Mehrseitige IT-Sicherheit und technischer Datenschutz

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

http://www-sec.uni-regensburg.de/

Management der Informationssicherheit

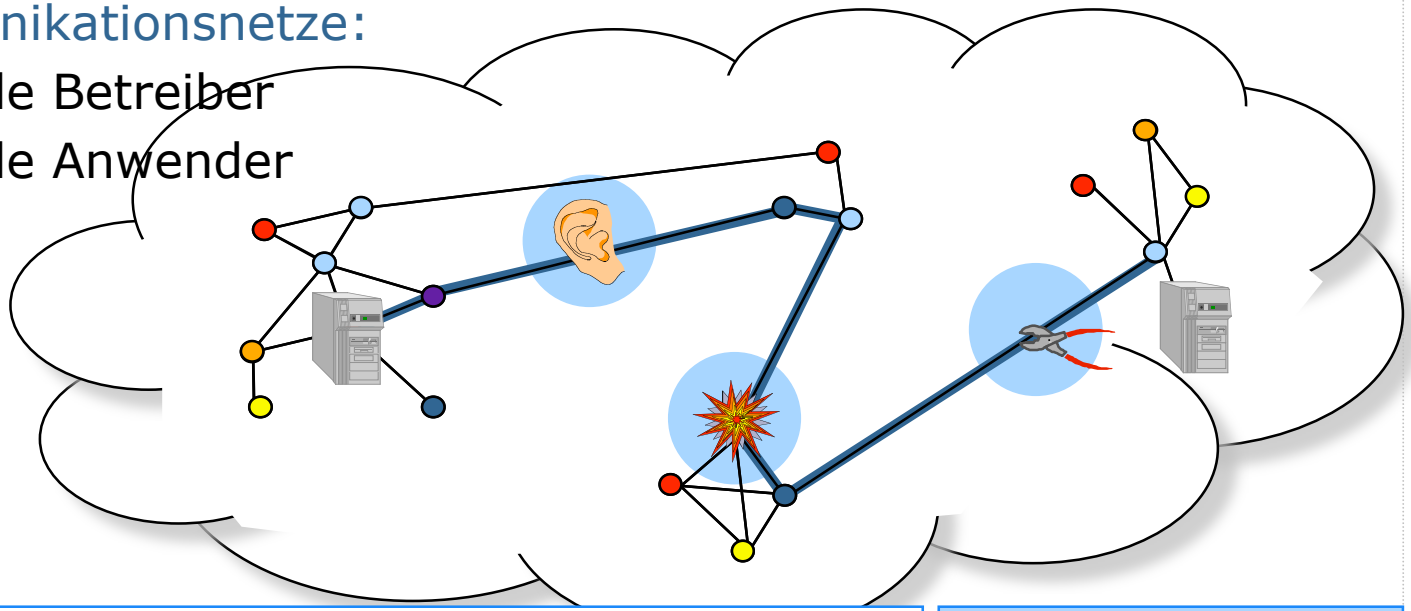
IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Themen, die am Lehrstuhl bearbeitet werden:
  - Sicherheit in verteilten Systemen und Mehrseitige Sicherheit
  - Datenschutzfreundliche Techniken
  - Sicherheit im Internet
  - Digital Rights Management Systeme
  - Sicherheit im E-Commerce und in mobilen Systemen

- Weitere Informationen:
  - http://www-sec.uni-regensburg.de

Sicherheit in Rechnernetzen

- Telekommunikationsnetze:
  - sehr viele Betreiber
  - sehr viele Anwender



Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Sicherheit: Abgrenzung von Security & Safety

SECURITY
Schutz gegen beabsichtigte Angriffe

Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit
- Ermöglichen von Kommunikation

SAFETY
Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

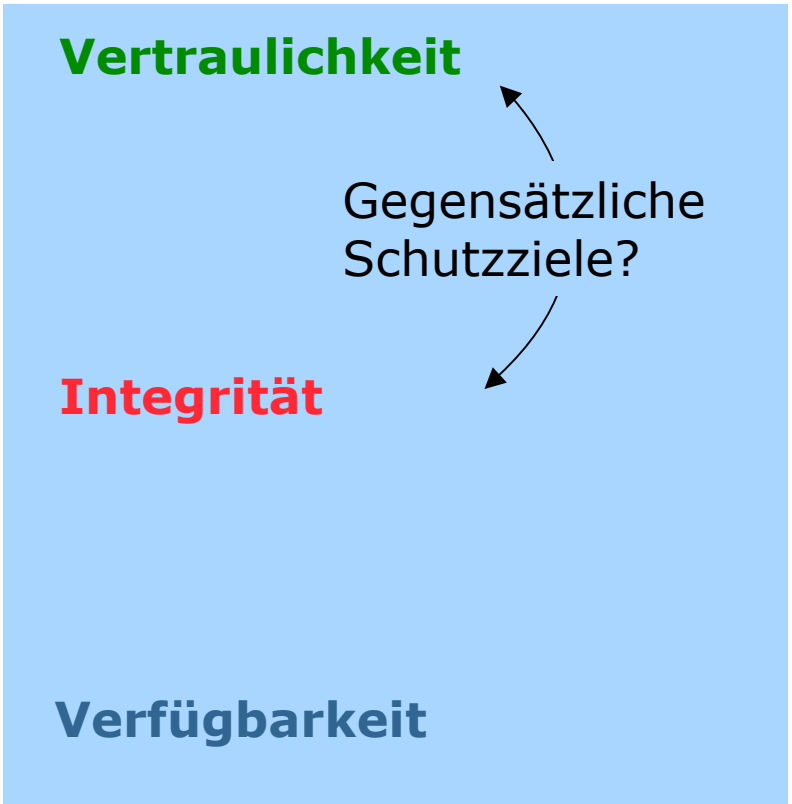
Schutzziele (Voydock, Kent 1983)

- 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 **Verdecktheit**	Inhalte	**Anonymität** **Unbeobachtbarkeit** Sender, Ort Empfänger
Integrität	Inhalte	**Zurechenbarkeit** **Rechtsverbindlichkeit** Absender, Bezahlung Empfänger
Verfügbarkeit	Inhalte	**Erreichbarkeit** Nutzer Rechner

Datenschutz

Kommunikationsgegenstand WAS?		**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	Inhalte	**Anonymität** **Unbeobachtbarkeit** Sender, Ort, Empfänger
Integrität	Inhalte	**Zurechenbarkeit** **Rechtsverbindlichkeit** Absender, 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.

Einseitige oder mehrseitige Sicherheit?

Kommunikationspartner haben nicht immer gleiche Sicherheitsinteresssen

Kunde

Händler

Der Händler soll an meine Bestellung gebunden sein.

