
Informatik im Kontext:

# Technischer Datenschutz und mehrseitige IT-Sicherheit

Prof. Dr. Hannes Federrath

http://svs.informatik.uni-hamburg.de/

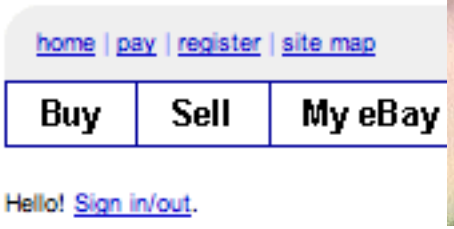
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

## Neue Technik

- wird nicht nur zu legalen Zwecken eingesetzt, sondern kann auch von Kriminellen genutzt werden; Beispiele:
  - Verabredung von Straftaten, Terrorakten
  - Betrug (Kreditkarten-, Produktbetrug)
  - Verbreitung illegaler Inhalte (Kinderpornographie, Raubkopien)
  - ist selbst Ziel krimineller Handlungen (Viren, Würmer, trojanische Pferde)

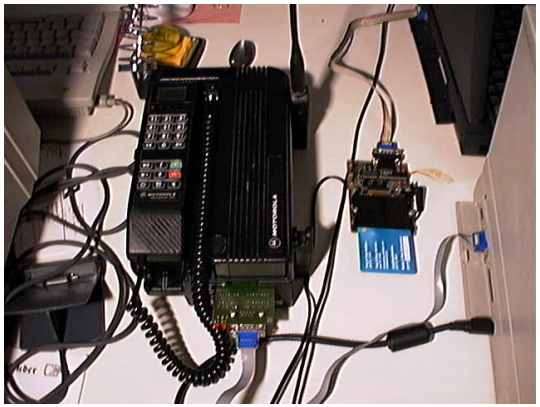
- führt zunächst zu einer Ohnmachtserfahrung des Staates
  - „Das Internet ist kein rechtsfreier Raum."
  - Forderung nach besseren Überwachungsmöglichkeiten des Staates



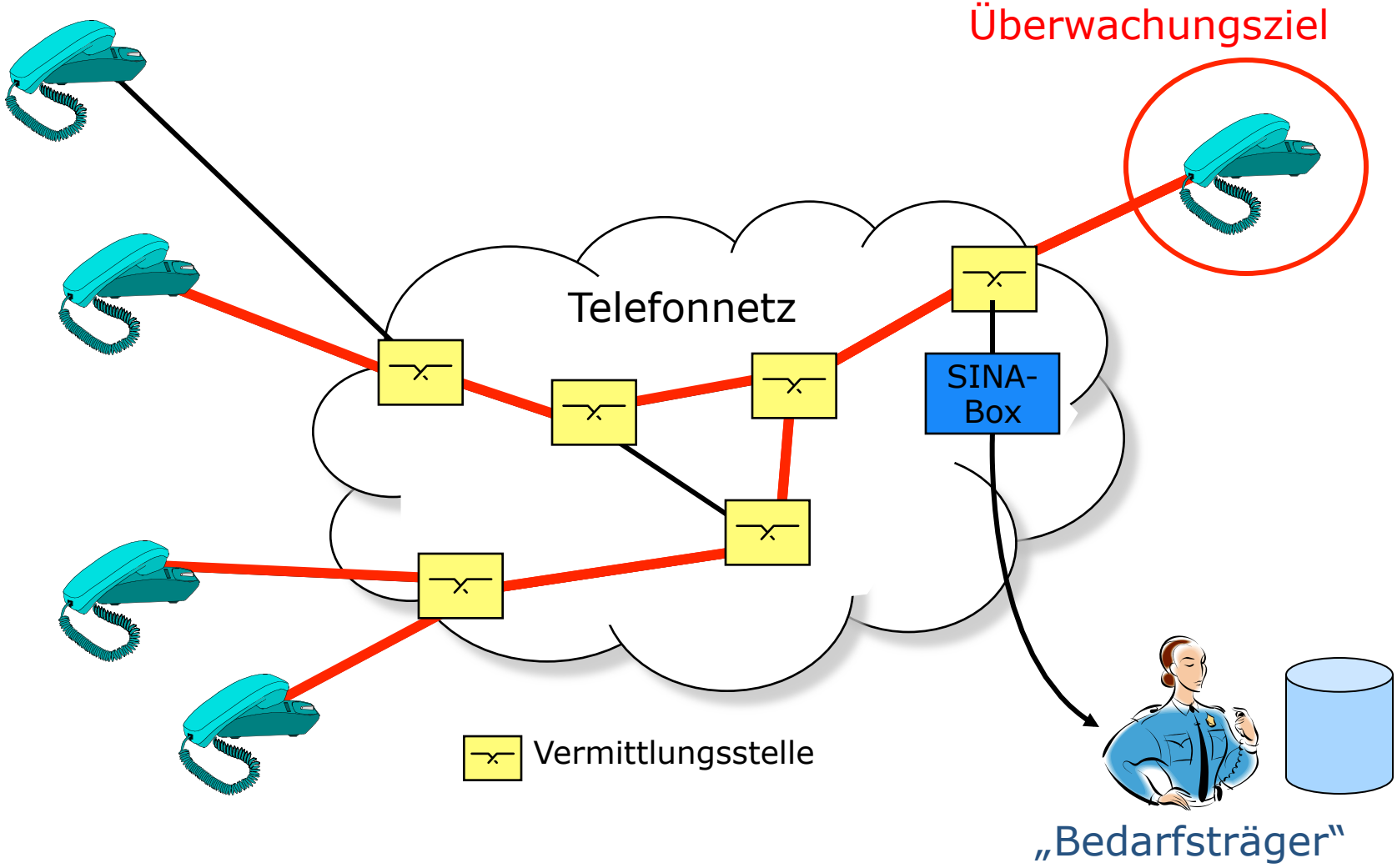



## Neue Technik

- 3 Beispiele zur Motivation
  - Telefonüberwachung
  - Mautsystem
  - Fingerabdrücke in Reisepässen



# Telefonüberwachung



# Telefonüberwachung: Reale Zahlen

Quelle: ct, Heft 10, 2006, S.60

- Deutschland im Jahr 2002:
  - Studie Uni Bielefeld:
    - 21974 Anordnungen
    - mehr als 20 Millionen abgehörte Telefongespräche
    - ca. 1,5 Millionen betroffene Bundesbürger
  - Kriminologisches Institut der Uni Münster:
    - Hochrechnung für 2002:
      knapp 4 Millionen betroffene Bundesbürger
- USA im Jahr 2005:
  - Verwaltungsbüro der US-Gerichtshöfe
    - 1773 Anordnungen von Bundes- und Staatengerichten
      + 625 Anordnungen von Bundesbehörden
    - je Anordnung durchschnittlich betroffene US-Bürger: 107

