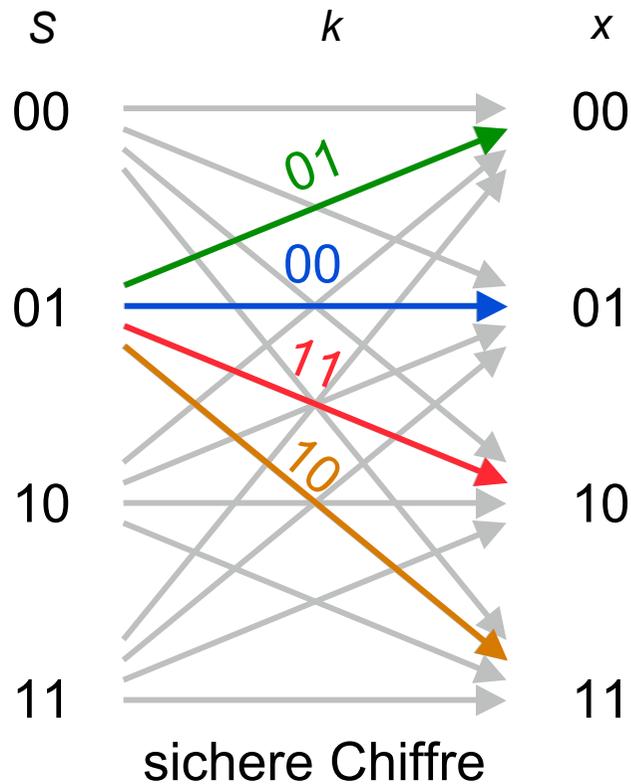
Schlüsseltext Schlüssel Klartext



Informationstheoretisch sichere Konzelation

"Hinter jedem Schlüsseltext S kann sich jeder Klartext gleich gut verbergen"

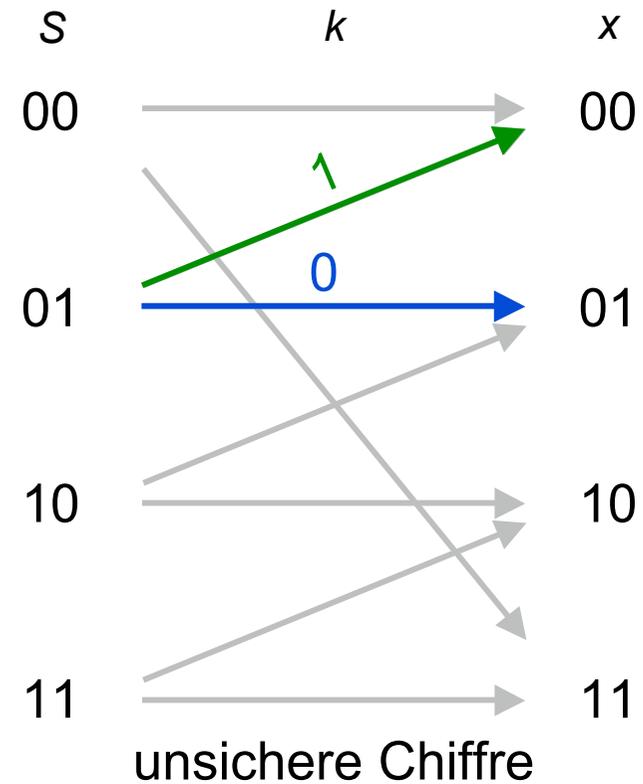
Schlüsseltext Schlüssel Klartext



Bsp.: Vernam-Chiffre mod 2

$$\begin{array}{r}
 x = 00\ 01\ 00\ 10 \\
 \oplus k = 10\ 11\ 01\ 00 \\
 \hline
 S = 10\ 10\ 01\ 10
 \end{array}$$

Schlüsseltext Schlüssel Klartext



Subtraktion von einem Schlüsselbit mod 4 von zwei Klartextbits

Vernam-Chiffre (one-time pad)

Alle Zeichen sind Elemente einer Gruppe G .
Klartext, Schlüssel und Schlüsseltext sind Zeichenketten.

Zur Verschlüsselung einer Zeichenkette x der Länge n wird ein zufällig gewählter und vertraulich auszutauschender Schlüssel $k=(k_1, \dots, k_n)$ verwendet.

Das i -te Klartextzeichen x_i wird verschlüsselt als

$$S_i := x_i + k_i$$

Entschlüsselt werden kann es durch

$$x_i := S_i - k_i.$$

Gegen adaptive Angriffe sicher; einfach zu berechnen; Schlüssel aber sehr lang

Für informationsth. Sicherheit *müssen* Schlüssel so lang sein

Sei \mathcal{K} Schlüsselmenge, \mathcal{X} Klartextmenge und \mathcal{S} Menge der mindestens einmal auftretenden Schlüsseltexte.

$|\mathcal{S}| \geq |\mathcal{X}|$ damit eindeutig entschlüsselbar (k fest)

$|\mathcal{K}| \geq |\mathcal{S}|$ damit hinter jedem Schlüsseltext jeder Klartext stecken kann (x fest)

also $|\mathcal{K}| \geq |\mathcal{X}|$.

Falls Klartext geschickt codiert, folgt:

Schlüssel mindestens so lang wie Klartext.

Definitionen für informationstheoretische Sicherheit

1. Definition für informationstheoretische Sicherheit

(alle Schlüssel mit gleicher Wahrscheinlichkeit gewählt)

$$\forall S \in \mathcal{S} \exists \text{const} \in \mathbb{N} \forall x \in \mathcal{X}: |\{k \in \mathcal{K} \mid k(x) = S\}| = \text{const}. \quad (1)$$

Die a-posteriori-Wahrscheinlichkeit eines Klartextes x , wenn der Angreifer den Schlüsseltext S gesehen hat, ist $W(x|S)$.

2. Definition

$$\forall S \in \mathcal{S} \forall x \in \mathcal{X}: W(x|S) = W(x). \quad (2)$$

Beide Definitionen sind äquivalent:

Nach Bayes gilt:

$$W(x|S) = \frac{W(x) \cdot W(S|x)}{W(S)}$$

(2) ist also äquivalent zu

$$\forall S \in \mathcal{S} \forall x \in \mathcal{X}: W(S|x) = W(S). \quad (3)$$

Wir zeigen, dass dies äquivalent ist zu

$$\forall S \in \mathcal{S} \exists \text{const}' \in \mathbb{R} \forall x \in \mathcal{X}: W(S|x) = \text{const}'. \quad (4)$$

Beweis

(3) \Rightarrow (4) ist klar mit $const' := W(S)$.

Umgekehrt zeigen wir $const' = W(S)$:

$$\begin{aligned}
 W(S) &= \sum_x W(x) \cdot W(S|x) \\
 &= \sum_x W(x) \cdot const' \\
 &= const' \cdot \sum_x W(x) \\
 &= const'.
 \end{aligned}$$

(4) sieht (1) schon sehr ähnlich: Allgemein ist

$$W(S|x) = W(\{k \mid k(x) = S\}),$$

und wenn alle Schlüssel gleichwahrscheinlich sind,

$$W(S|x) = |\{k \mid k(x) = S\}| / |\mathcal{K}|.$$

Dann ist (4) äquivalent (1) mit

$$const = const' \cdot |\mathcal{K}|.$$

Symmetrische Authentifikationssysteme (1)

Schlüsselverteilung:

Wie symmetrische Konzelationssysteme

Einfaches Beispiel (Angreifersicht)

		x, MAC			
		H,0	H,1	T,0	T,1
k	00	H	-	T	-
	01	H	-	-	T
	10	-	H	T	-
	11	-	H	-	T

Sicherheit: z.B. Angreifer will T senden.

a) blind : Erwischt mit Wahrscheinlichkeit 0,5

b) sehend : z.B. H,0 abgefangen $\Rightarrow k \in \{00, 01\}$

Immer noch T,0 und T,1 mit Wahrscheinlichkeit 0,5

Symmetrische Authentifikationssysteme (2)

Definition „Informationstheoretische Sicherheit“ mit Fehlerwahrscheinlichkeit ε :

$\forall x, \text{MAC}$ (die Angreifer sieht)

$\forall y \neq x$ (das Angreifer statt x sendet)

$\forall \text{MAC}'$ (von denen Angreifer den besten für y aussucht)

$$W(k(y) = \text{MAC}' \mid k(x) = \text{MAC}) \leq \varepsilon$$

(Wahrscheinlichkeit, dass MAC' stimmt, wenn man nur die Schlüssel k betrachtet, die wegen (x, MAC) noch möglich sind.)