Digitale Signatur

Digitale Signatur

Der Kunde soll an seine Bestellung gebunden sein.

Ich möchte anonym bleiben, solange ich nichts kaufe.

Vertrauen nötig

Pseudonymität: Treuhänder kennt Identität des Kunden, prüft Ware und Geld vor Lieferung

Der Kunde soll sich identifizieren.

Der Zustand der Ware soll einwandfrei sein, sonst: Geld zurück!

Der Bezahlvorgang soll sicher sein (Kein Betrug durch Kunden).

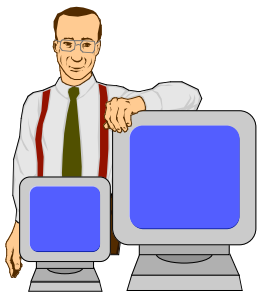
Ich möchte anonym bleiben beim Einkauf.

Anonyme Zahlungssysteme

Der Händler soll keine Kundenprofile anlegen dürfen.

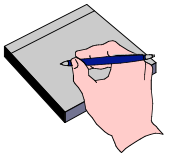
Vertrauen nötig

Selbstverpflichtung, P3P



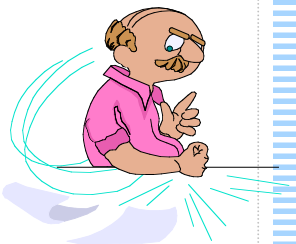
Mehrseitige Sicherheit

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



  1. Sicherheitsinteressen formulieren
     - Setzt Verständnis des Benutzers voraus
     - Gute Bedienoberflächen sind nötig

  2. Konflikte erkennen und Lösungen aushandeln
     - Setzt entsprechende Tools und
     - Technische Protokolle voraus

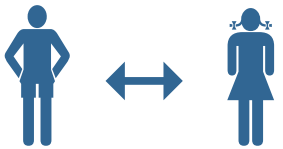


  3. Sicherheitsinteressen durchsetzen
     - Anwender brauchen Werkzeuge zum Selbstschutz
- Randbedingung
  - möglichst wenig Vertrauen in andere setzen müssen, d.h.
  - »Sicherheit mit minimalen Annahmen über andere«

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

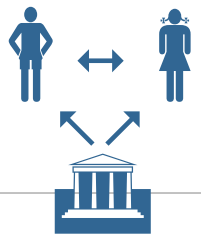
Techniken für Mehrseitige Sicherheit haben das Potential, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un)-Sicherheit zu befreien.