22.000 ÜA · 100 Betroffene = 2.200.000 Betroffene

80 Mio. Bundesbürger / 2,2 Mio. Betroffene ≈ 40, d.h. jeder 40. Bürger ist betroffen

## Telefonüberwachung

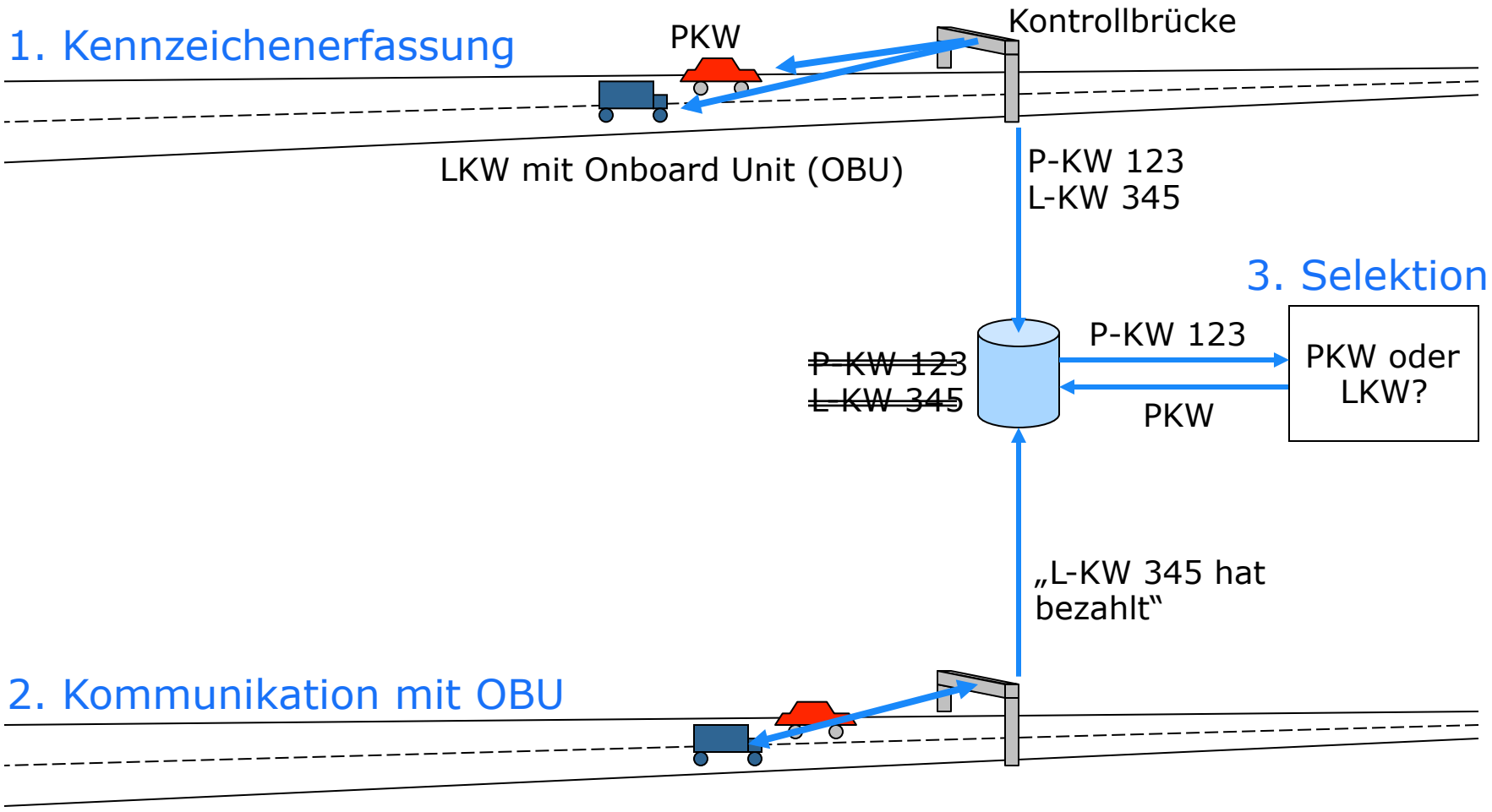
- Gesetzliche Grundlagen:
  - GG Art. 10 (Fernmeldegeheimnis)
  - G-10 Gesetz (Ermächtigung für Nachrichtendienste)
  - § 100 a, b StPO (besonders schwere Straftaten)
- Katalogstraftaten (§ 100 a StPO)
  - Hochverrat
  - Gefährdung des demokratischen Rechtsstaates
  - Geld- oder Wertpapierfälschung
  - schweren Menschenhandel
  - Mord
  - Bandendiebstahl
  - Raub
  - Erpressung
  - Geldwäsche
  - …

- Gutachten der Max-Planck-Instituts für ausländ. und int. Strafrecht:
  - nur ein Bruchteil der Betroffenen wird im Nachhinein informiert
  - Richtervorbehalt läuft ins Leere

# Deutsches Mautsystem


- dient der Erhebung von LKW-Straßenbenutzungsgebühren
- Kennzeichen aller durchfahrenden Fahrzeuge werden vorsorglich erfasst
  - PKW und LKW
- Fahrzeuge mit Onboard Unit tauschen Daten mit Kontrollbrücke aus
  - Prepaid System: Alle bezahlten Fahrzeuge werden sofort wieder aus Datenbank gelöscht

# Deutsches Mautsystem



## Deutsches Mautsystem

- Alle Fahrzeuge werden erfasst (PKW und LKW).
- Gesetzlich verankerte Zweckbindung der Datenerhebung:
  - nur zur Erhebung von Autobahnmaut (LKW)
- Generalbundesanwalt (a.D.) Nehm:
  - Daten sollen auch für Strafverfolgung zur Verfügung stehen (44. Deutscher Verkehrsgerichtstag, Januar 2006)
- Technisch problemlos möglich wären heute schon:
  - Automatische Geschwindigkeitskontrollen
  - Flächendeckende Bewegungsprofile
  - Einführung einer PKW-Maut
- Tollcollect hat für die technische Realisierung dieses perfekten Überwachungssystems den Big Brother Award 2002 erhalten.

# Biometrische Reisepässe

- Seit Herbst 2005 zur Verbesserung der inneren Sicherheit eingeführt

- Neue Funktionen:
  - Speicherung eines Fotos und zukünftig zusätzlich eines Fingerabdrucks des Passinhabers auf einem Chip
  - Kontaktloses Auslesen der biometrischen Merkmale aus dem Chip
- Probleme:
  - Biometrische Merkmale
    - erhöhen nicht die Zuverlässigkeit der Identifikation
    - geben möglicherweise Auskunft über weitere Eigenschaften der Person
  - Kontaktlose Chips
    - lassen sich unter bestimmten Umständen leicht von Jedermann auslesen

# Fälschen eines Fingerabdrucks

- Vom Chaos Computer Club im Jahre 2005 praktisch demonstriert.

- Fingerabdruck sichtbar machen
- fotografieren
- nachbearbeiten
- ausdrucken
- Leim drauf
- warten
- abziehen

- Von uns im Rahmen einer Fernsehsendung praktisch nachvollzogen
- Ergebnis: Es funktioniert wirklich (nicht).

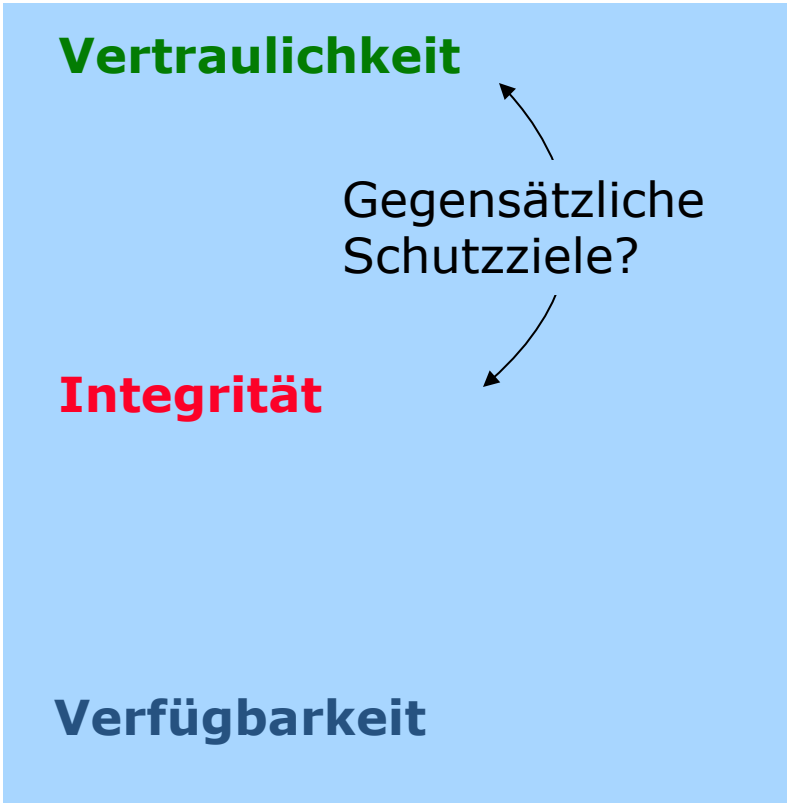
# Schutzziele (Voydock, Kent 1983)

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

| | |
|---|---|
| **Vertraulichkeit** | unbefugter Informationsgewinn |
| **Integrität** | unbefugte Modifikation |
| **Verfügbarkeit** | unbefugte Beeinträchtigung der Funktionalität |

# Mehrseitige Sicherheit (Müller et. al. 1997)

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.




- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

# Was ist zu schützen?

| Kommunikationsgegenstand WAS? | | Kommunikationsumstände WANN?, WO?, WER? |
|---|---|---|
| **Vertraulichkeit**<br>**Verdecktheit** | Inhalte | **Anonymität**<br>**Unbeobachtbarkeit**<br>Sender, Ort, Empfänger |
| **Integrität** | Inhalte | **Zurechenbarkeit**<br>**Rechtsverbindlichkeit**<br>Absender, Bezahlung, Empfänger |
| **Verfügbarkeit** | Inhalte | **Erreichbarkeit**<br>Nutzer, Rechner |