Verbesserung des Beispiels:

a) 2σ Schlüsselbits statt 2: $k = k_1 k_1^* \dots k_\sigma k_\sigma^*$

$\text{MAC} = \text{MAC}_1, \dots, \text{MAC}_\sigma$; MAC_i aus $k_i k_i^*$

\Rightarrow Fehlerwahrscheinlichkeit $2^{-\sigma}$

b) l Nachrichtenbits: $x^{(1)}, \text{MAC}^{(1)} = \text{MAC}_1^{(1)}, \dots, \text{MAC}_\sigma^{(1)}$

\vdots

\vdots

\vdots

$x^{(l)}, \text{MAC}^{(l)} = \text{MAC}_1^{(l)}, \dots, \text{MAC}_\sigma^{(l)}$

Symmetrische Authentifikationssysteme (3)

Grenzen:

σ -bit-MAC \Rightarrow Fehlerwahrscheinlichkeit $\geq 2^{-\sigma}$
(MAC raten)

σ -bit-Schlüssel \Rightarrow Fehlerwahrscheinlichkeit $\geq 2^{-\sigma}$
(Schlüssel raten, MAC ausrechnen)

Noch klar: Für Fehlerwahrscheinlichkeit $2^{-\sigma}$ reichen σ -bit-Schlüssel nicht,
denn $k(x) = \text{MAC}$ schließt viele k 's aus.

Satz: Man braucht 2σ -bit-Schlüssel

(Für weitere Nachrichten reichen σ , wenn Empfänger auf Authentifikations“fehler“ geeignet reagiert.)

Möglich zur Zeit: $\approx 4\sigma \cdot \log_2(\text{Länge}(x))$

(Wegman, Carter)

Viel kürzer als one-time pad.

RSA - asymmetrisches Kryptosystem

R. Rivest, A. Shamir, L. Adleman: A Method for obtaining Digital Signatures and Public-Key Cryptosystems
Communications of the ACM 21/2 (Feb. 1978) 120-126.

Schlüsselgenerierung

1) Wähle zwei Primzahlen p und q zufällig sowie stochastisch unabhängig mit $|p| \approx |q| = l$, $p \neq q$

2) Berechne $n := p \cdot q$

3) Wähle c mit $\text{ggT}(c, \underbrace{(p-1)(q-1)}_{\Phi(n)}) = 1$

4) Berechne d mittels p , q , c als multiplikatives Inverses von c modulo $\Phi(n)$

$$c \cdot d \equiv 1 \pmod{\Phi(n)}$$

Veröffentliche c und n .

Ver-/Entschlüsselung

Exponentiation mit c bzw. d in \mathbb{Z}_n

Beh.: $\forall m \in \mathbb{Z}_n$ gilt: $(m^c)^d \equiv m^{c \cdot d} \equiv (m^d)^c \equiv m \pmod{n}$

Beweis (1)

$$c \cdot d \equiv 1 \pmod{\Phi(n)} \Leftrightarrow$$

$$\exists k \in \mathbb{Z} : c \cdot d - 1 = k \cdot \Phi(n) \Leftrightarrow$$

$$\exists k \in \mathbb{Z} : c \cdot d = k \cdot \Phi(n) + 1$$

Also gilt $m^{c \cdot d} \equiv m^{k \cdot \Phi(n) + 1} \pmod{n}$

Mittels des **Fermatschen Satzes**

$$\forall m \in \mathbb{Z}_n^* : m^{\Phi(n)} \equiv 1 \pmod{n}$$

folgt für alle zu p teilerfremden m

$$m^{p-1} \equiv 1 \pmod{p}$$

Da $p-1$ ein Teiler von $\Phi(n)$ ist, gilt

$$m^{k \cdot \Phi(n) + 1} \equiv_p m^{k \cdot (p-1)(q-1) + 1} \equiv_p m \cdot \underbrace{(m^{p-1})^{k \cdot (q-1)}}_1 \equiv_p m$$

Beweis (2)

Gilt trivialerweise für $m \equiv_p 0$

Entsprechende Argumentation für q ergibt

$$m^{k \cdot \Phi(n) + 1} \equiv_q m$$

Da Kongruenz sowohl bzgl. p als auch q gilt, gilt sie auch

bzgl. $p \cdot q = n$

$$m^{c \cdot d} \equiv m^{k \cdot \Phi(n) + 1} \equiv m \pmod{n}$$

Vorsicht:

Es gibt (bisher ?) **keinen** Beweis

RSA leicht zu brechen \Rightarrow Faktorisierung leicht

Naiver unsicherer Einsatz von RSA

RSA als asymmetrisches Konzelationssystem

Codiere Nachricht (ggf. geblockt) als Zahl $m < n$.

Verschlüsselung von m : $m^c \bmod n$

Entschlüsselung von m^c : $(m^c)^d \bmod n = m$

RSA als digitales Signatursystem

Umbenennung: $c \rightarrow t, d \rightarrow s$

Signieren von m : $m^s \bmod n$

Testen von m, m^s : $(m^s)^t \bmod n = m ?$

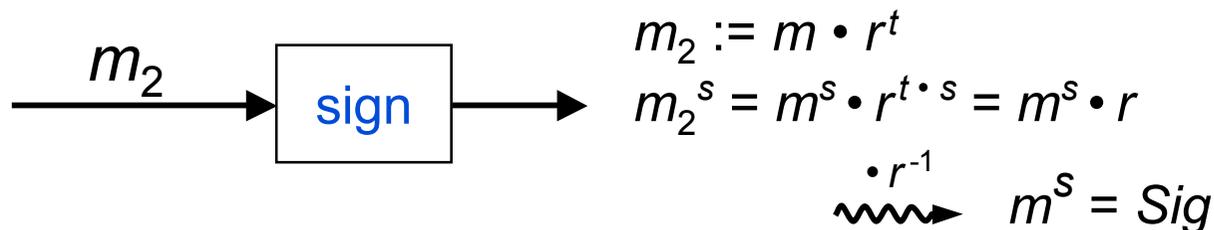
Hinführung zu den Davida-Angriffen

Einfache Version eines Davida-Angriffs: (auf RSA als Signatursystem)

- Gegeben $Sig_1 = m_1^s$
 $Sig_2 = m_2^s$
 $\Rightarrow Sig := Sig_1 \cdot Sig_2 = (m_1 \cdot m_2)^s$
 Neue Signatur erzeugt!
 (Passiver Angriff, dafür m nicht wählbar.)

- Aktiv, gewünscht** $Sig = m^s$
 Wähle m_1 beliebig; $m_2 := m \cdot m_1^{-1}$
 Lasse m_1, m_2 signieren.
 Weiter wie oben.

- Aktiv, trickreicher** (Moore)
 "Blinding" : Wähle r beliebig,



Aktiver Angriff von Davida auf RSA

1.) asymmetrisches Konzelationssystem: Entschlüsselung der gewählten Nachricht m^c

Angreifer	wählt Zufallszahl r , $0 < r < n$ bildet $r^c \bmod n$; dies ist gleichverteilt in $[1, n-1]$ läßt Angegriffenen $r^c \cdot m^c \equiv_n prod$ entschlüsseln
Angegriffener	bildet $prod^d \bmod n$
Angreifer	weiß, dass $prod^d \equiv_n (r^c \cdot m^c)^d \equiv_n r^{c \cdot d} \cdot m^{c \cdot d} \equiv_n r \cdot m$ teilt also $prod^d$ durch r und erhält so m .

Wenn das nicht geht: Faktorisiere n .

2.) digitales Signatursystem: Signieren der gewählten Nachricht m .