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

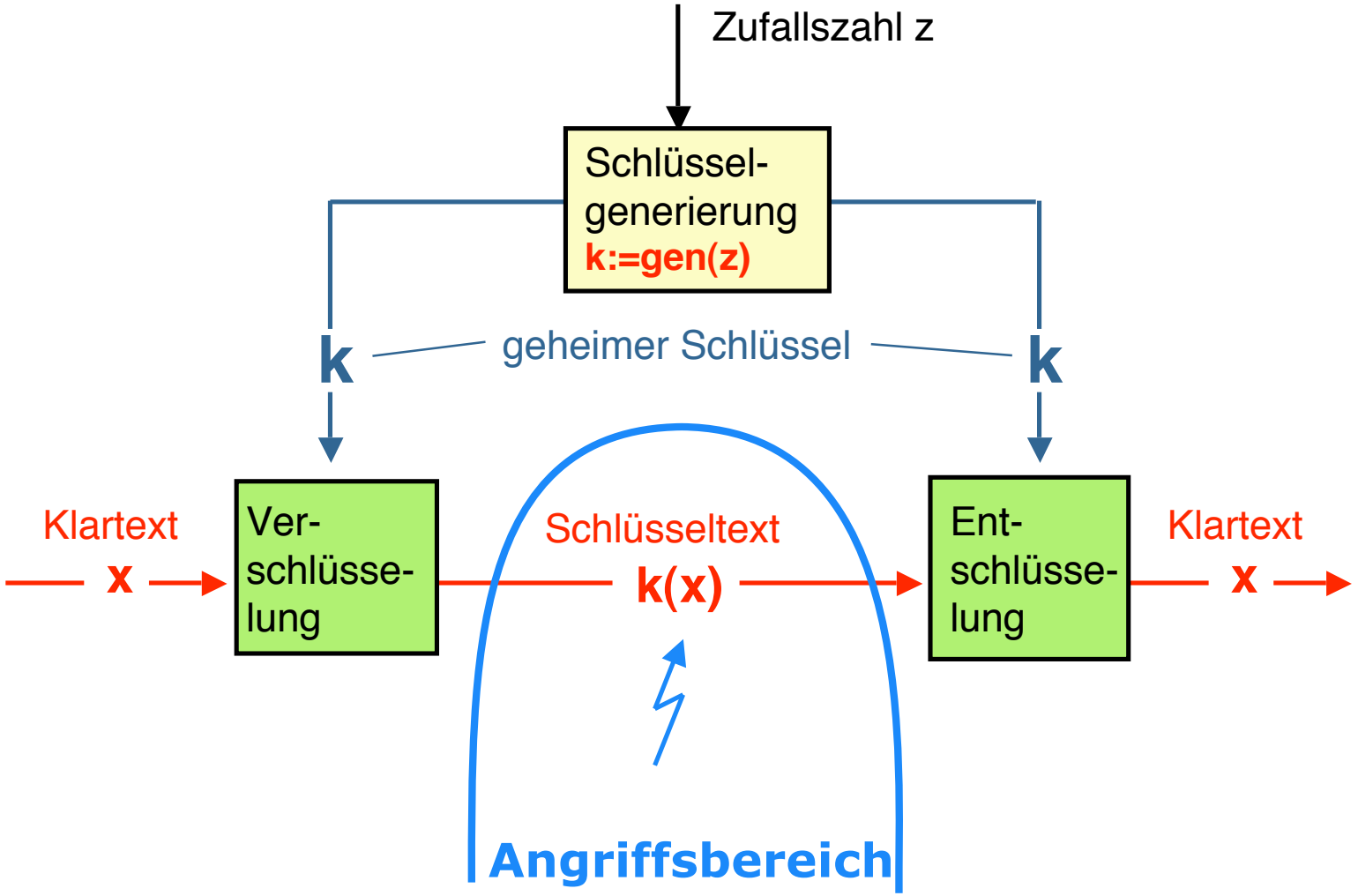
  - Anonymisierer: JAP, TOR

Verschlüsselung

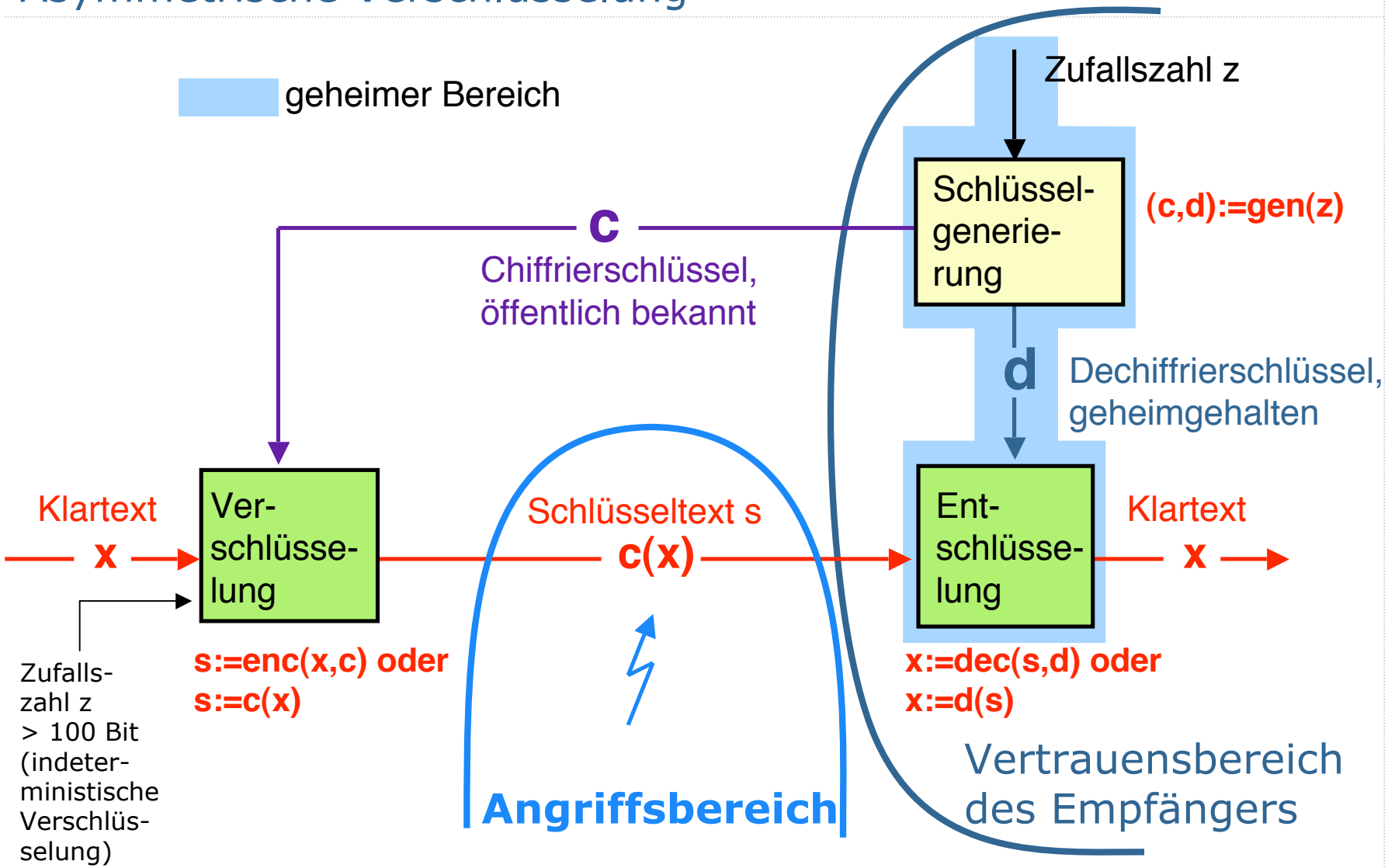
- Symmetrische Verschlüsselung, z.B. DES, AES
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits

- Asymmetrische Verschlüsselung, z.B. RSA
  - Jeder Nutzer generiert Schlüsselpaar:
    - Öffentlichen Verschlüsselungsschlüssel
    - Privaten Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit

Symmetrische Verschlüsselung

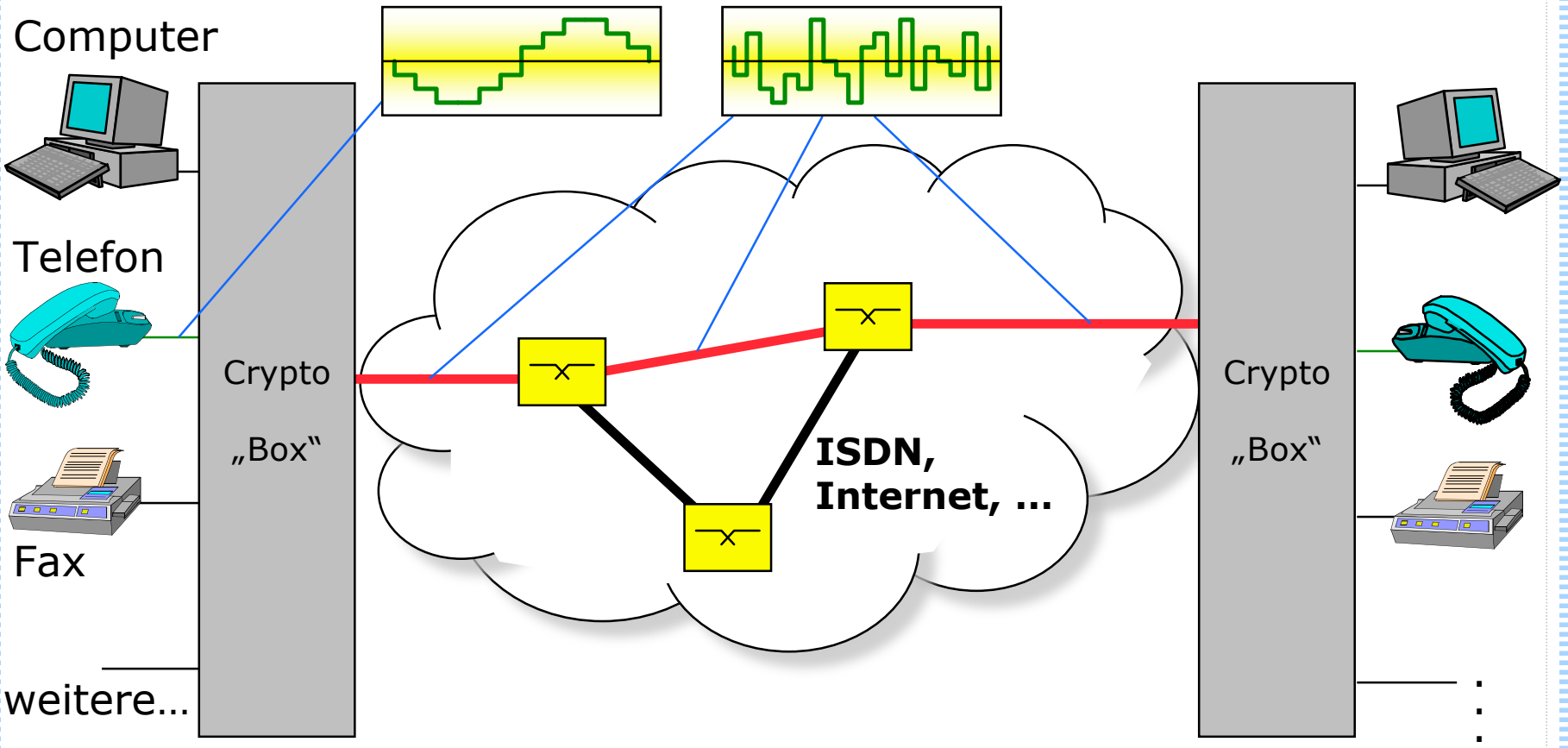


Asymmetrische Verschlüsselung



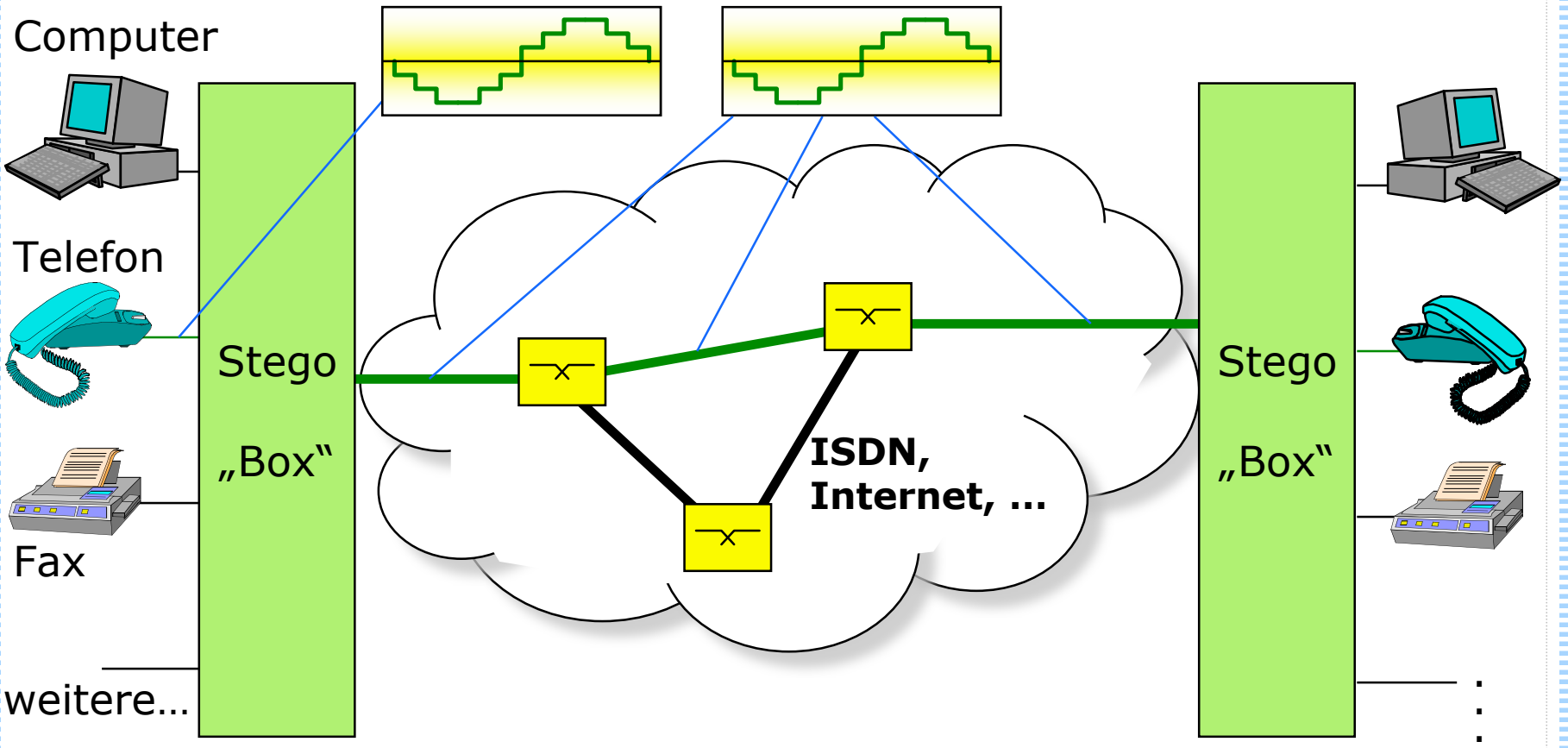
Kryptographie

- Verwendung von Kryptographie ist erkennbar



Steganographie

- Verwendung von Steganographie ist nicht erkennbar



Steganographie

Ziel: vertrauliche Kommunikation

Schlüssel

Schlüssel

Hülldaten

einzubettende Daten

Einbetten

Stegodaten

Extrahieren

eingebettete Daten

Geheime Nachricht, ggf. vorverschlüsselt

Sender

Angreifer/ Überwacher sieht nur das Foto

keine Änderungen

Empfänger

Geheime Nachricht

- exakt gleich
- nicht feststellbar
- möglichst viel