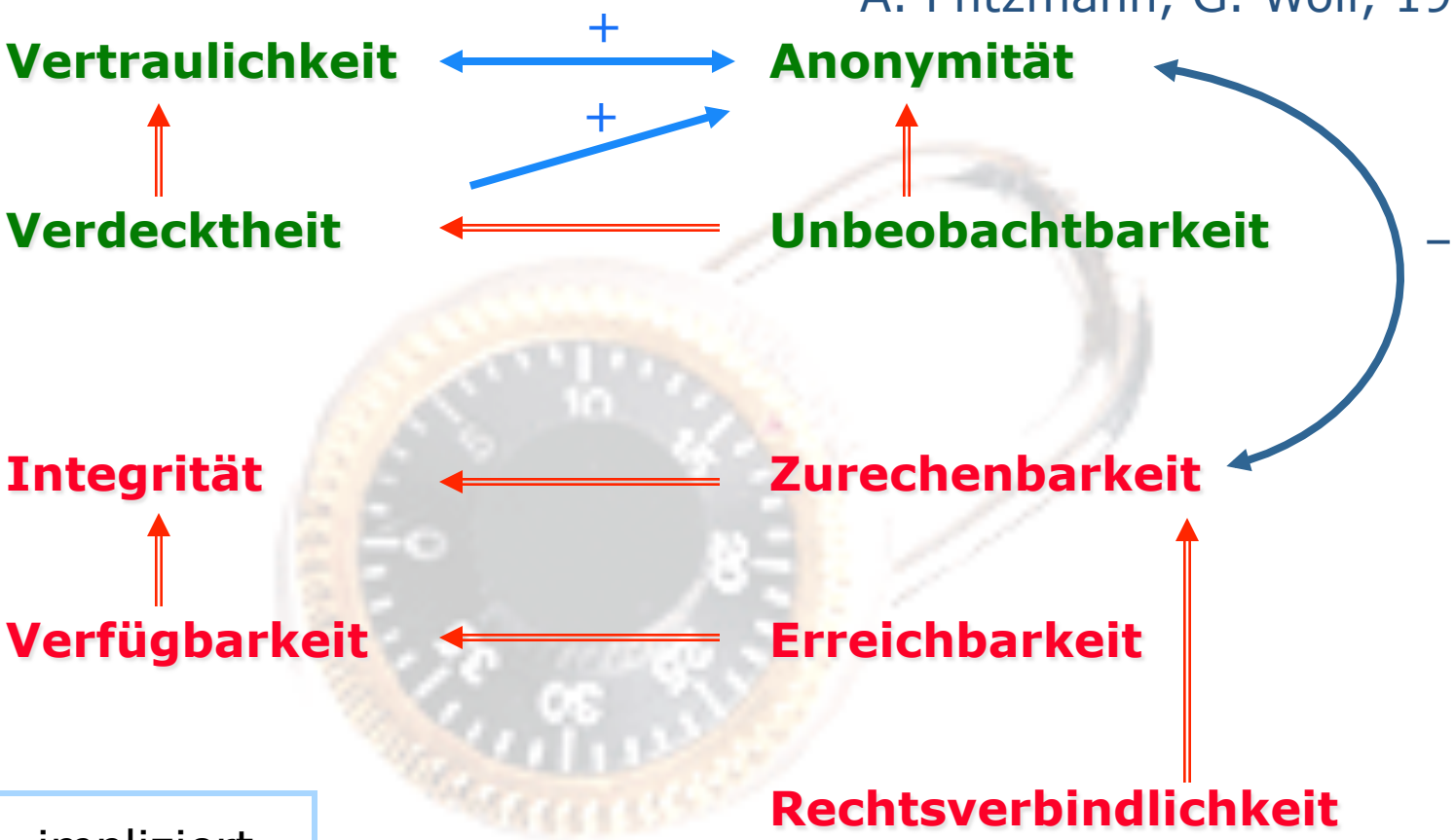
# Datenschutz

| Kommunikationsgegenstand WAS? | | Kommunikationsumstände WANN?, WO?, WER? |
|---|---|---|
| **Vertraulichkeit**<br>**Verdecktheit** | Inhalte | **Anonymität**<br>**Unbeobachtbarkeit**<br>Sender<br>Ort<br>Empfänger |
| **Integrität** | Inhalte | **Zurechenbarkeit**<br>**Rechtsverbindlichkeit**<br>Absender<br>Bezahlung |

**Schutz personenbezogener Daten:**
Verkehrsdaten
Interessensdaten

# Wechselwirkungen zwischen Schutzzielen

A. Pfitzmann, G. Wolf, 1999




impliziert

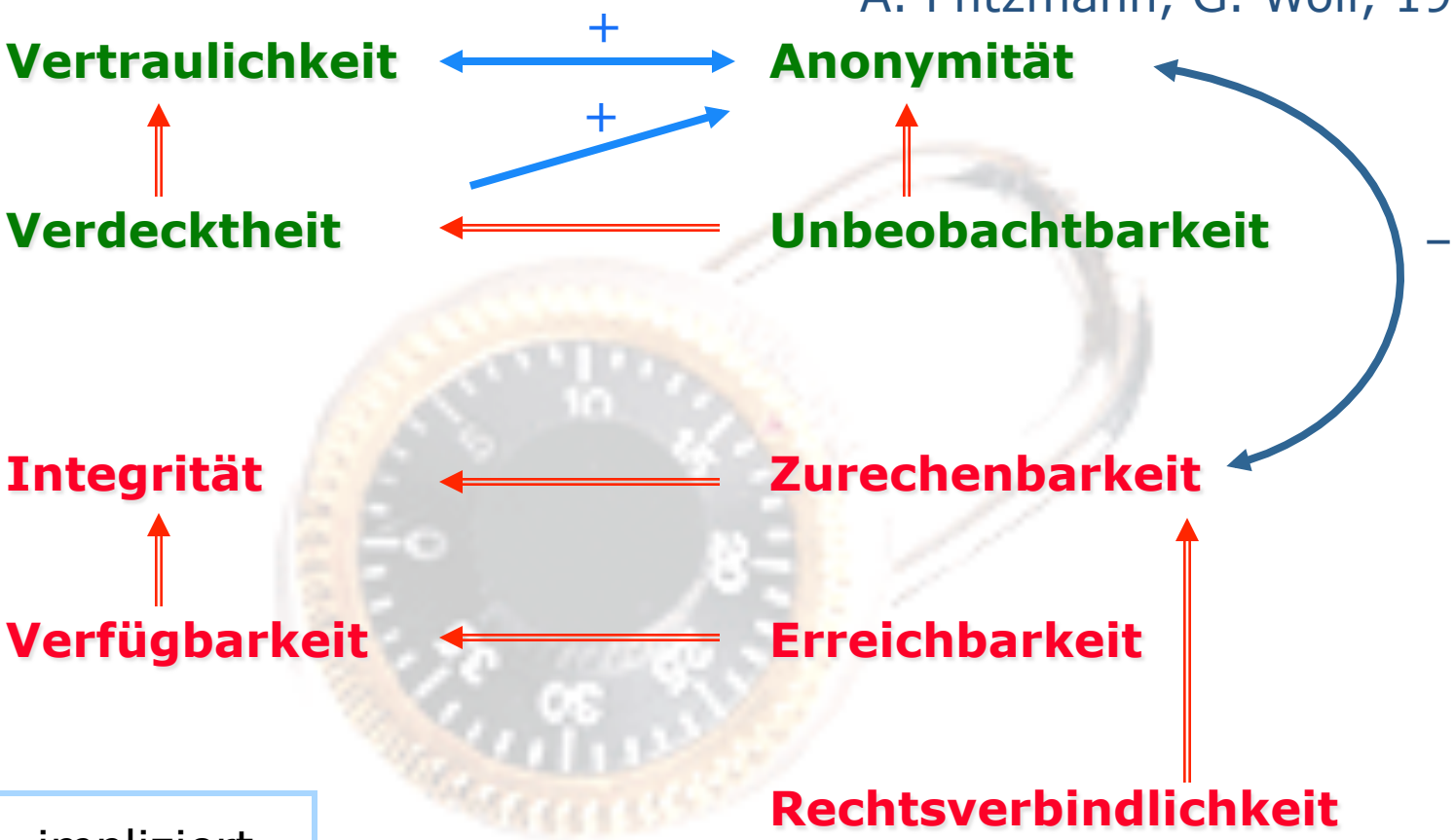
\+ verstärkt

– schwächt

Beobachtungen zum Monotonieverhalten:
Vertraulichkeitseigenschaften können nur geringer werden.
Integrität und Zurechenbarkeit können nur größer werden.

# Wechselwirkungen zwischen Schutzzielen

A. Pfitzmann, G. Wolf, 1999




impliziert

\+ verstärkt

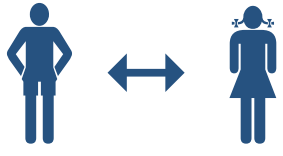
– schwächt

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

# Techniken für Mehrseitige Sicherheit

- Unilateral nutzbar
  - jede(r) kann allein entscheiden

- Bilateral nutzbar
  - nur wenn der Kommunikationspartner kooperiert



- Trilateral nutzbar
  - nur wenn zusätzlich ein vertrauenswürdiger Dritter kooperiert

- Multilateral nutzbar
  - nur wenn viele Partner kooperieren

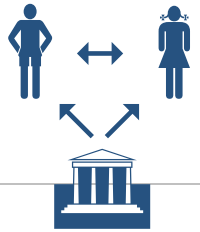
Techniken für Mehrseitige Sicherheit haben das Potential, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un)-Sicherheit zu befreien.

# Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Selbstschutz-Beispiele
  - Verschlüsselung mit PGP, GnuPG
  - Filter: Webwasher, JunkBuster, CookieCooker
  - Personal Firewalls
  - Offene Betriebssysteme: Linux, BSD

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Sichere Dienste anstelle ihrer unsicheren Vorläufer: telnet → ssh, ftp → scp, http → https

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

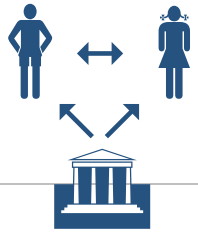
  - Anonymisierer: JAP, TOR

# Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Stand der Forschung?
  - Kryptographie: sehr gut
  - Betriebssysteme theoret.: sehr gut
  - Betriebssysteme praktisch: schlecht

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Kryptographie: sehr gut
  - Steganographie: gut

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

  - PKI: sehr gut

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

# Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf



  - **Kryptographie**: sehr gut
  - **Betriebssysteme** theoret.: sehr gut
  - Betriebssysteme praktisch: schlecht

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Kryptographie: sehr gut
  - **Steganographie**: gut

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

  - PKI: sehr gut

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen



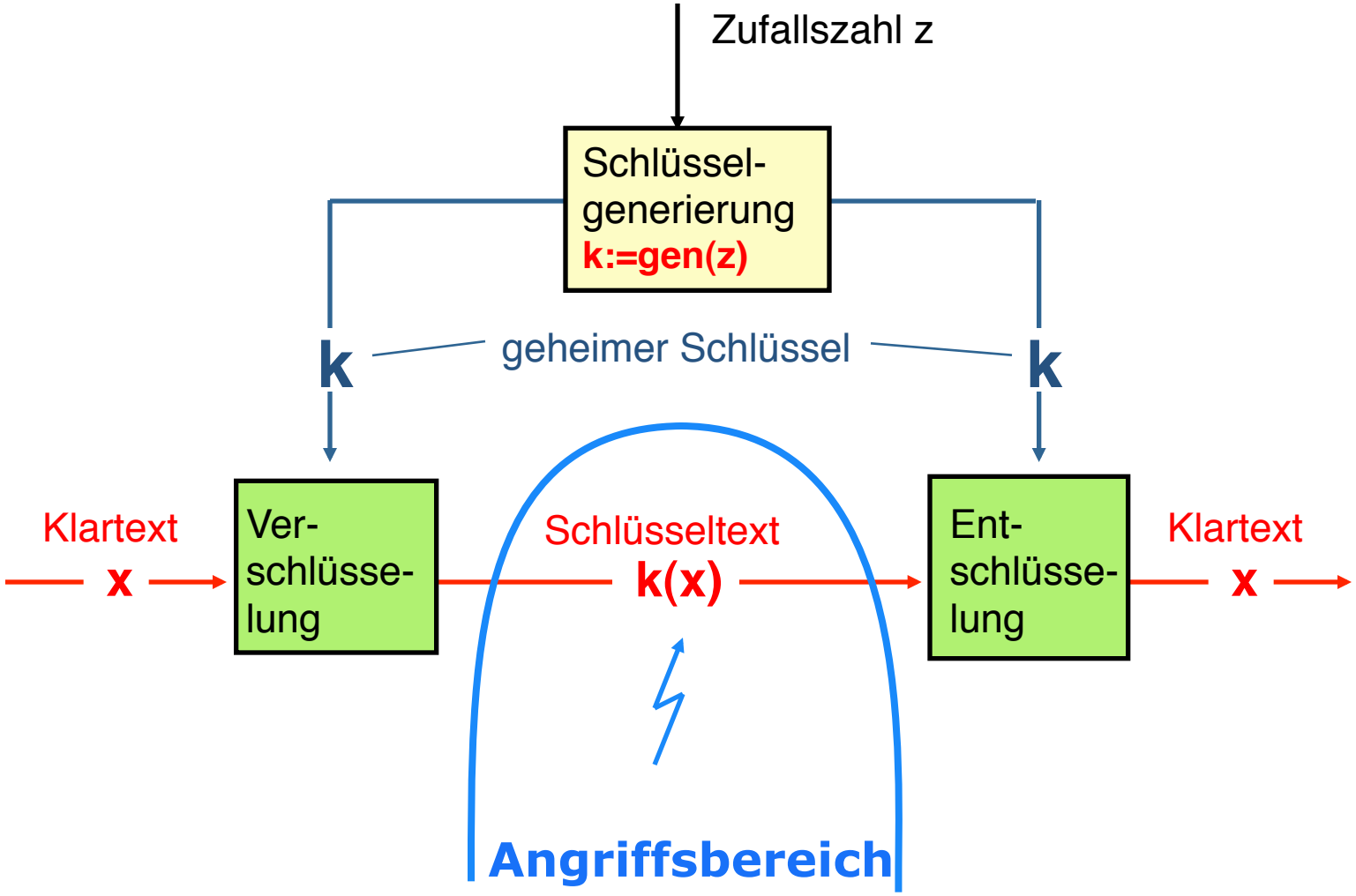
  - **Anonymität** theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

- Symmetrisches Konzelationssystem
- Asymmetrisches Konzelationssystem

- Symmetrisches Authentikationssystem
- Asymmetrisches Authentikationssystem
  = Digitales Signatursystem

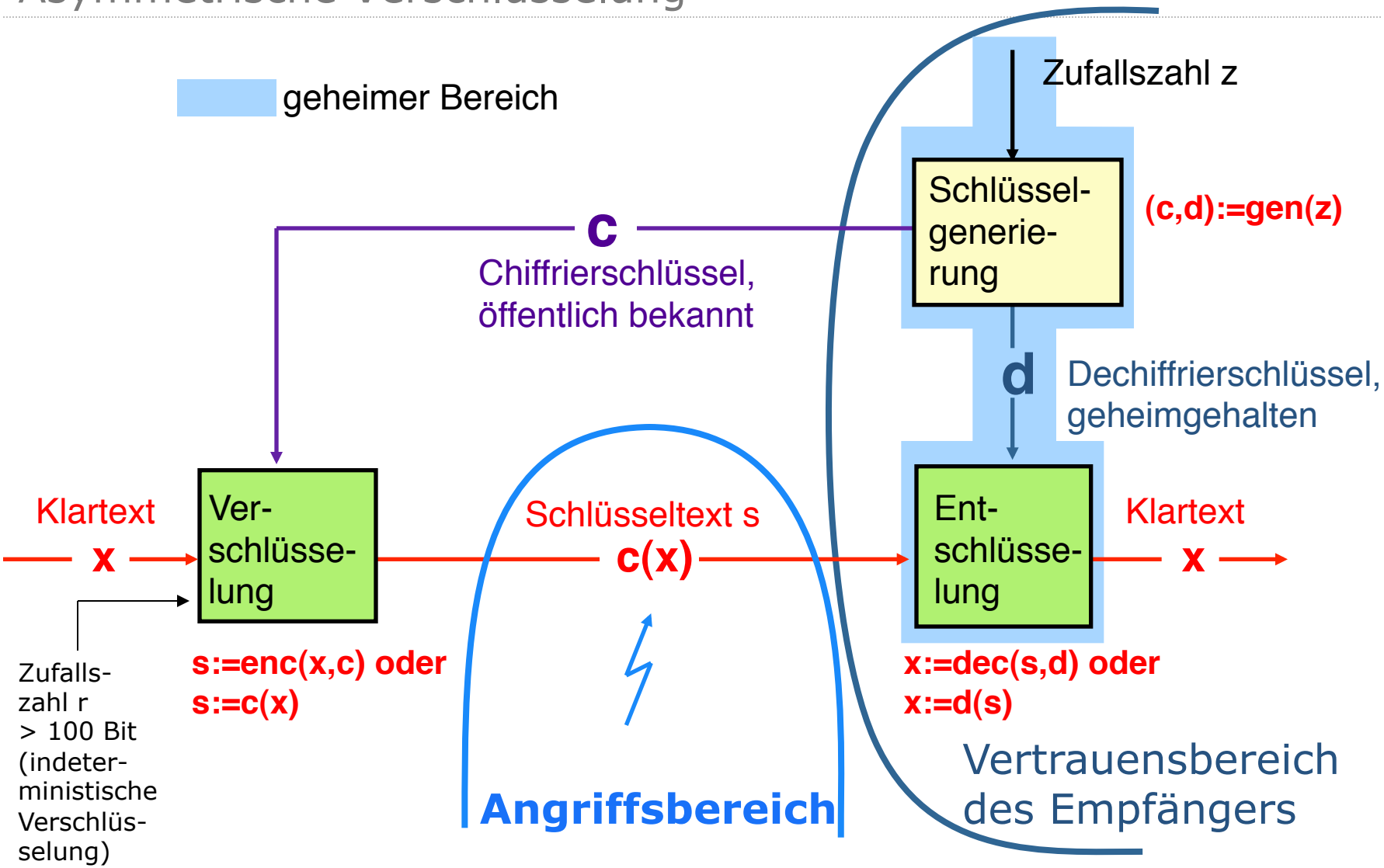
- (Symmetrische) Steganographie

# Symmetrische Verschlüsselung




Undurchsichtiger Kasten mit Schloss. Es gibt zwei gleiche Schlüssel.