Angreifer	wählt Zufallszahl r , $0 < r < n$ bildet $r^t \bmod n$; dies ist gleichverteilt in $[1, n-1]$ läßt Angegriffenen $r^t \cdot m \equiv_n prod$ signieren
Angegriffener	bildet $prod^s \bmod n$
Angreifer	weiß, dass $prod^s \equiv_n (r^t \cdot m)^s \equiv_n r^{t \cdot s} \cdot m^s \equiv_n r \cdot m^s$ teilt also $prod^s$ durch r und erhält so m^s .

Wenn das nicht geht: Faktorisiere n .

Abwehr der Davida-Angriffe mittels kollisionsresist. Hashfkt.

$h()$: kollisionsresistente Hashfunktion

1.) asymmetrisches Konzelationssystem

Klartextnachrichten müssen Redundanzprädikat erfüllen

m , Redundanz \Rightarrow prüfe ob $h(m) = \text{Redundanz}$

2.) digitales Signatursystem

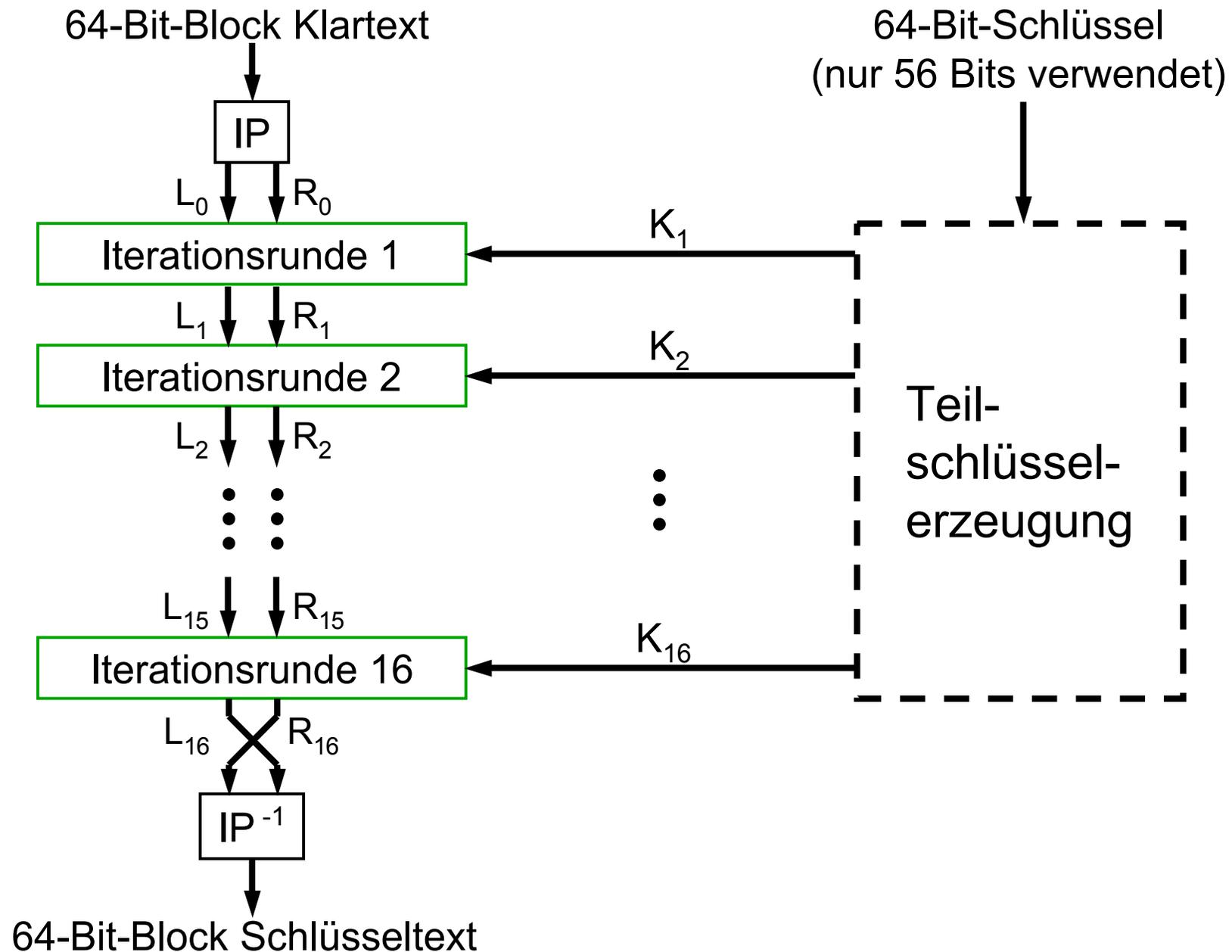
Vor dem Signieren wird auf die Nachricht h angewendet

Signatur zu $m = (h(m))^s \bmod n$

prüfe ob $h(m) = ((h(m))^s)^t \bmod n$

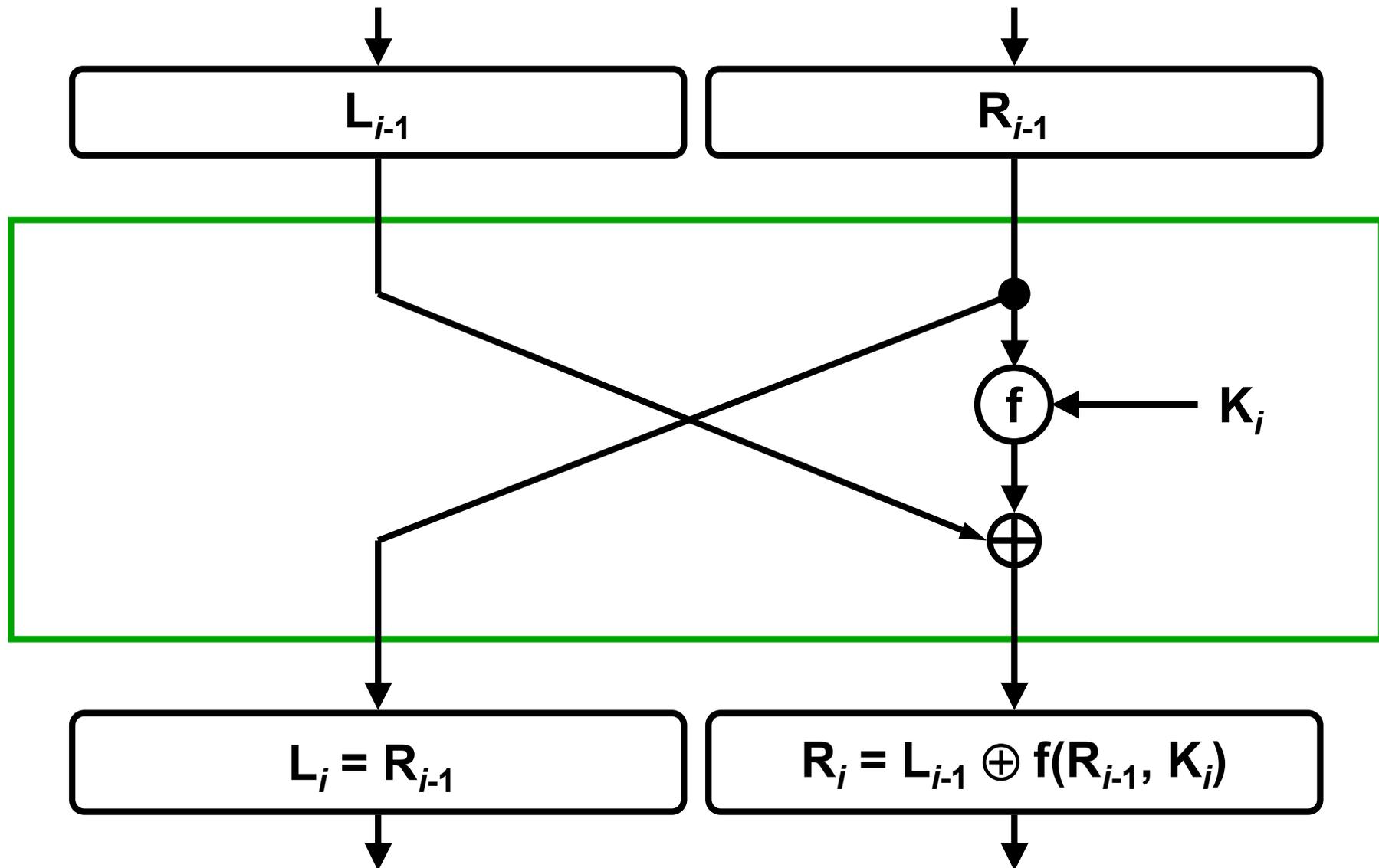
Vorsicht: Es gibt (bisher?) keinen Beweis für Sicherheit!