Steganographie

- Verbergen der Existenz einer geheimen Nachricht

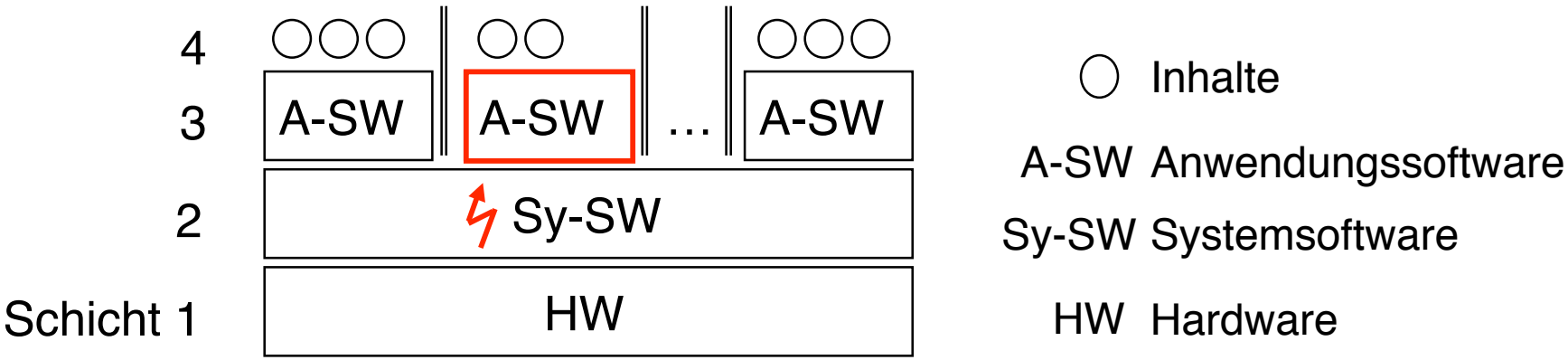
Original

Verändert

Differenz

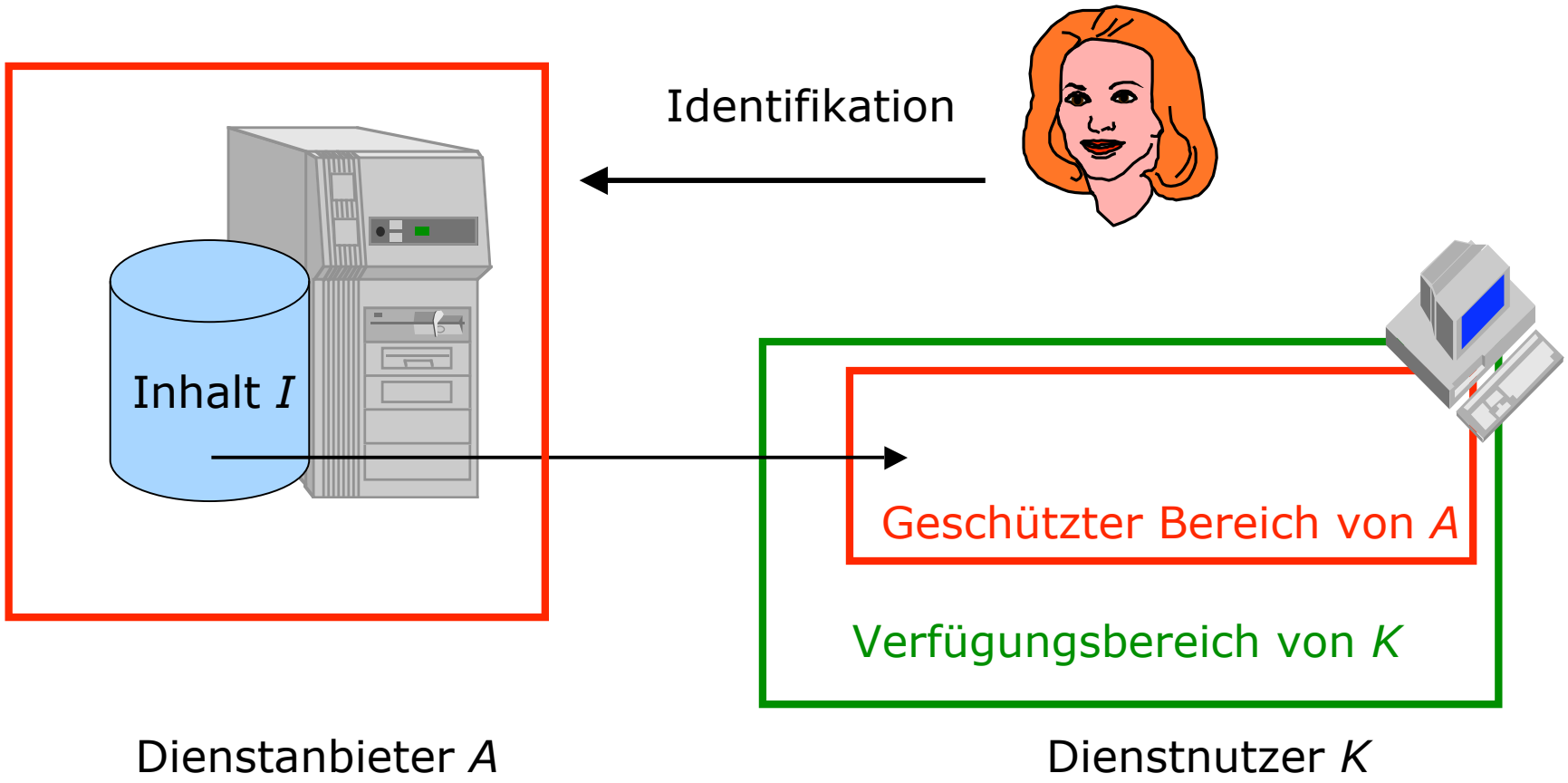
Offenlegung Entwurf: Frei programmierbarer Universal-PC

- Ausführungs-Schichtenstruktur
  - Objekte können vor den darunter liegenden Schichten nicht effizient geschützt werden.
- Folge:
  - Auf frei programmieren PCs werden Inhalte nie wirklich schützbar sein.



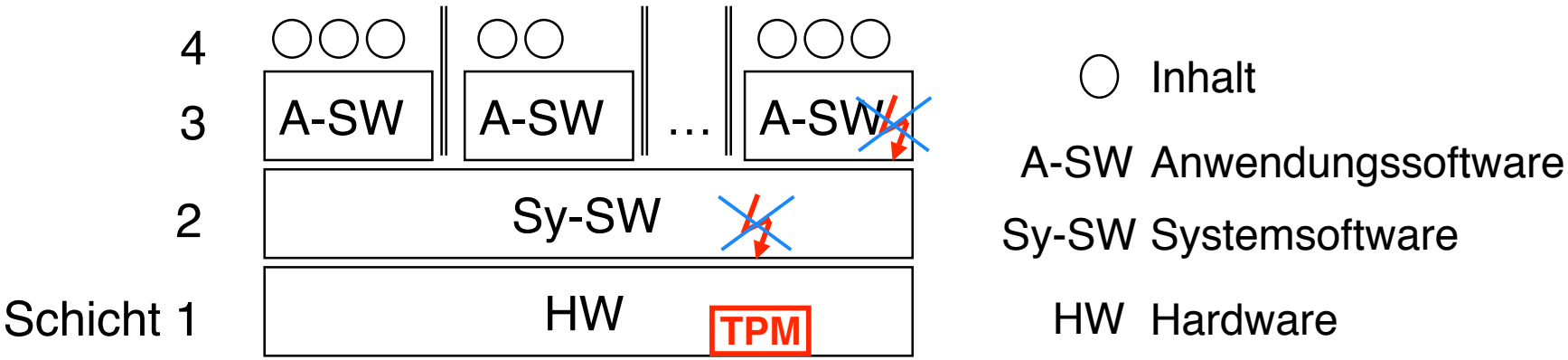
Das DRM-Problem

- Einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihm aber daran hindern, *alles* damit tun zu können.