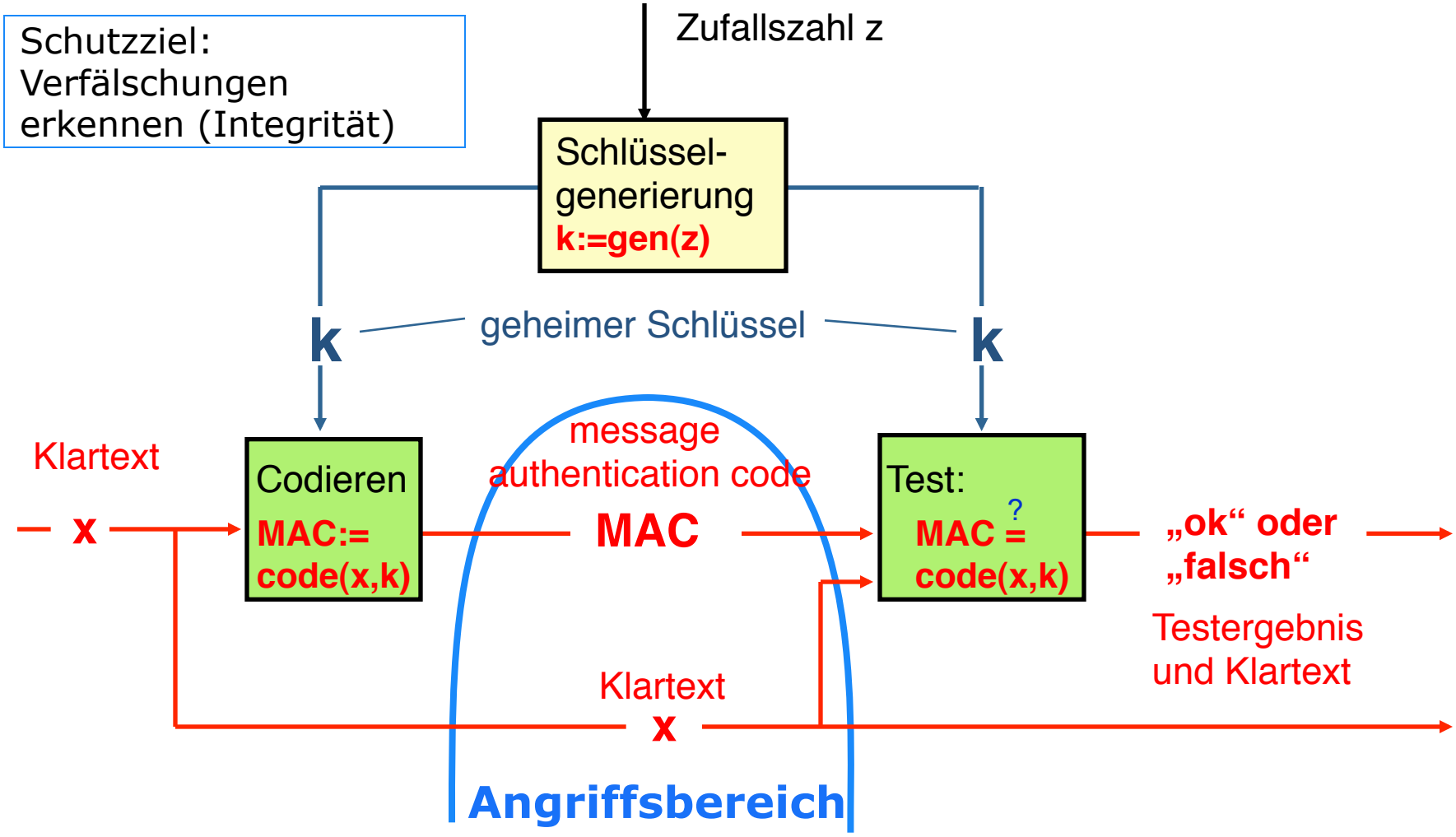
# Asymmetrische Verschlüsselung




Kasten mit Schnappschloss. Es gibt nur einen Schlüssel.

# Symmetrische Authentikation

Schutzziel:
Verfälschungen erkennen (Integrität)

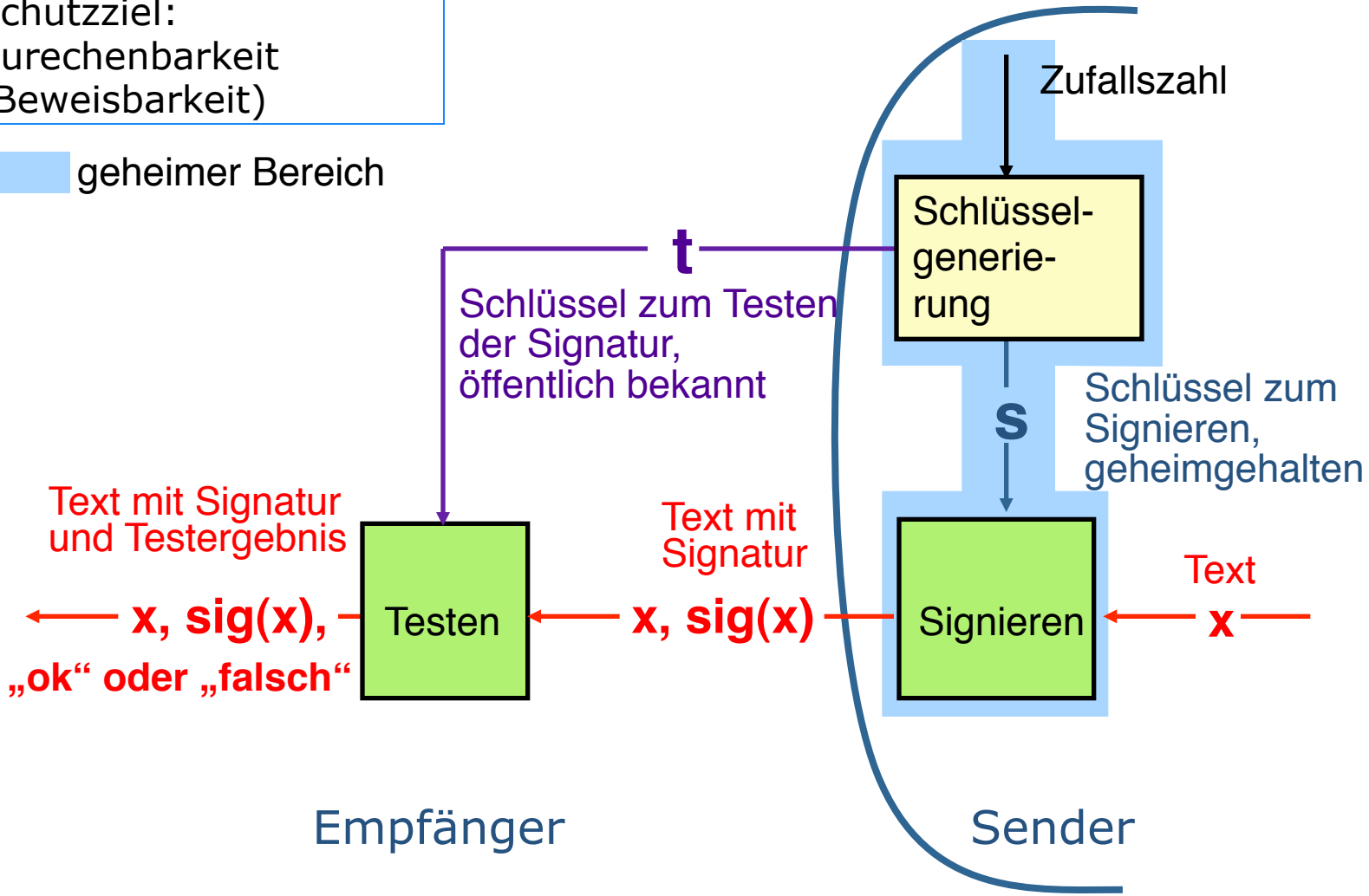



Glasvitrine mit Schloss. Es gibt zwei gleiche Schlüssel.