Symmetrisches Kryptosystem DES

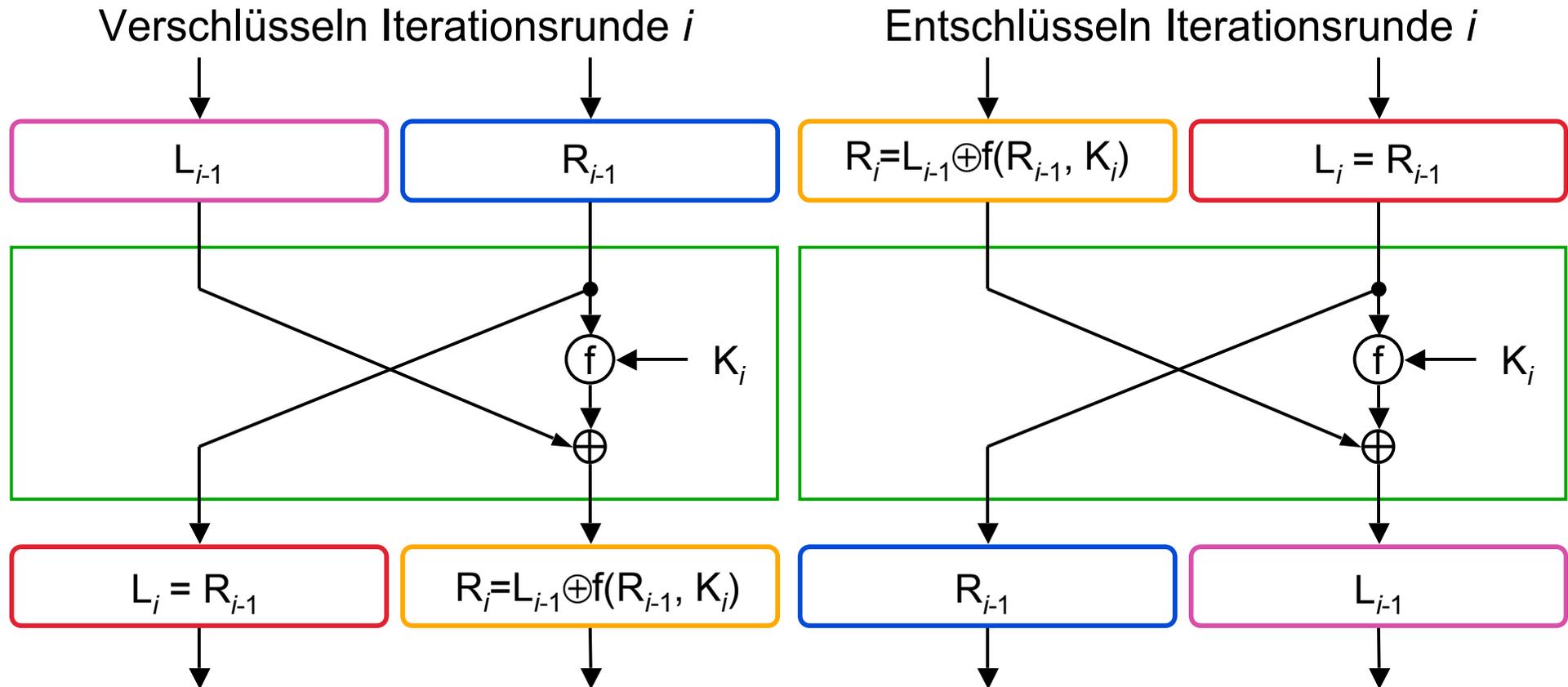


Eine Iterationsrunde

Feistel Chiffren



Entschlüsselungsprinzip



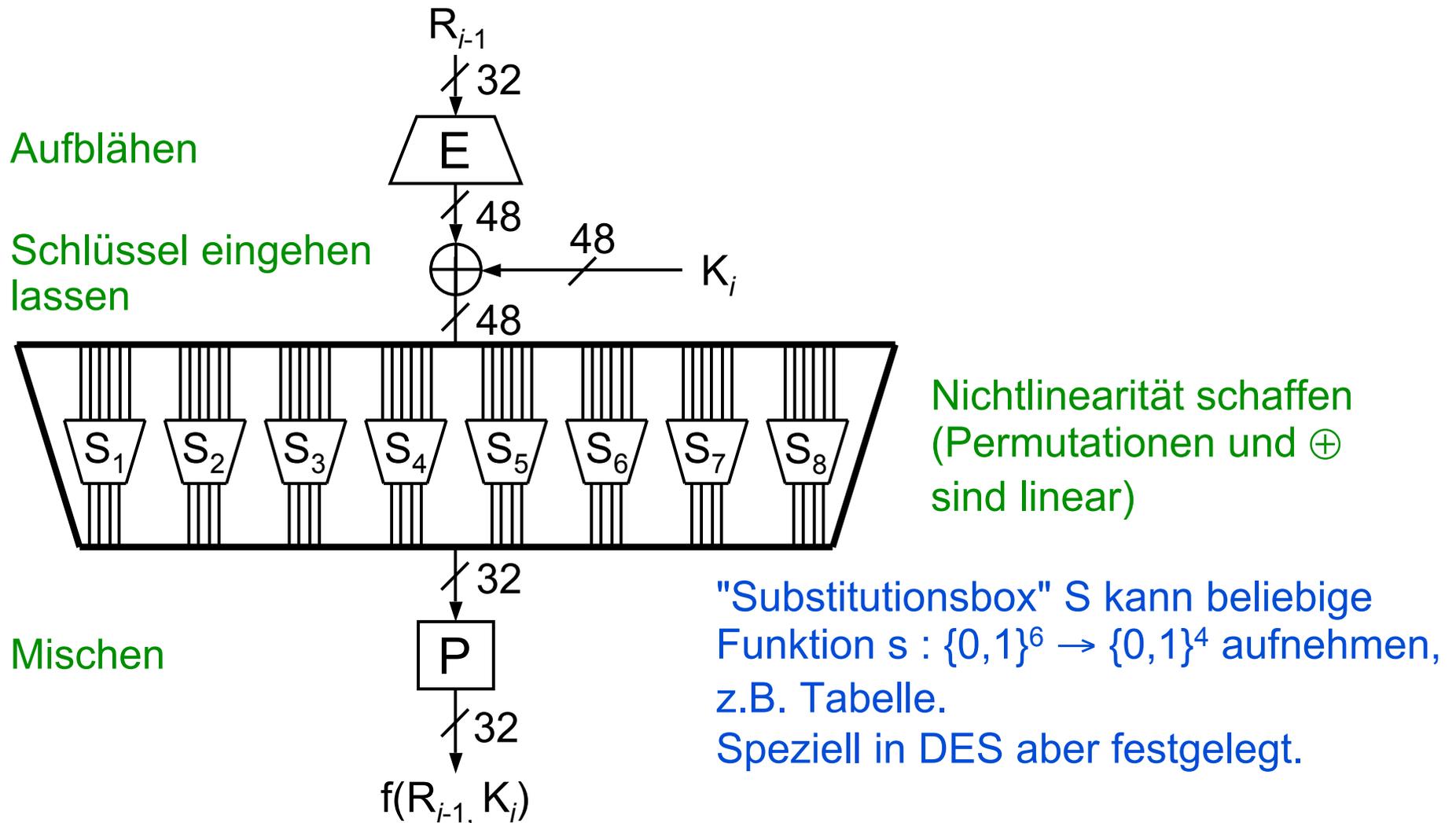
Entschlüsselungsprinzip

 \rightarrow trivial

 \rightarrow $L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(L_i, K_i) =$
 $L_{i-1} \oplus f(L_i, K_i) \oplus f(L_i, K_i) = L_{i-1}$

Ersetze R_{i-1} durch L_i

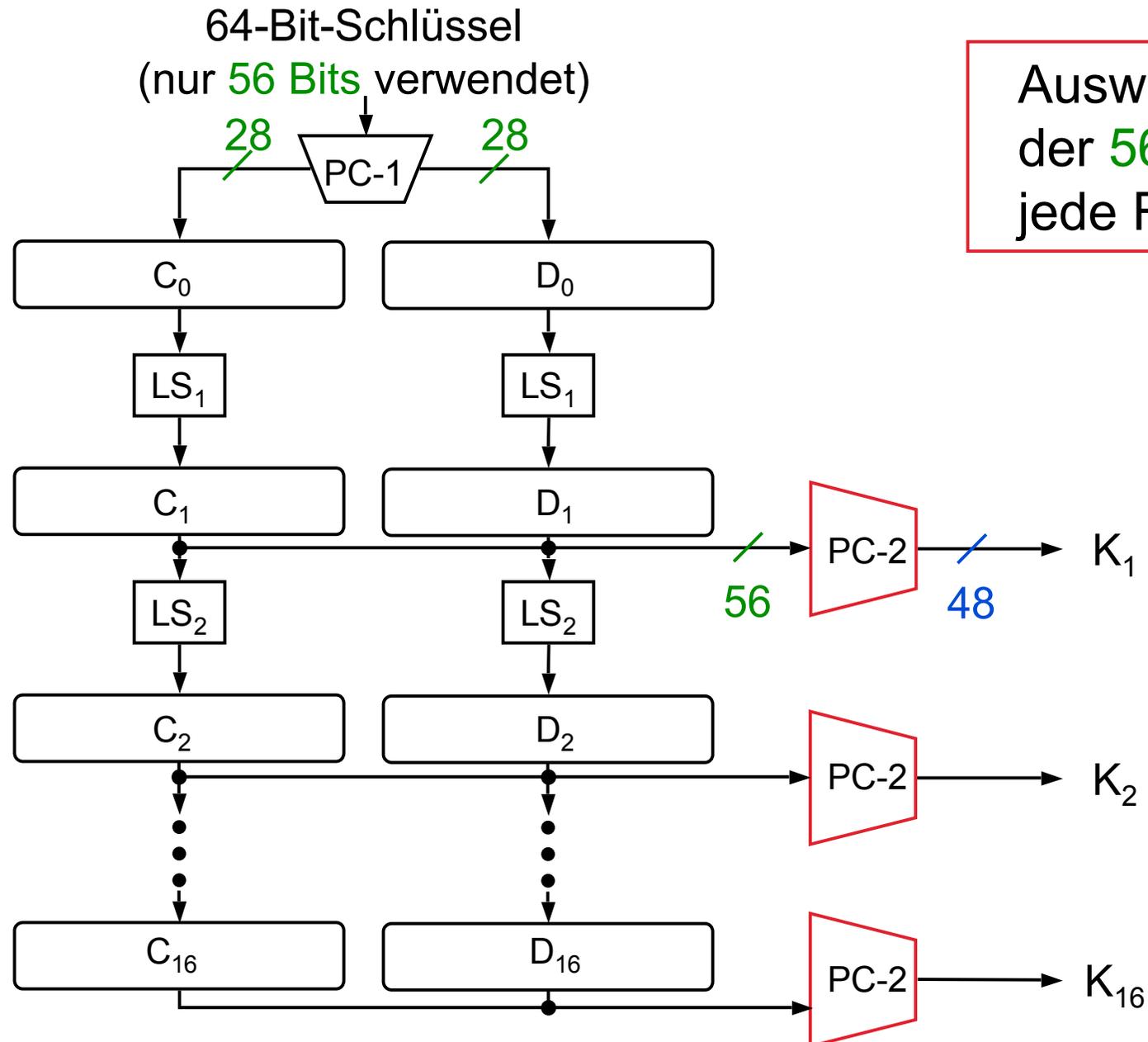
Verschlüsselungsfunktion f



Begriffe

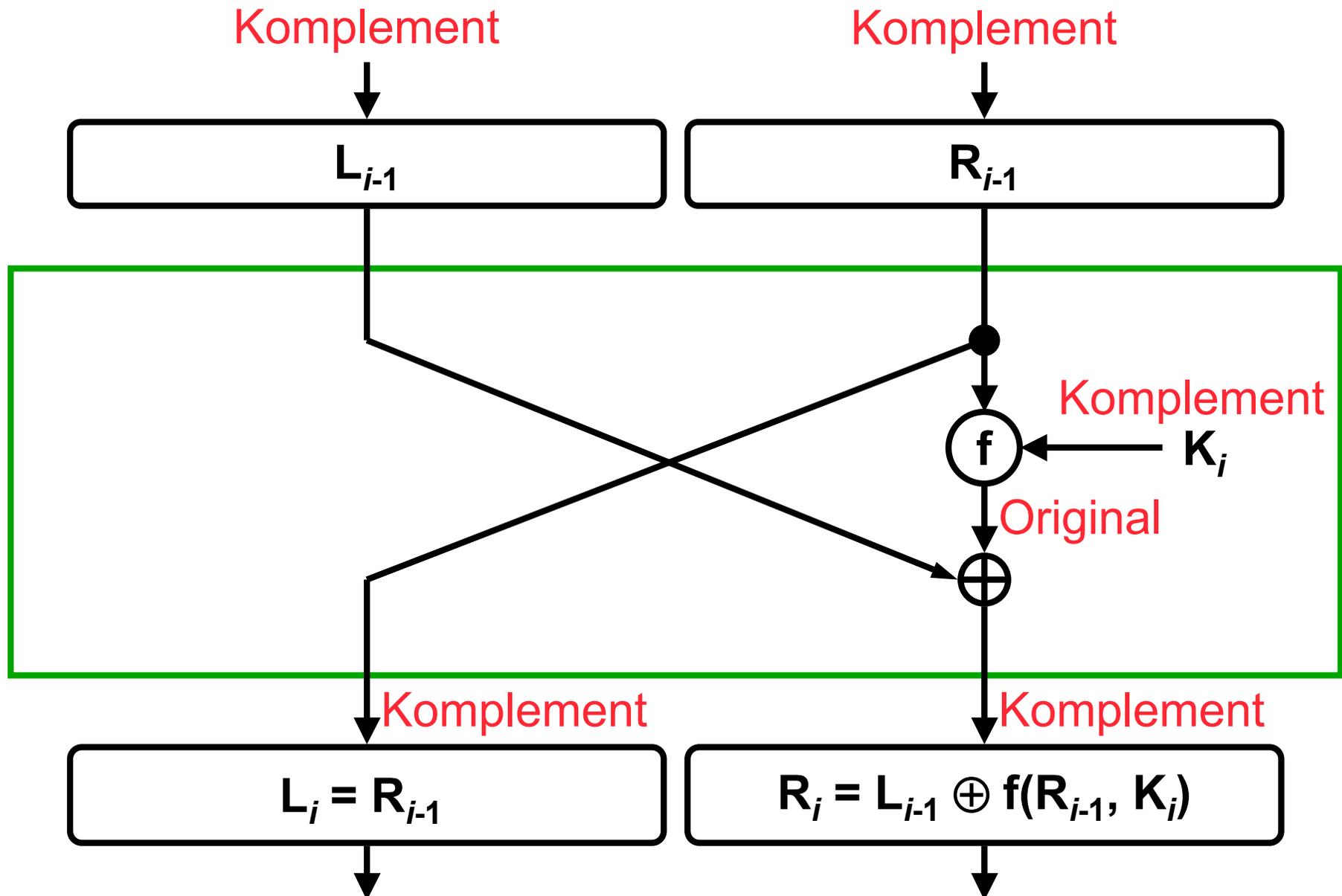
- Substitutions-Permutationsnetze
- Confusion - Diffusion

Teilschlüsselerzeugung

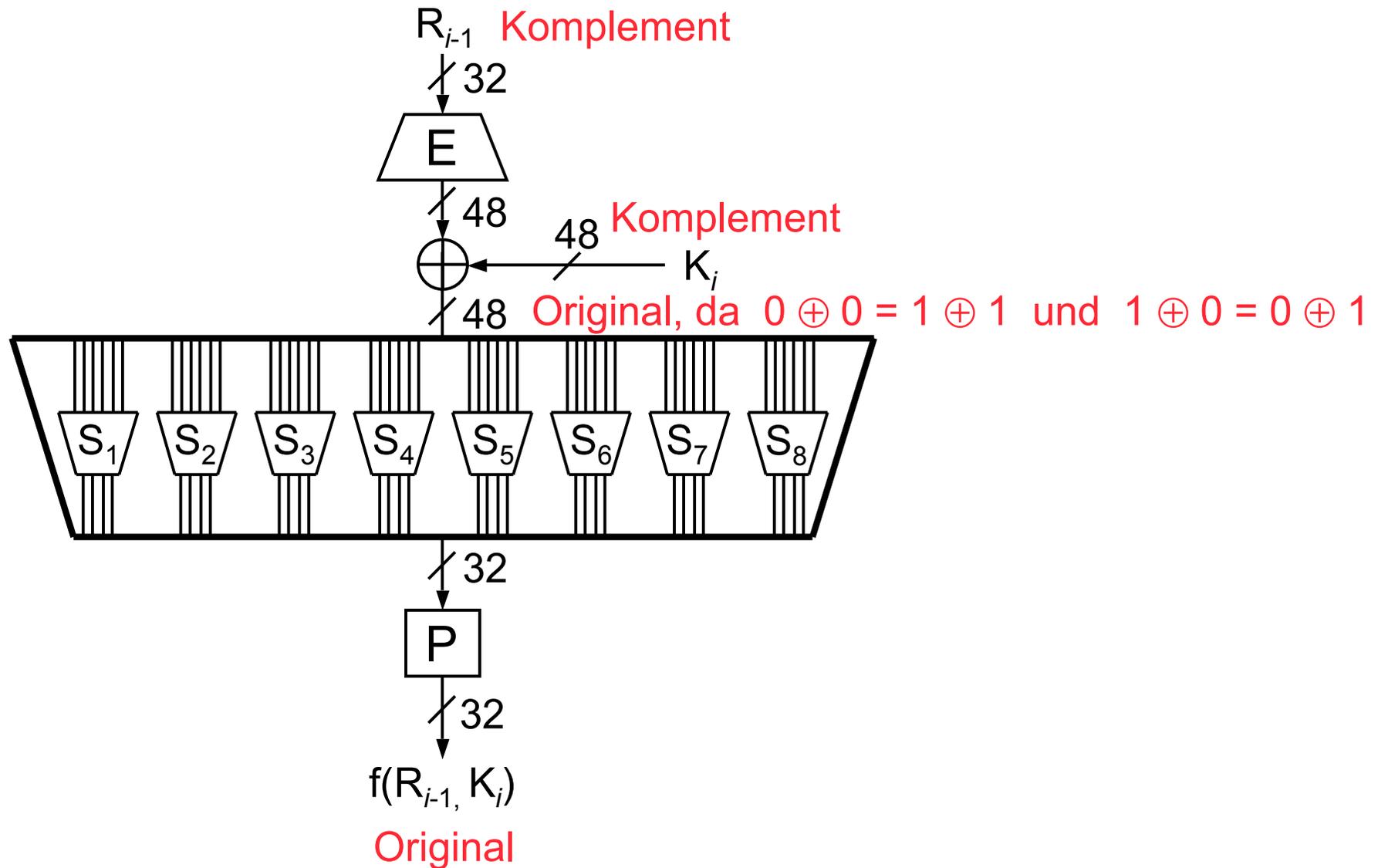


Auswahl von 48
der 56 Bits für
jede Runde

Eine Iterationsrunde



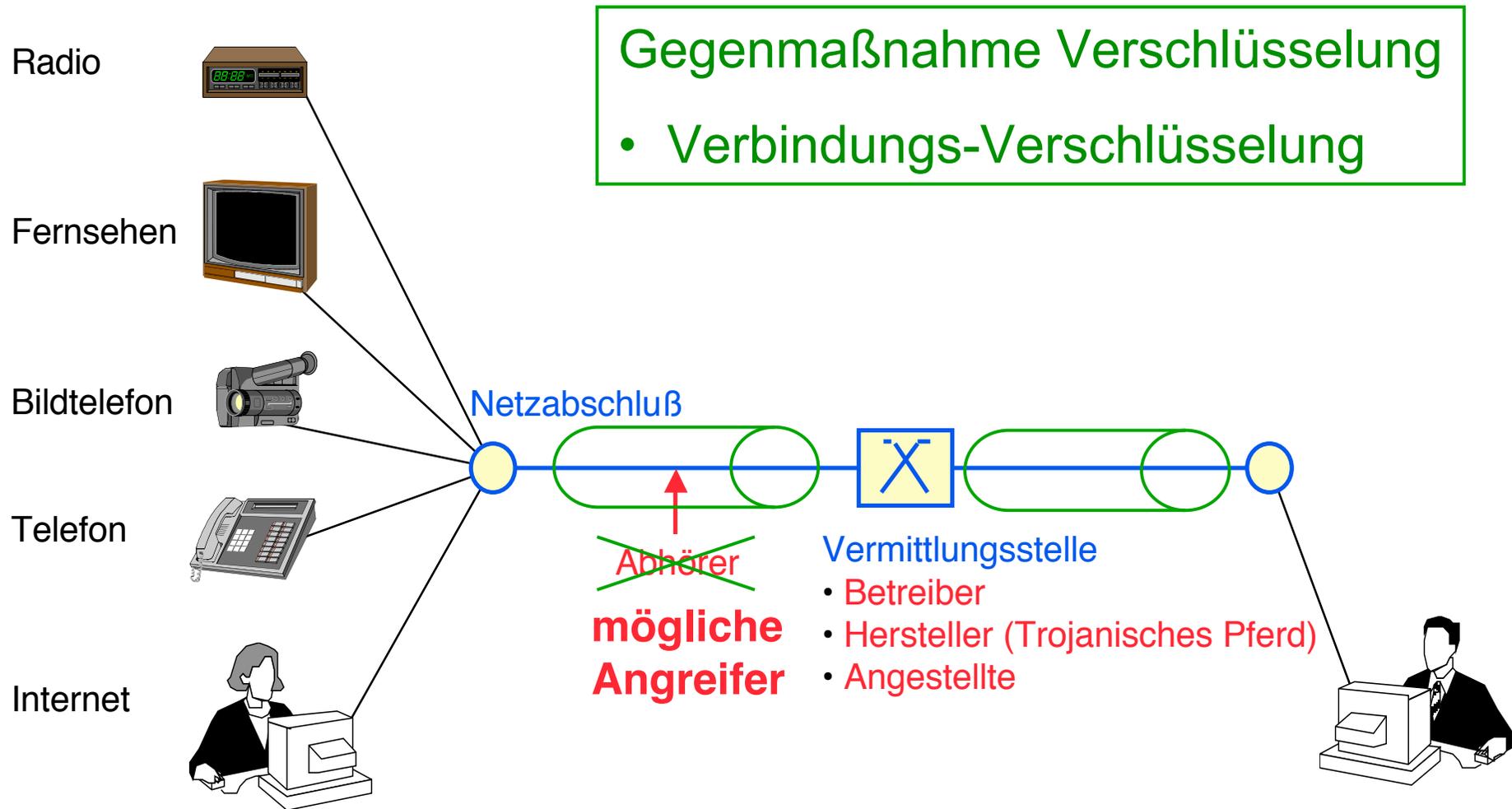
Verschlüsselungsfunktion f



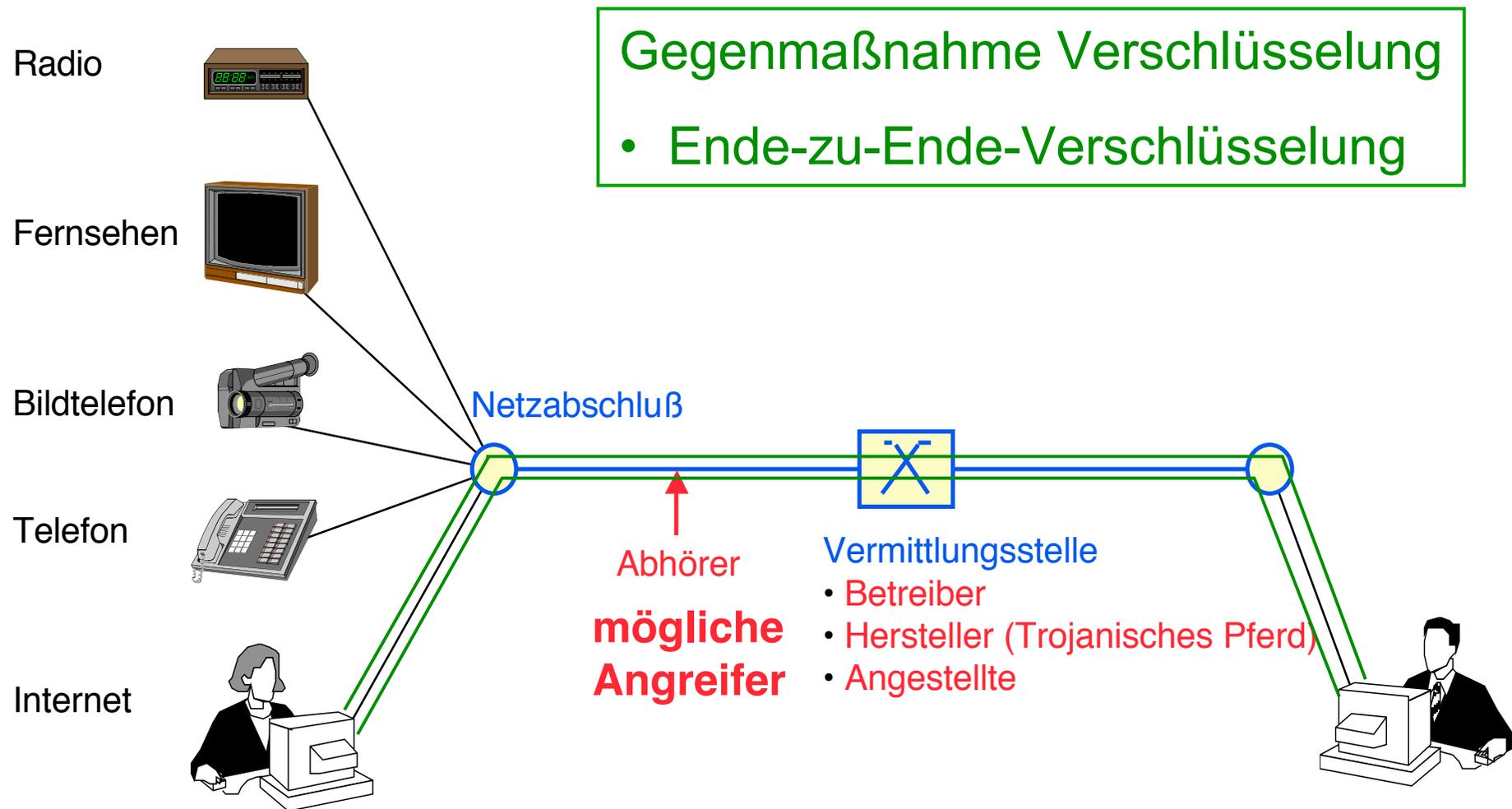
Verallgemeinerung von DES

- 1.) $56 \Rightarrow 16 \cdot 48 = 768$ Schlüsselbits
- 2.) variable Substitutionsboxen
- 3.) variable Permutationen
- 4.) variable Expansionspermutation
- 5.) variable Anzahl Iterationsrunden

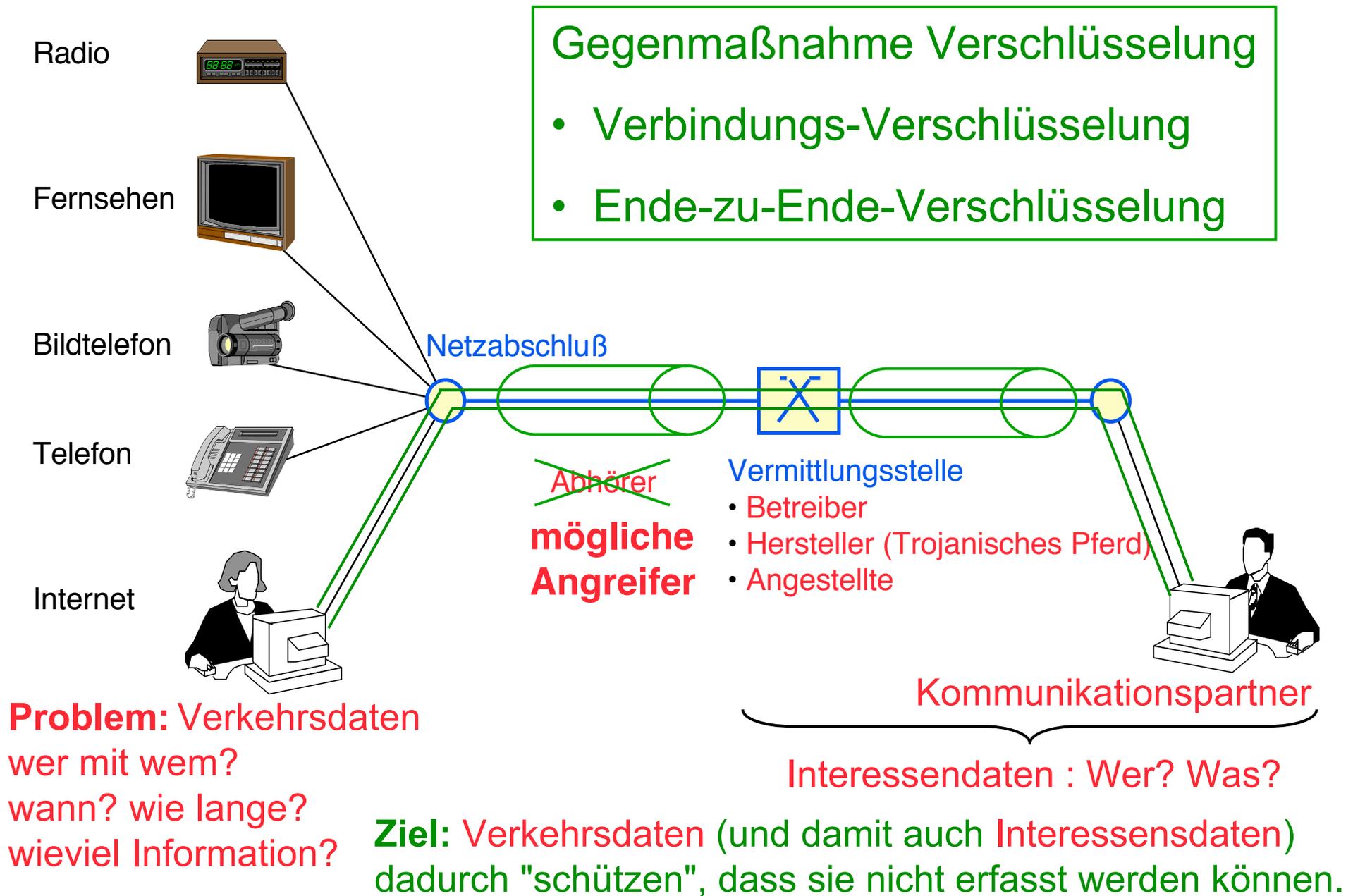
Beobachtbarkeit von Benutzern in Vermittlungsnetzen



Beobachtbarkeit von Benutzern in Vermittlungsnetzen

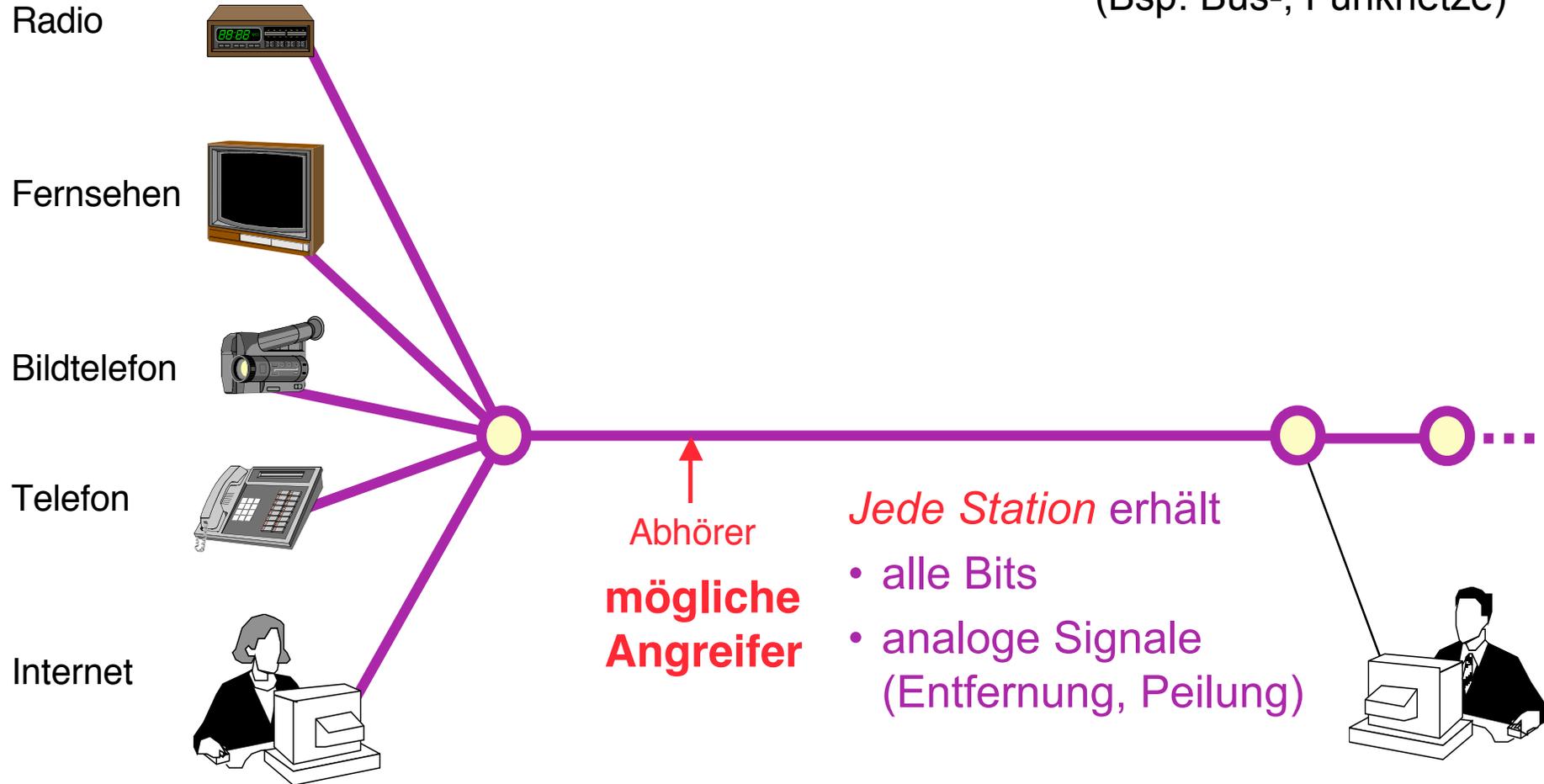


Beobachtbarkeit von Benutzern in Vermittlungsnetzen



Beobachtbarkeit von Benutzern in Broadcastnetzen

(Bsp. Bus-, Funknetze)



Realität oder Science Fiction?

Seit etwa 1990 Realität

Video-8

5 G-Byte

= 3 * Volkszählung 1987

Speicherkosten < 25 EUR

100 Video-8 (oder in 2003: 2 Festplatten mit je 250 G-Byte für je < 280 EUR) speichern

alle Fernsprechverbindungen eines Jahres:

Wer mit wem ?

Wann ?

Wie lange ?

Von wo ?

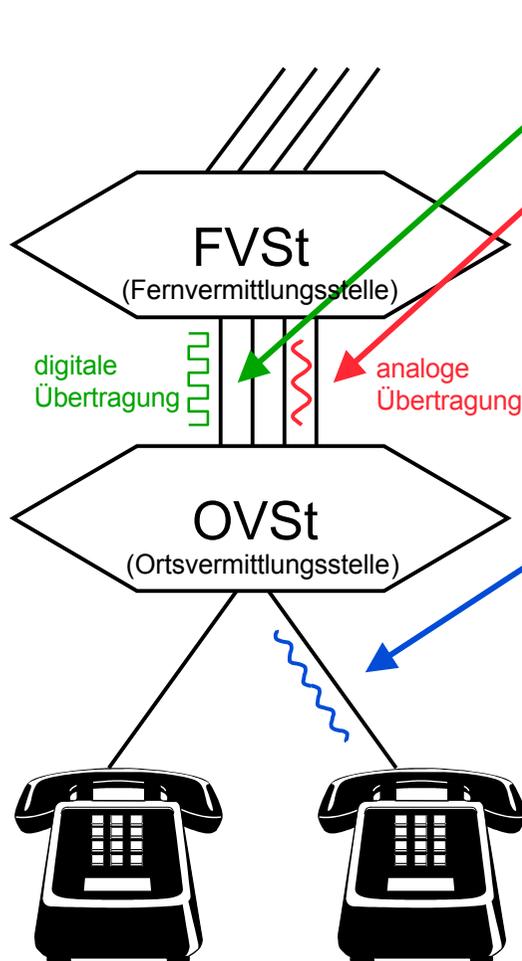
Auszug aus: 1984

With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end.

George Orwell, 1948

Probleme bei Vermittlungsstellen

Durch differenzierte Gestaltung getrennter Vermittlungsstellen ungelöste Probleme:



+ Verschlüsselung

– Nutzdaten

– Verbindungsdaten, falls Sprechererkennung oder \subset Nutzdaten

Trojanisches Pferd v Zusatzgerät: wie unten

Abhören von Teilnehmeranschlussleitungen (Zerhacken der Signale ist aufwendig und ineffektiv, Verschlüsselung der analogen Signale nicht möglich):

– Nutzdaten (Gesprächsinhalte)

– Verbindungsdaten

- Zielrufnummer

- Sprechererkennung oder \subset Nutzdaten

Verfahren zum Schutz der Verkehrsdaten

Schutz außerhalb des Netzes

Öffentliche Anschlüsse

- Benutzung ist umständlich

Zeitlich entkoppelte Verarbeitung

- Kommunikationsformen mit Realzeitanforderungen

Lokale Auswahl

- Übertragungsleistung des Netzes
- Abrechnung von kostenpflichtigen Diensten

Schutz innerhalb des Netzes

Angreifer (-modell)

Fragen:

- wie weit verbreitet ? (Stationen, Leitungen)
- beobachtend / verändernd ?
- wie viel Rechenkapazität ? (informationstheoretisch, komplexitätstheoretisch)

Unbeobachtbarkeit eines Ereignisses E

Für Angreifer gilt für alle Beobachtungen B: $0 < P(E|B) < 1$

perfekt: $P(E) = P(E|B)$

Anonymität einer Instanz

Unverkettbarkeit von Ereignissen

gegebenenfalls **Klasseneinteilung**