Offenlegung Entwurf: [Nicht] Frei programmierbarer Universal-PC

- Abwehr:
  - spezielle Hardware (Tamper Proof Module, TPM), die im PC eingebaut ist
  - schützt vor Ausführung nicht autorisierter Programme
- Folge:
  - Es können nur noch offizielle Programme mit einem geschützten Inhalt verwendet werden.



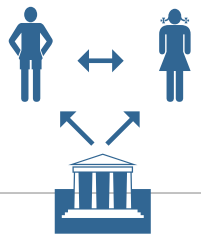
Warum Offelegung des Entwurfs? Nutzer muss sicher sein, dass Ausführungsumgebung(en) frei von trojanischen Pferden sind.

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

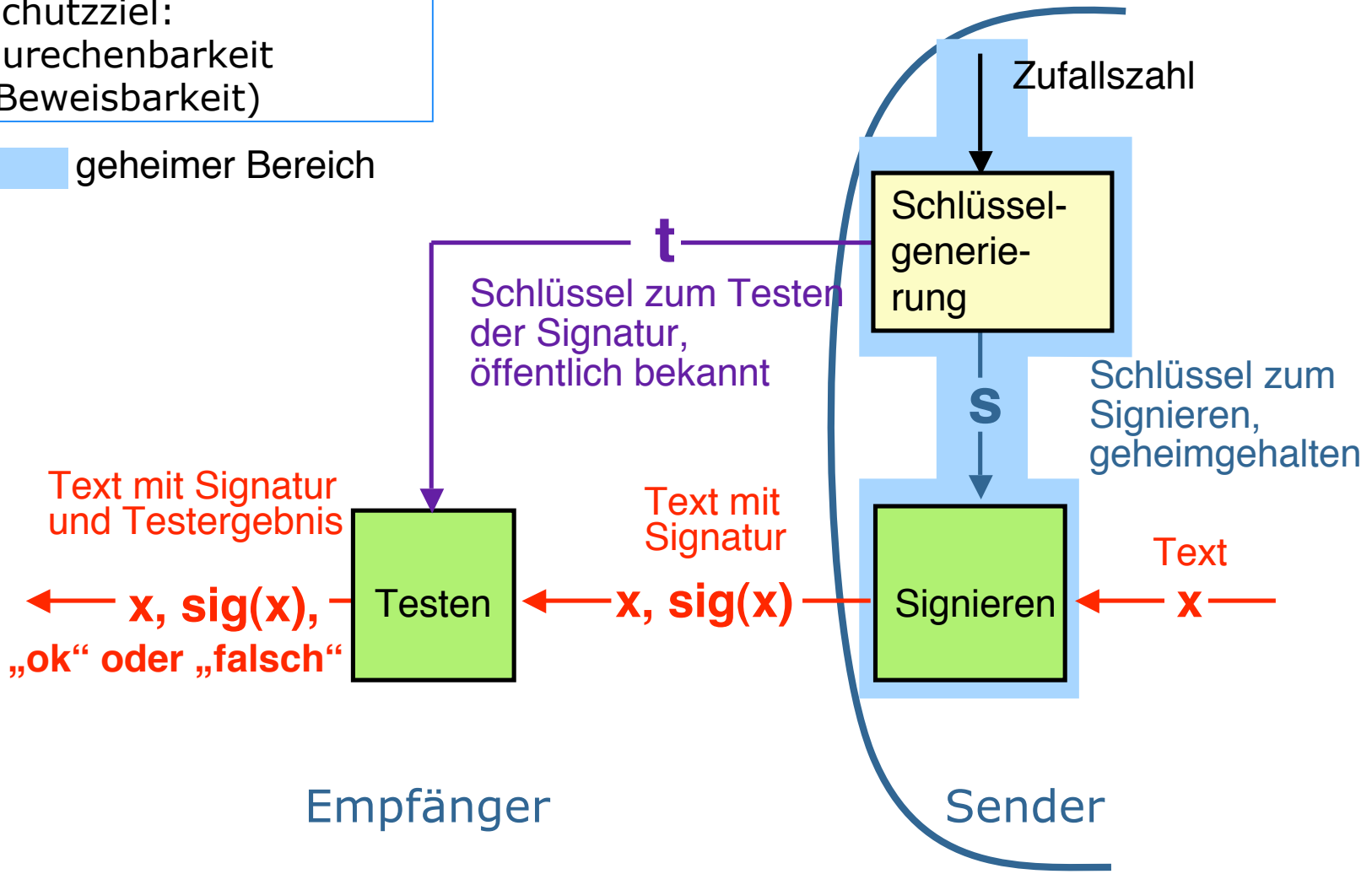
- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

Digitales Signatursystem

Schutzziel:
Zurechenbarkeit
(Beweisbarkeit)

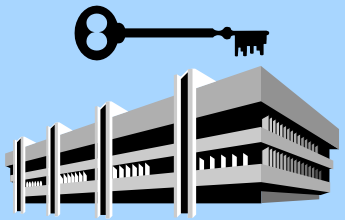
geheimer Bereich



Zertifizierung des öffentlichen Testschlüssels

Schlüsselzertifikat:
Beglaubigung der Zusammengehörigkeit von t_A und Identität von A

Zertifizierungsstelle Z

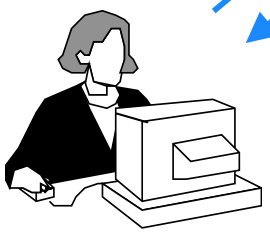


2. Z prüft Identität von A und stellt digitales Schlüsselzertifikat aus, d.h. signiert (A, t_A) mit seinem Signierschlüssel s_Z

1. A beantragt digitales Schlüsselzertifikat für t_A.

3. $cert(A, t_A)$

5. B prüft Zertifikat mit t_Z und Signatur mit t_A



4. Nachricht von A, s_A(Nachricht von A), $cert(A, t_A)$

Teilnehmerin A

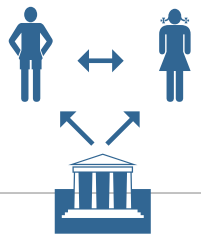
Teilnehmer B

Techniken für Mehrseitige Sicherheit

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Regulierungsversuche?
  - Krypto-Verbot läuft leer, da «Kriminelle» auf Steganographie ausweichen können

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Verbote laufen leer, da Steganographie nicht mehr erkennbar ist

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Vorratsdatenspeicherung ist weitestgehend sinnlos, da «Kriminelle» auf multilateral nutzbare Technik ausweichen, außerdem öffentliche Telefone, Prepaid Handies, offene WLANs, unsichere Bluetooth-Mobilfunkgeräte

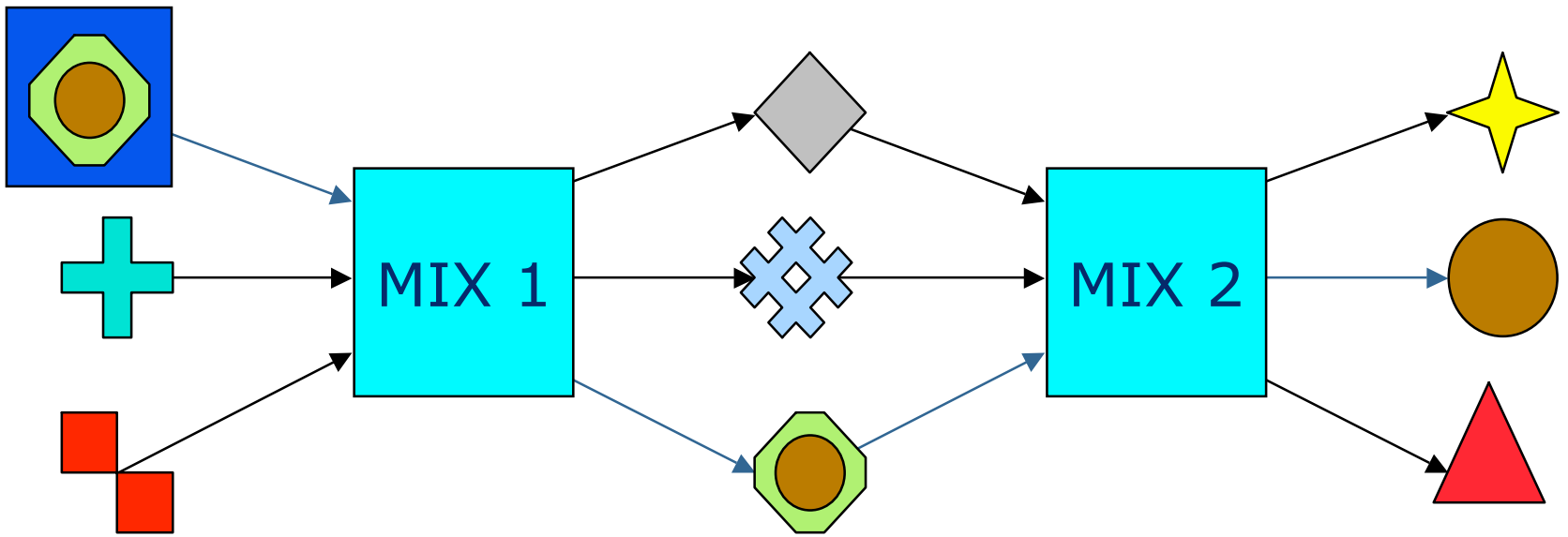
Anonymität, Unbeobachtbarkeit und Pseudonymität

- Teledienstedatenschutzgesetz (TDDSG)
  - § 4 Absatz 6: Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

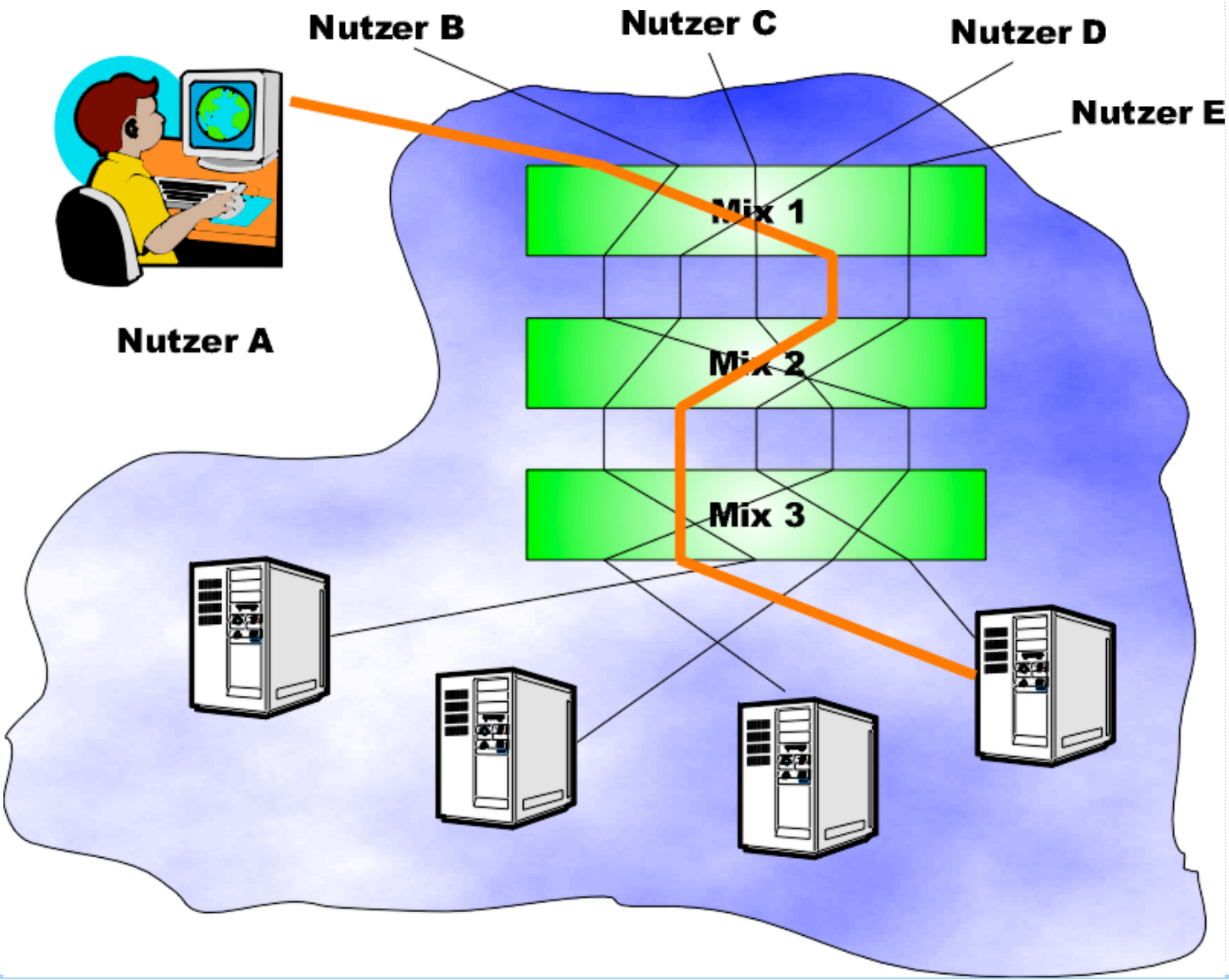
- Technischer Datenschutz
  - Systeme so konstruieren, dass unnötige Daten vermieden und nicht miteinander verkettet werden können.
- Zu verschleiern sind:
  - Adressen: Sender, Empfänger, Kommunikationsbeziehung
  - Zeitliche Korrelationen: Zeitpunkte, Dauer
  - Übertragenes Datenvolumen und inhaltliche Korrelationen
  - Orte: Aufenthaltsorte, Bewegungsspuren

Mix-Netz (Chaum, 1981)

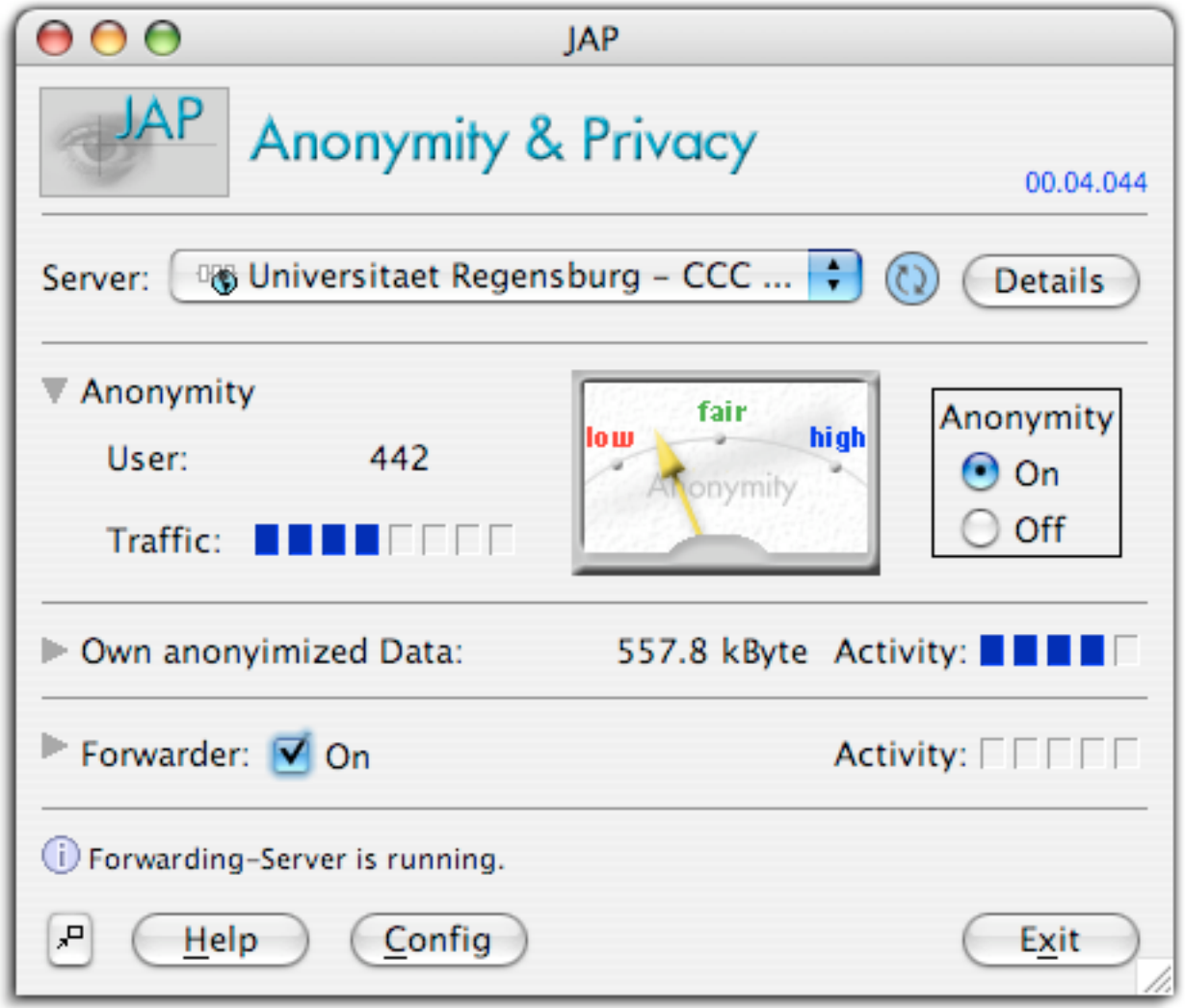
- Grundidee:
  - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.
- Schutzziel:
  - perfekte Unverkettbarkeit von Sender und Empfänger



Nutzbarmachung der Mixe für Webzugriff



AN.ON/JAP



Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de

AN.ON/JAP

Förderer: BMWA, Projektpartner: TU Dresden, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, FU Berlin, HU Berlin, Universität Regensburg, Medizinische Universität Lübeck, Chaos Computer Club, Ulmer Akademie für Datenschutz und IT-Sicherheit, RWTH Aachen, New York University

Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de

Stand der Sicherheitstechnik

Schutzziel	Technik	Stand der Technik	Nutzbarkeit
Vertraulichkeit	Verschlüsselung	sehr gut	gut
Verdecktheit	Steganographie	gut	schlecht
Anonymität Unbeobachtbarkeit	Remailer, Proxies, Mixe	befriedigend	befriedigend
Zurechenbarkeit	Digitale Signatur	befriedigend	befriedigend

Stand der Sicherheitstechnik

- Viele Verfahren sind theoretisch ausgereift und sichere Technik ist teilweise verfügbar:
  - meistens noch Detailprobleme
  - selten Grundsatzprobleme:
    - Beispiel: Wie realisiert man eine dauerhaft sichere, nicht ausforschbare Hardware (z.B. zur Aufbewahrung von kryptographischen Schlüsseln)

- Defizite:
  - Integration von Sicherheitsfunktionen in existierende Systeme
  - Mehrseitig sichere Technik: Beachtung von Sicherheit
    - der Betreiber und der Betroffenen

    bereits beim Systemdesign berücksichtigen
  - Schulung, Sensibilisierung, Weiterbildung im Bereich Sicherheit

Prof. Dr. Hannes Federrath
Management of Information Security
University of Regensburg
D-93040 Regensburg
Germany

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888