# Digitales Signatursystem

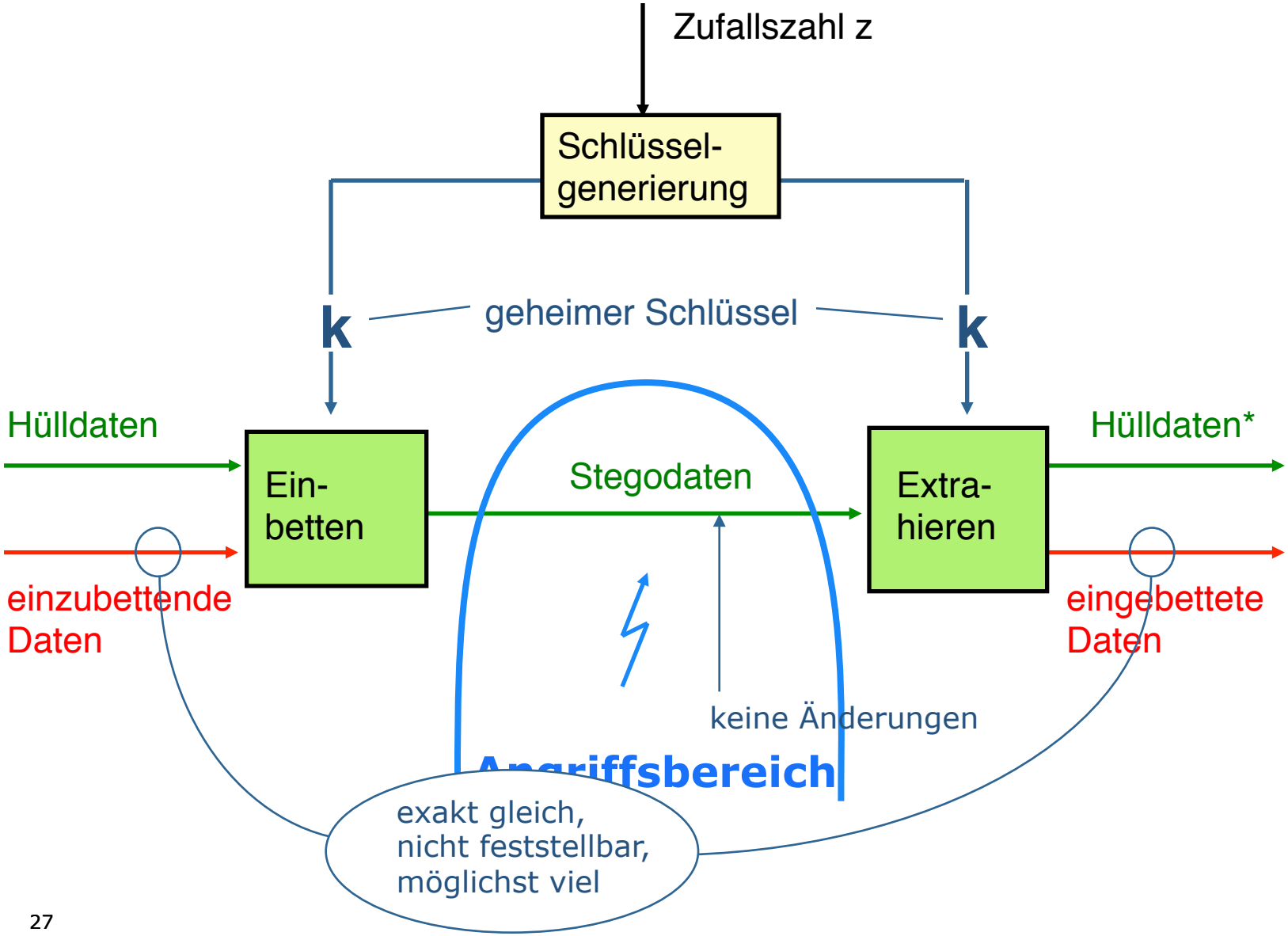
Schutzziel:
Zurechenbarkeit
(Beweisbarkeit)

geheimer Bereich

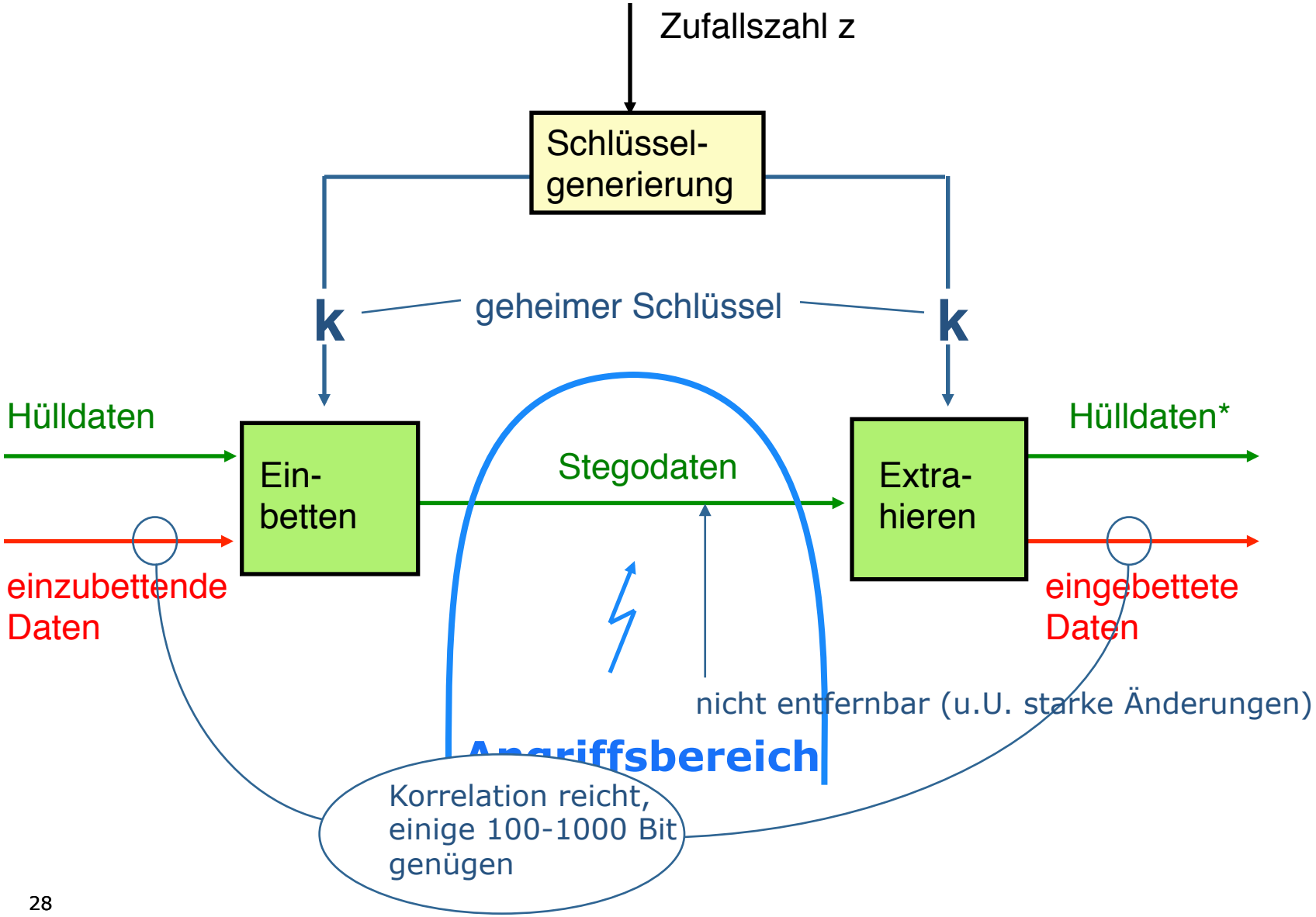



Glasvitrine mit Schloss. Es gibt nur einen Schlüssel.

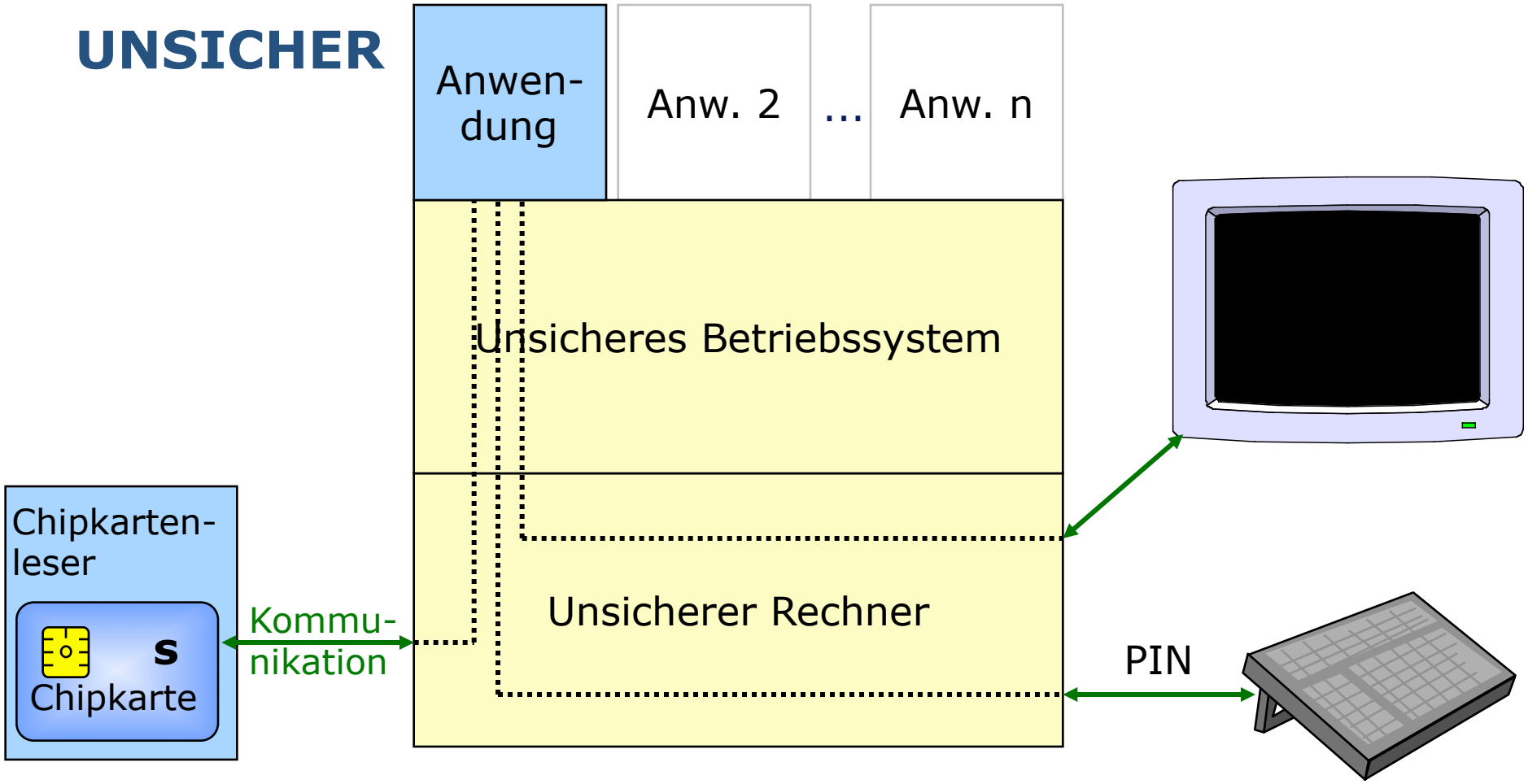
# Aufbau eines Stegosystems



# Watermarking

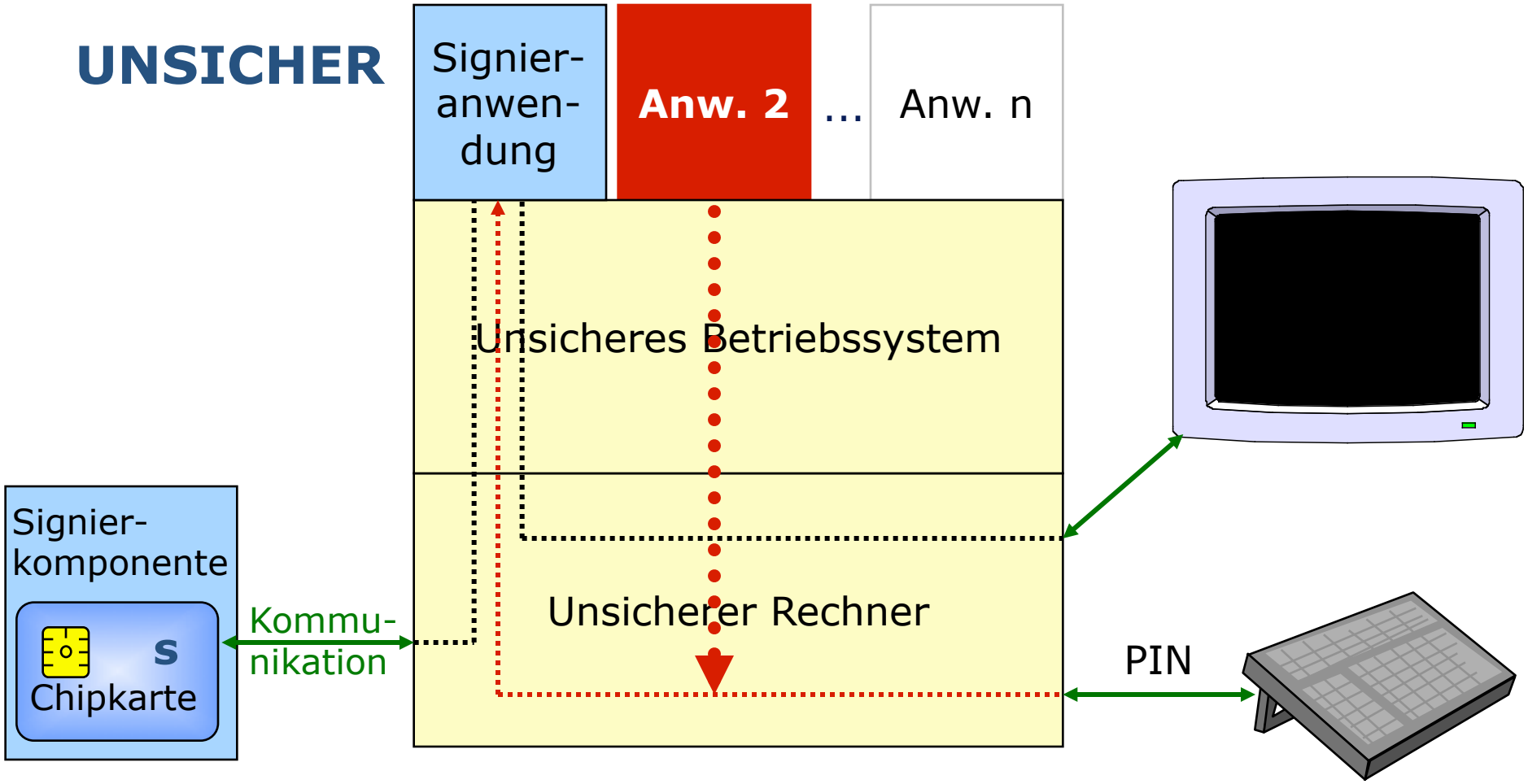


- Sichere Geräte sind eine Voraussetzung für sichere Systeme



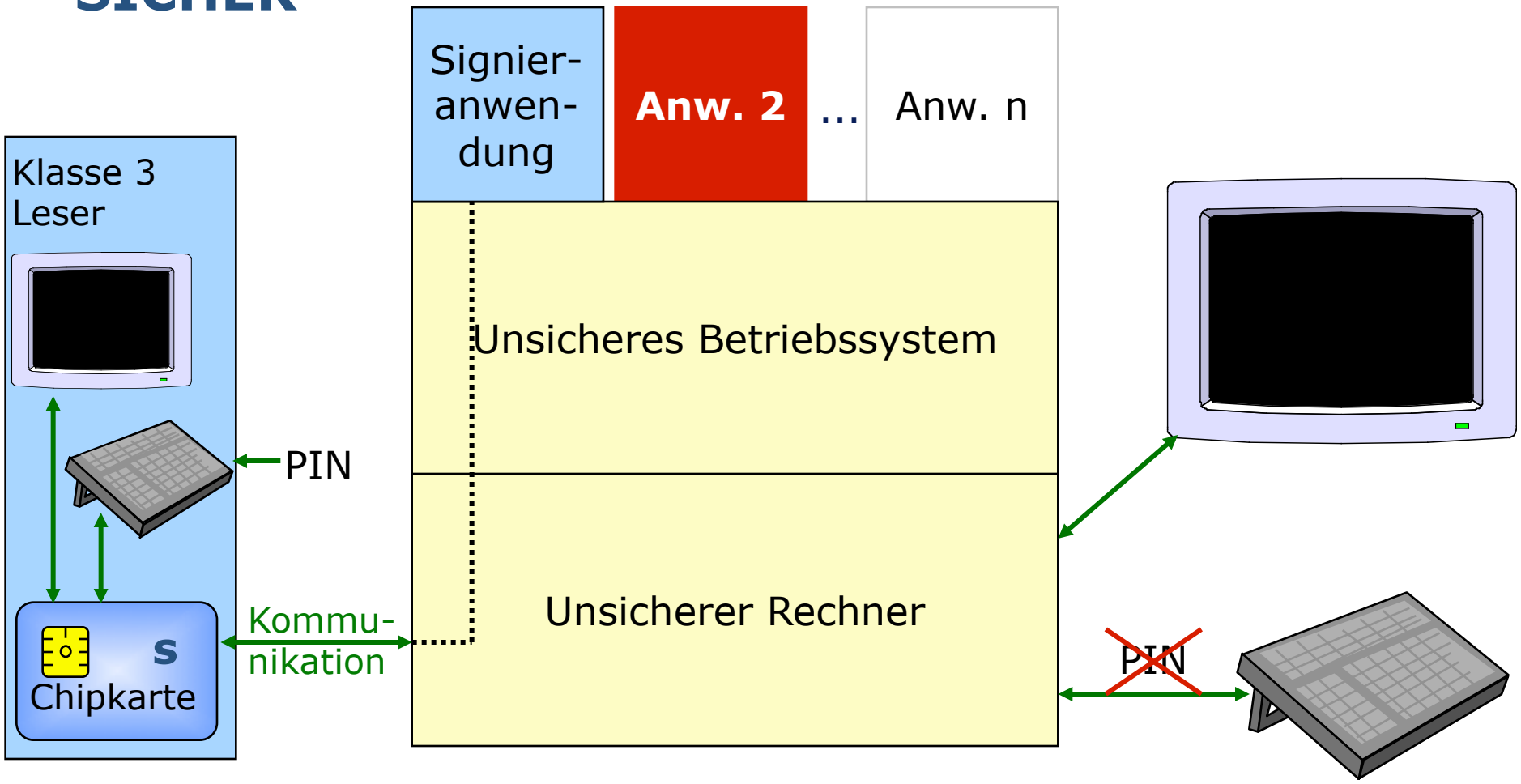
# Standard-PC mit Chipkarte

**Bösartige Anwendung könnte z.B. PIN abfangen oder unverschlüsselten Text mitlesen**

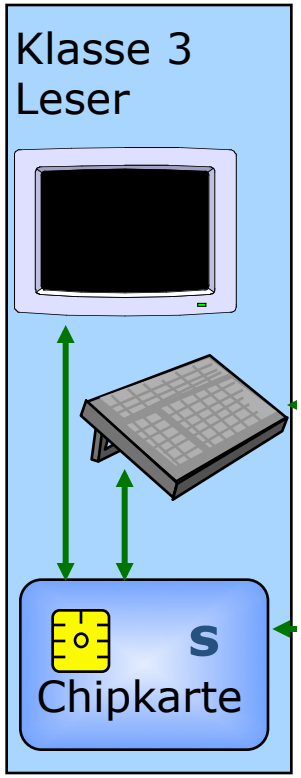


# Sichere Hardware mit Standard-PC

**SICHER**



# Sichere Hardware mit Standard-PC



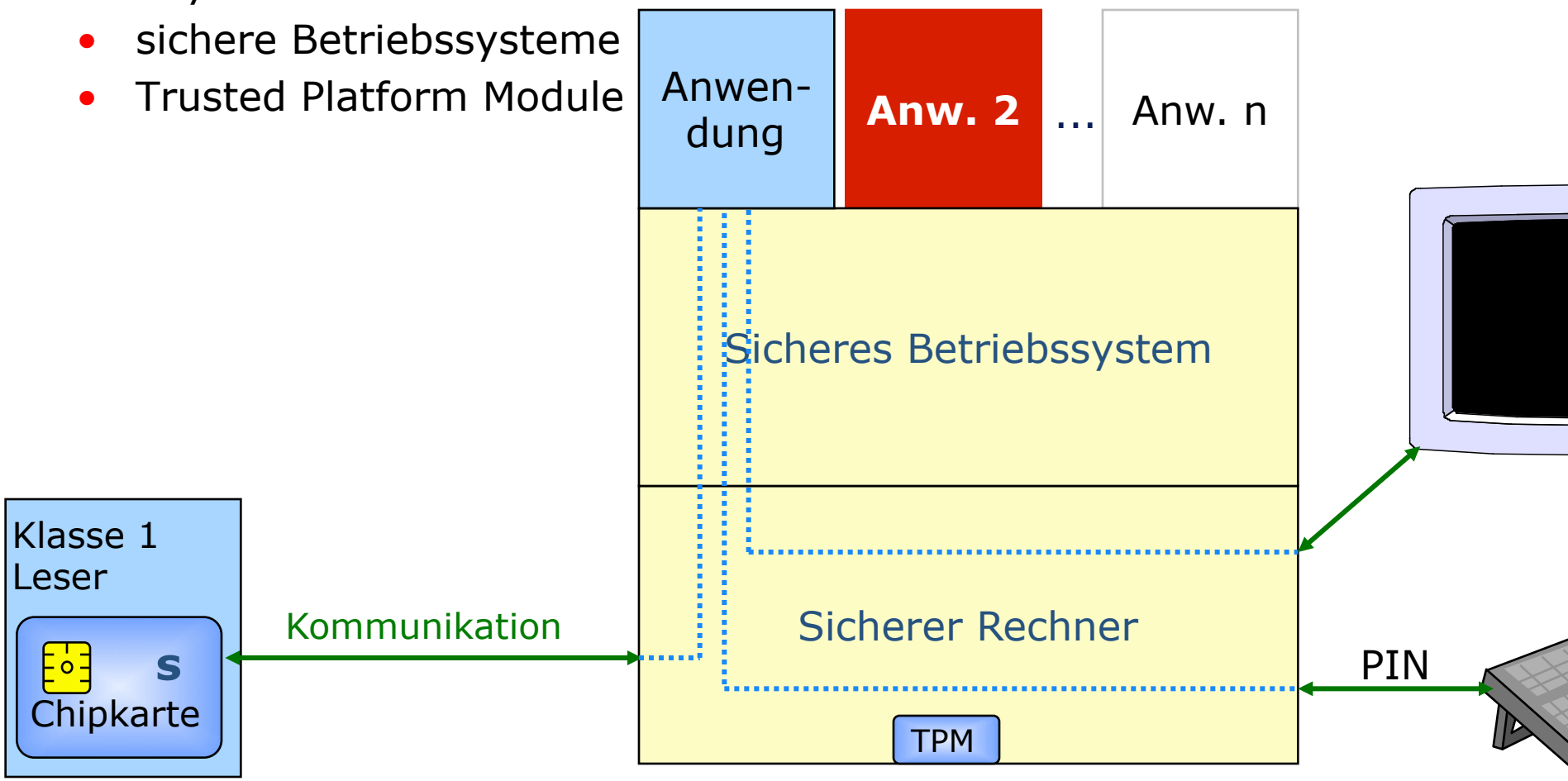

=

- Display
- Tastatur
- Physischer Schutz: Manipulationserkennung

- Entwurf offengelegt (keine versteckten Trojanischen Pferde)

# SICHER, wenn

- Physisch sichere Geräte
- sichere Betriebssysteme
- Trusted Platform Module



# Anonymität: Historische Entwicklung der Techniken

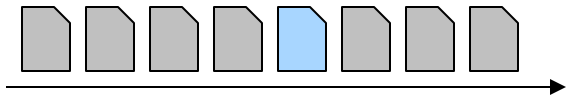
| Jahr | Idee / PET system |
|---|---|
| 1978 | Public-key encryption |
| 1981 | MIX, Pseudonyms |
| 1983 | Blind signature schemes |
| 1985 | Credentials |
| 1988 | DC network |
| 1990 | Privacy preserving value exchange |
| 1991 | ISDN-Mixes |
| 1995 | Blind message service |
| 1995 | Mixmaster |
| 1996 | MIXes in mobile communications |
| 1996 | Onion Routing |
| 1997 | Crowds Anonymizer |
| 1998 | Stop-and-Go (SG) Mixes introduced |
| 1999 | Zeroknowledge Freedom Anonymizer |
| *2000* | *AN.ON/JAP Anonymizer* |
| 2004 | TOR |

Grundverfahren
Anwendung

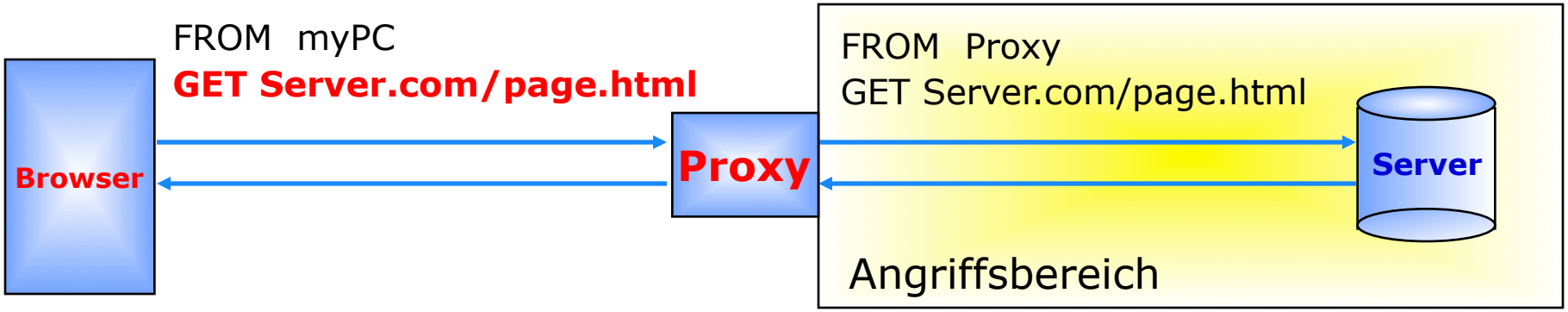
# Grundsätzliche Techniken

- Verteilung (Broadcast) + implizite Adressierung
  - Schutz des Empfängers; alle erhalten alles
  - lokale Auswahl

- Dummy Traffic: Senden bedeutungsloser Nachrichten
  - Schutz des Senders



- Proxies zwischenschalten
  - Server erfährt nichts über Client, Proxy kann mitlesen



## Grundsätzliche Techniken

- DC-Netz: kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- Blind-Message-Service: Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- MIX-Netz: kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen Betreibern, Kryptographie und Dummy Traffic
  - Schutz der Kommunikationsbeziehung
  - Effizient in Vermittlungsnetzen
- Steganographie
  - Verbergen einer Nachricht in einer anderen

# Kurse zur IT-Sicherheit, angeboten vom Arbeitsbereich SVS

- GSS
  - Einführung in die IT-Sicherheit
  - Rechner- und Betriebssystem-Sicherheit
  - Einführung in die Kryptographie
  - Internet-Sicherheit
- VIS
  - Safety und Fehlertoleranz
  - Kryptographie
  - Public Key Infrastructures (PKI)
  - Steganographie
  - Digital Rights Management
  - Privacy Enhancing Technologies (PET)
- SKI
  - Sicherheitsmanagement
  - Sicherheit mobiler Systeme


Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG