Informationssicherheit und technischer Datenschutz durch verteilte Systeme

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

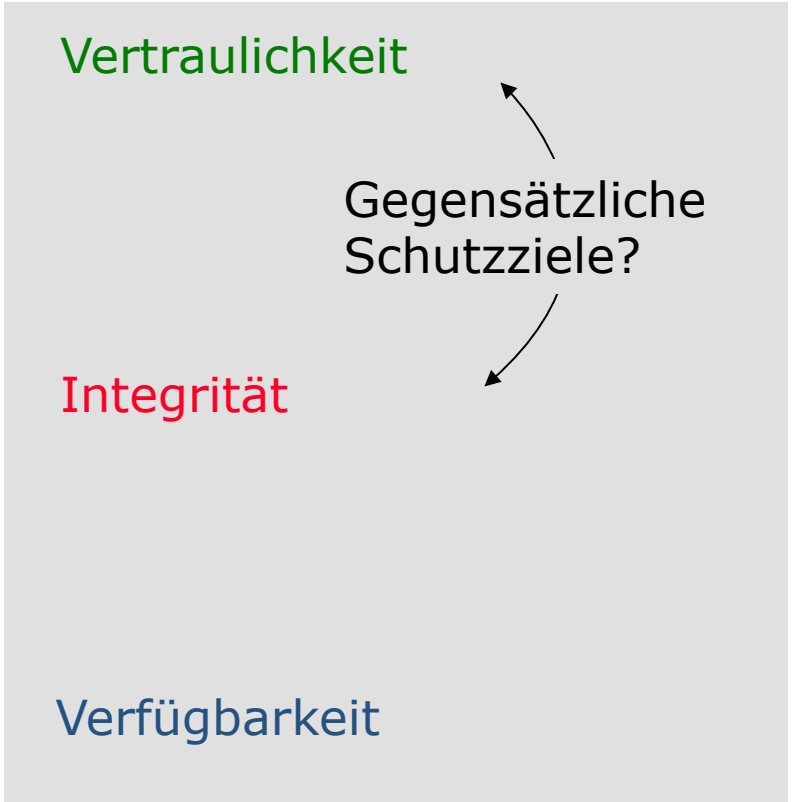
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Herbsttagung »Sicherheit im Internet« der Mathematischen Gesellschaft Hamburg,
26. Oktober 2013

Schutzziele

Voydock, Kent 1983

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



unbefugter Informationsgewinn

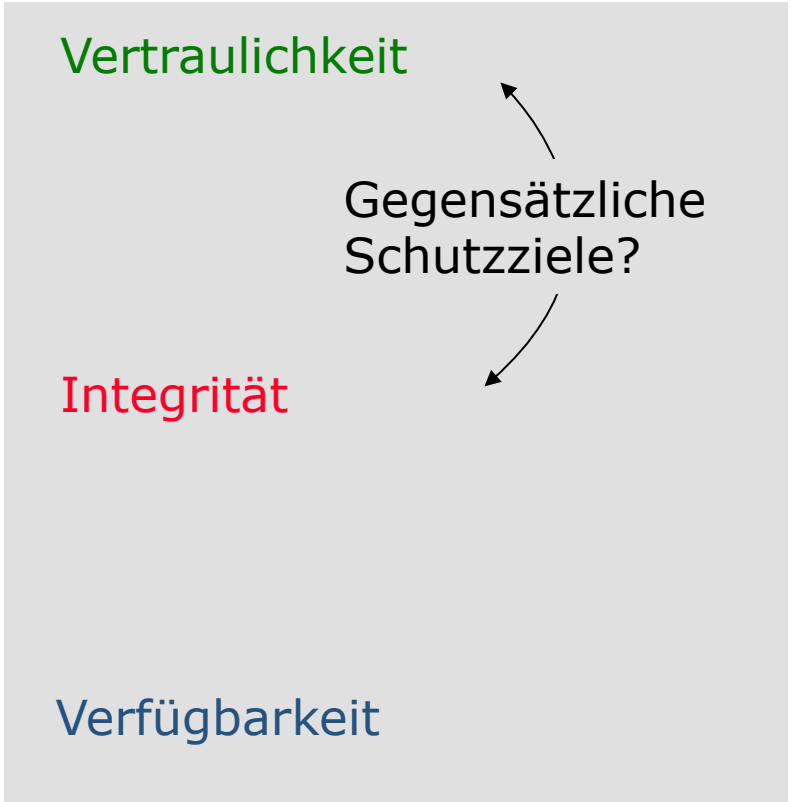
unbefugte Modifikation

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.



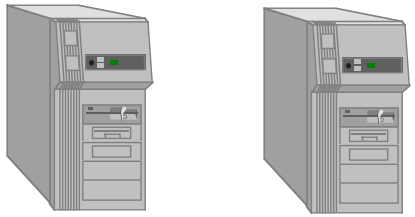
- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Verfügbarkeit: Redundanz und Diversität

Redundanz

Mehrfache Auslegung von Systemkomponenten

Bei Ausfall übernimmt Ersatzkomponente



Diversität

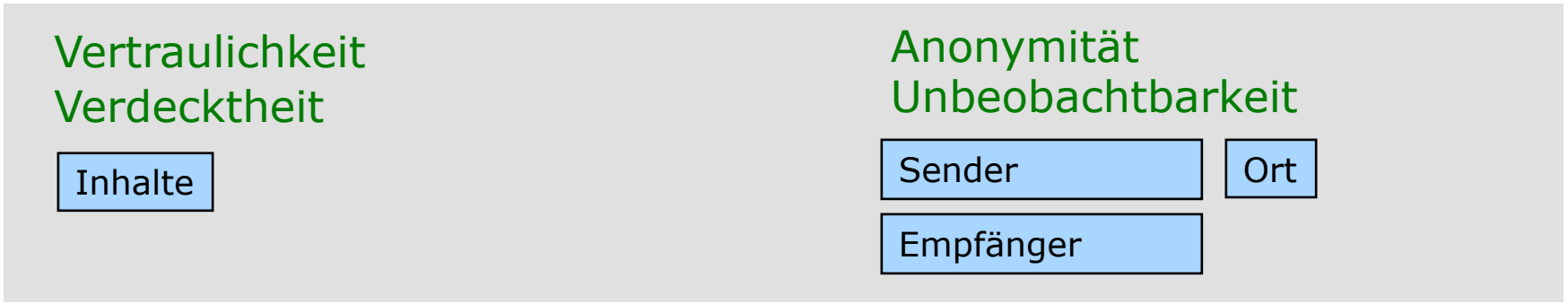
Verschiedenartigkeit der Herkünfte

Tolerieren von systemat. Fehlern und verdeckten trojanischen Pferden

Unabhängige Entwicklung von redundanten (Software)-Komponenten

Verfügbarkeit

Vertraulichkeit: Schutzziele und Angreifermodell



- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen

- Insider
  - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
  - Staatliche Organisationen (insb. fremde)

Vertraulichkeit: Verfahren und Algorithmen

Verfahren

Algorithmen

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES, RSA, ElGamal, …

Verdecktheit

Steganographie

Inhalte + Existenz

F5, …

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer, Remailer, anonyme Zahlungssysteme

Pseudonyme, Proxies, umkodierende Mixe, DC Netz, Private Information Retrieval, …

Datenschutzfreundliche Techniken

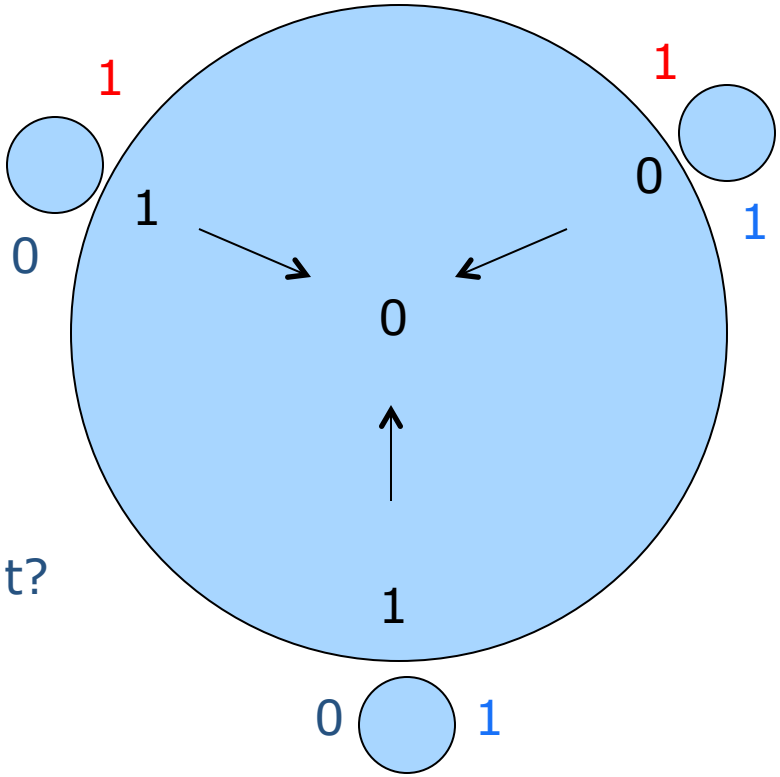
- DC-Netz: kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- Blind-Message-Service: Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- MIX-Netz: kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen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

DC-Netz

Chaum, 1988

- Jeder für sich:
  1. Jeder wirft mit jeden eine Münze
  2. Berechnet das xor der beiden Bits
  3. Wenn bezahlt, dann xor mit 1 (Komplement des Ergebnisses aus Schritt 2)
  4. Ergebnis veröffentlichen

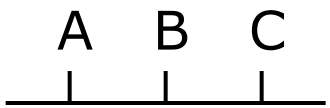
- Alle zusammen:
  1. Berechnen das xor der drei (lokalen) Ergebnisse
  2. Wenn globales Ergebnis 0, hat jmd. anderes bezahlt



Wer hat bezahlt?

DC-Netz

Chaum, 1988



Broadcastnetz

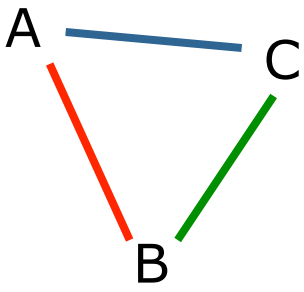
Echte Nachricht von A	00110101
Schlüssel mit B	00101011
Schlüssel mit C	00110110
Summe	00101000

A sendet 00101000

Leere Nachricht von B	00000000
Schlüssel mit A	00101011
Schlüssel mit C	01101111
Summe	01000100

B sendet 01000100

Schlüsselgraph



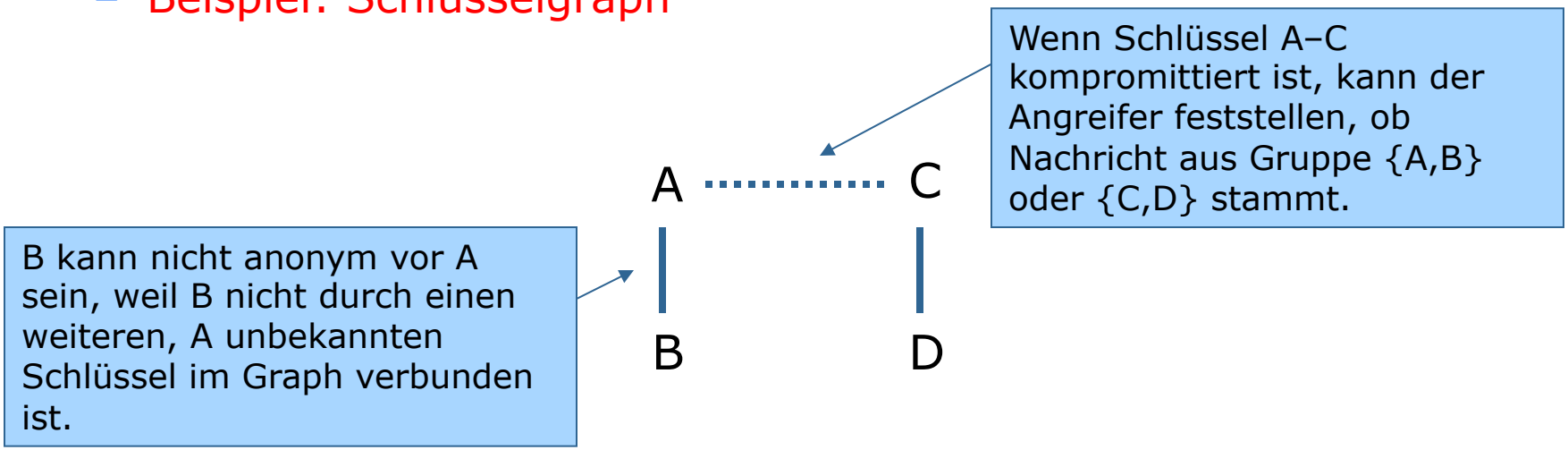
Leere Nachricht von C	00000000
Schlüssel mit A	00110110
Schlüssel mit B	01101111
Summe	01011001

C sendet 01011001

Summe = Echte Nachricht von A 00110101

- Perfekte Unbeobachtbarkeit des Sendens
- Erfordert Synchronisierung der Teilnehmer: Runden
- Zu jedem Zeitpunkt kann immer nur ein Teilnehmer senden
  - Kollisionserkennung und -auflösung nötig

- Sicherheitseigenschaft
  - Jede Nachricht ist innerhalb der Teilnehmer unbeobachtbar, die durch einen zusammenhängenden Schlüsselgraph gebildet werden.
  - Beispiel: Schlüsselgraph



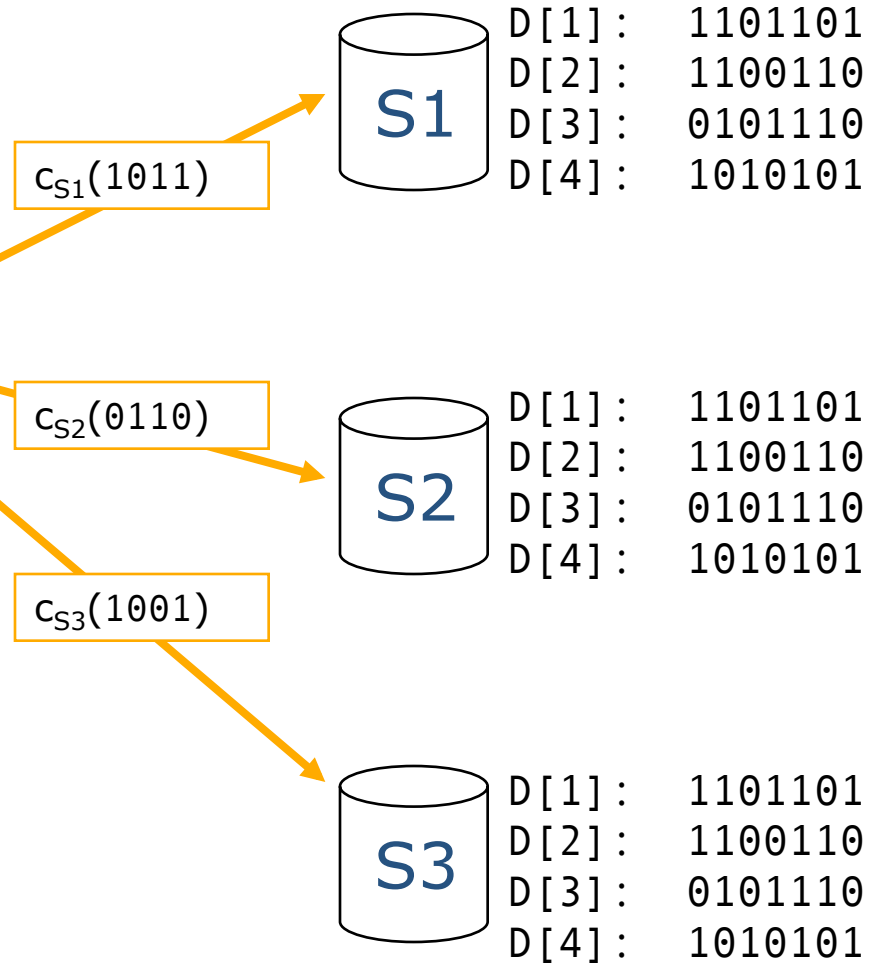
Blind-Message-Service: Anfrage

Cooper, Birman, 1995

Client interessiert sich für D[2]:

Index = 1234

Setze Vektor = 0100
Wähle zufällig request(S1) = 1011
Wähle zufällig request(S2) = 0110
Berechne request(S3) = 1001



- Schutzziel:
  - Client möchte auf Datenbestand zugreifen, ohne dass Datenbank erfährt, wofür sich der Client interessiert
- Replizierte Datenbanken mit unabhängigen Betreibern

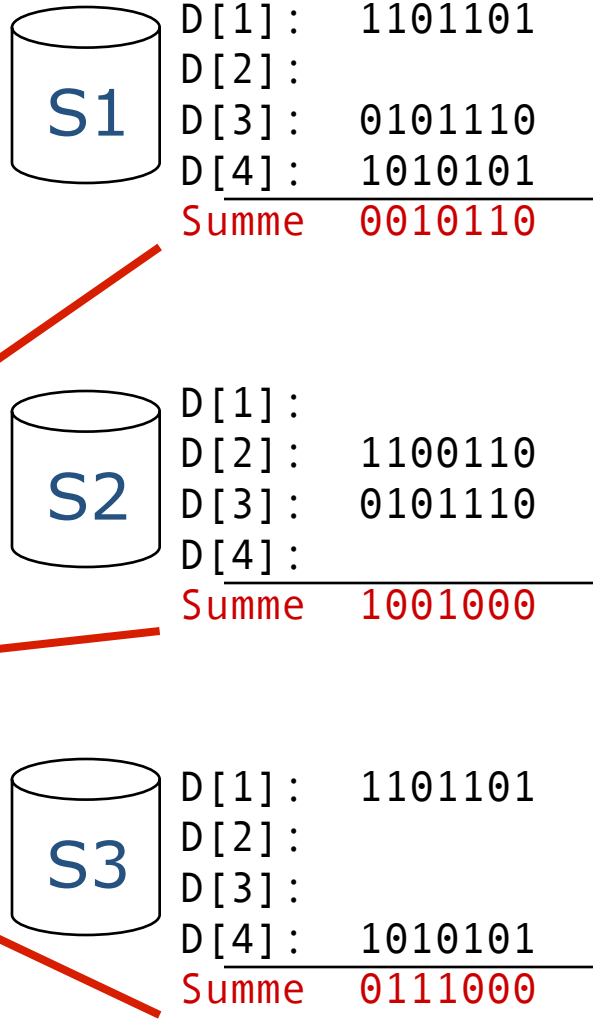
Blind-Message-Service: Antwort

Cooper, Birman, 1995

Client interessiert sich für D[2]:

Index = 1234

Setze Vektor = 0100
Wähle zufällig request(S1) = 1011
Wähle zufällig request(S2) = 0110
Berechne request(S3) = 1001



Antworten von

S1: 0010110
S2: 1001000
S3: 0111000

Summe entspricht D[2]: 1100110

Verbindungsverschlüsselung zwischen Servern und Client unbedingt notwendig

Mix-Netz

Chaum, 1981

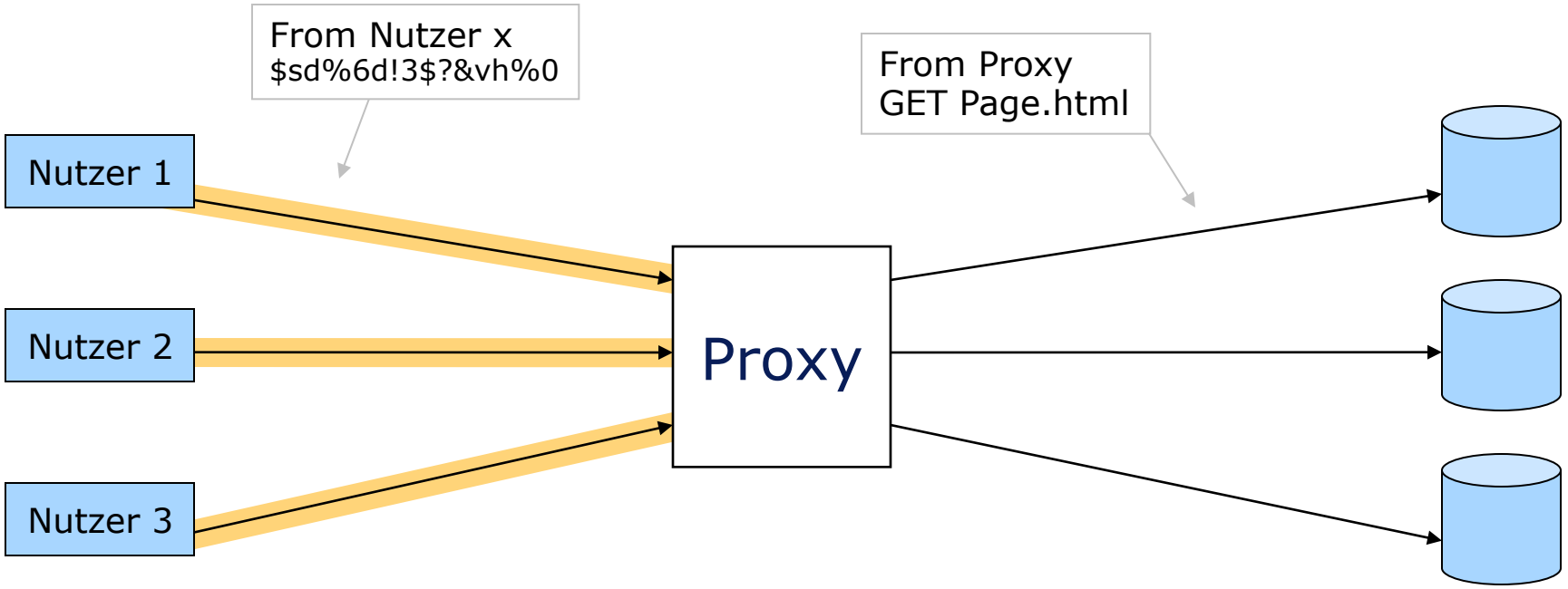
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- Grundfunktionen:
  - Nachrichten in einem »Schub« sammeln,
  - Wiederholungen ignorieren,
  - Nachrichten 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:
  - Unverkettbarkeit von Sender und Empfänger

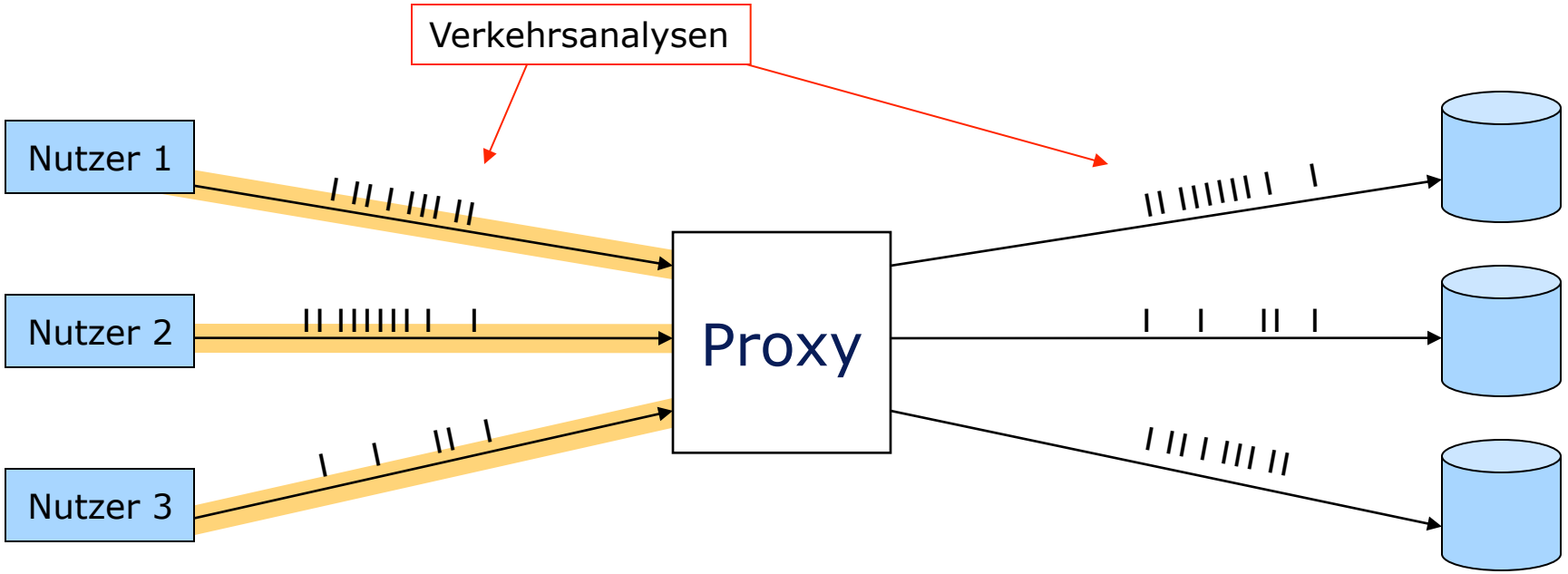
Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Beobachter nach Proxy und Serverbereiber:
    - erfahren nichts über den wirklichen Absender eines Requests
  - Beobachter vor Proxy:
    - Schutz des Senders, wenn Verbindung zu Proxy verschlüsselt

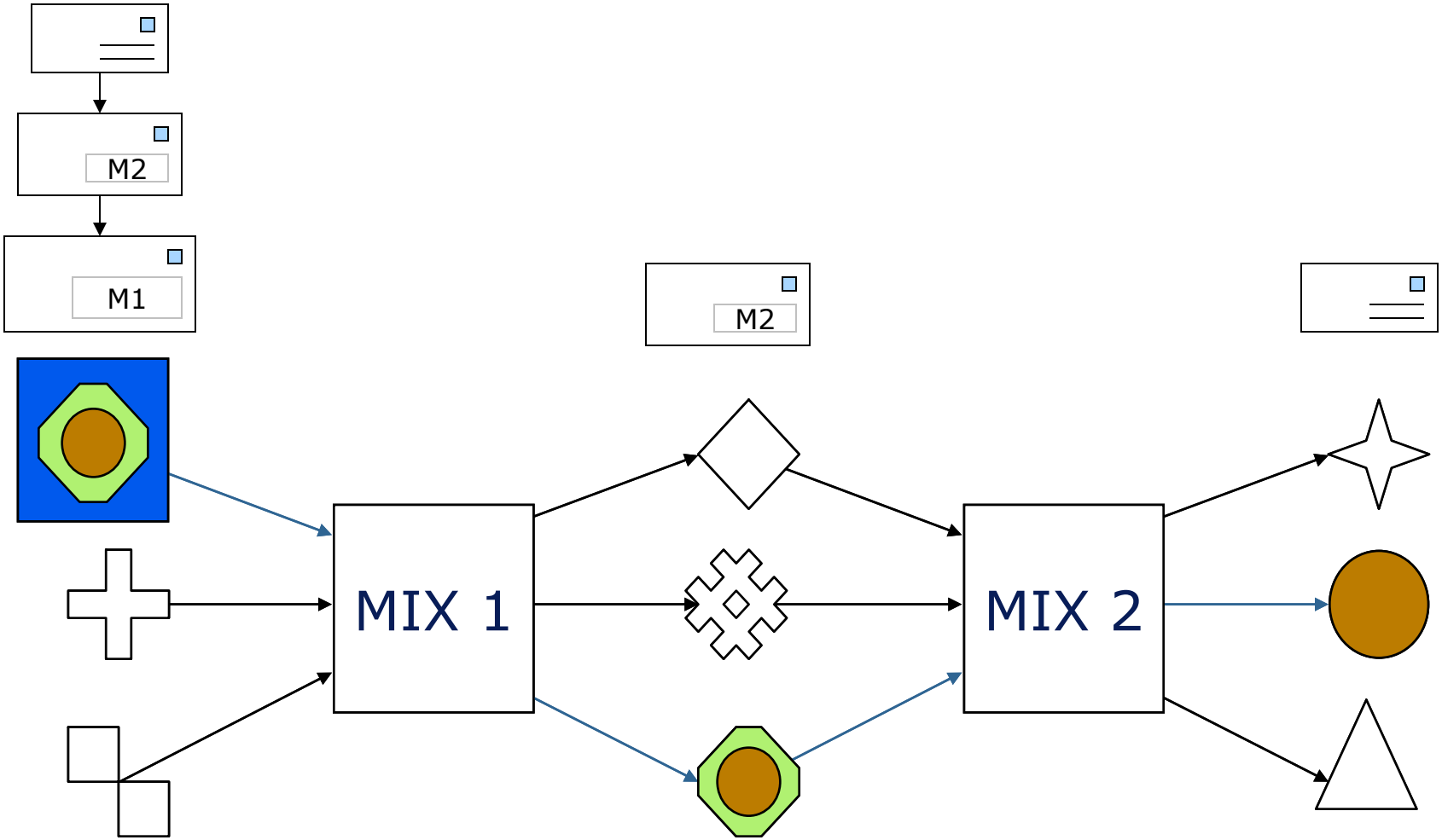


Proxies: Outsider

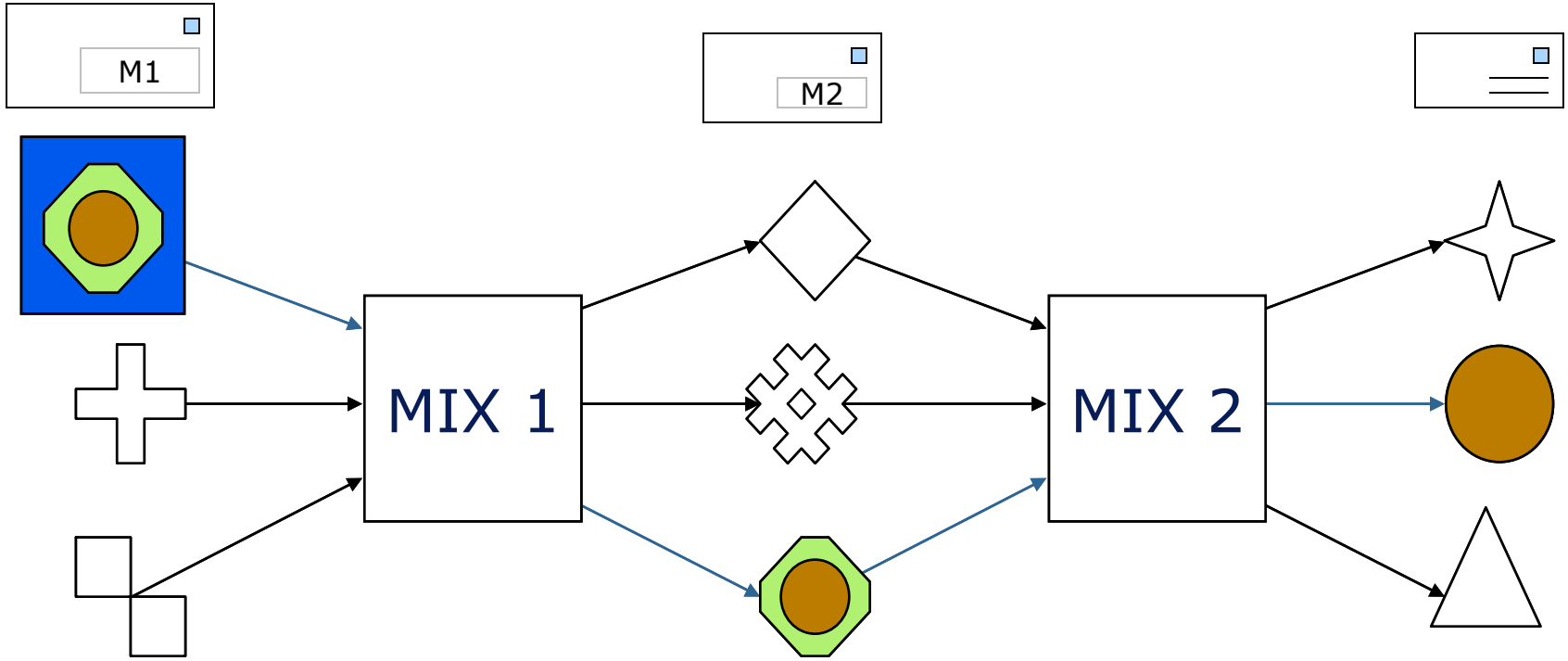
- Erreichbare Sicherheit (Outsider)
  - Aber: Trotz Verschlüsselung:
    - kein Schutz gegen Verkehrsanalysen
      - Verkettung über Nachrichtenlängen
      - zeitliche Verkettung



- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

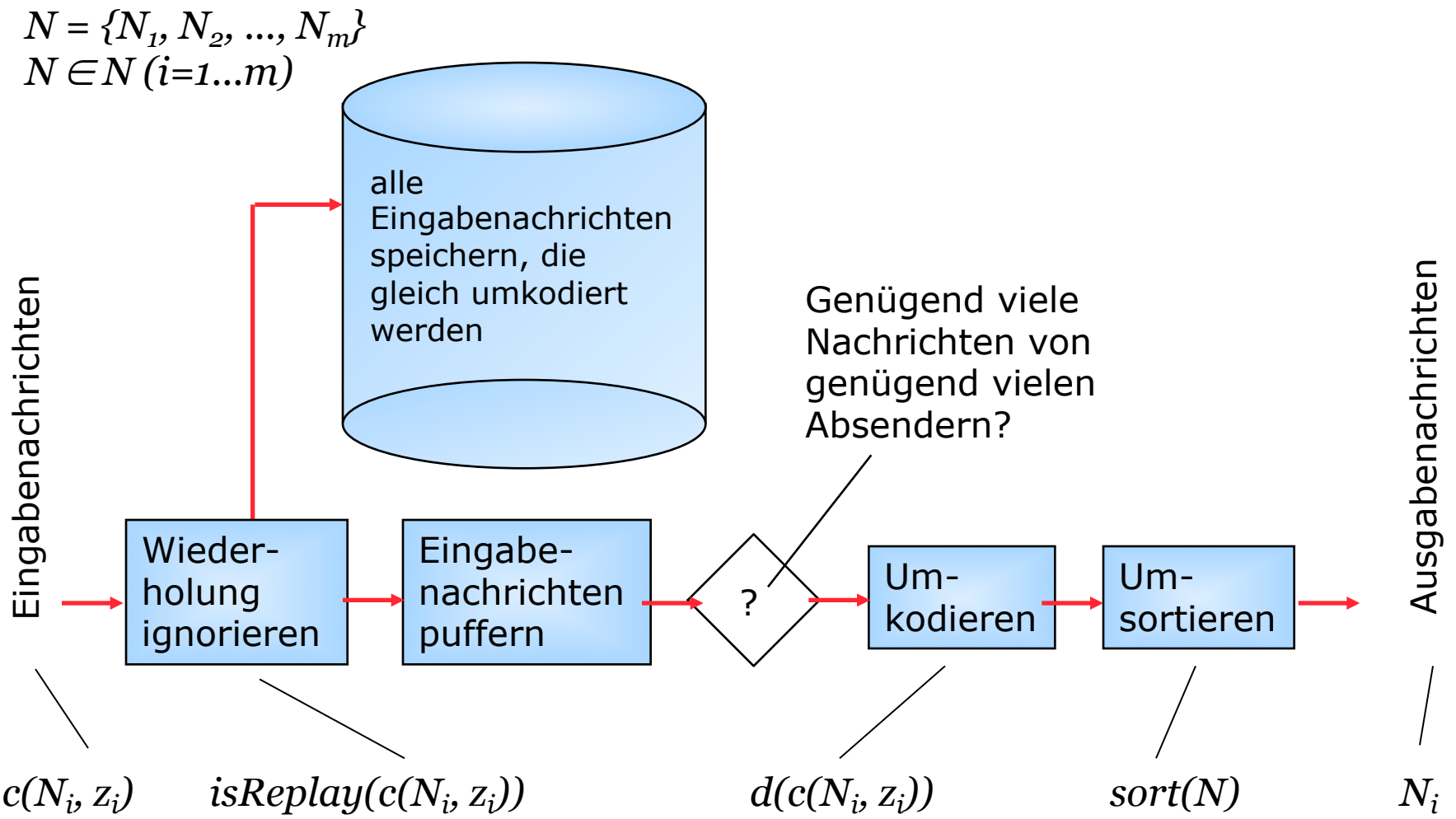


- Stärke der Mixe:
  - Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.
- Notwendige Bedingungen:
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.



Blockschaltbild eines Mix

Chaum, 1981

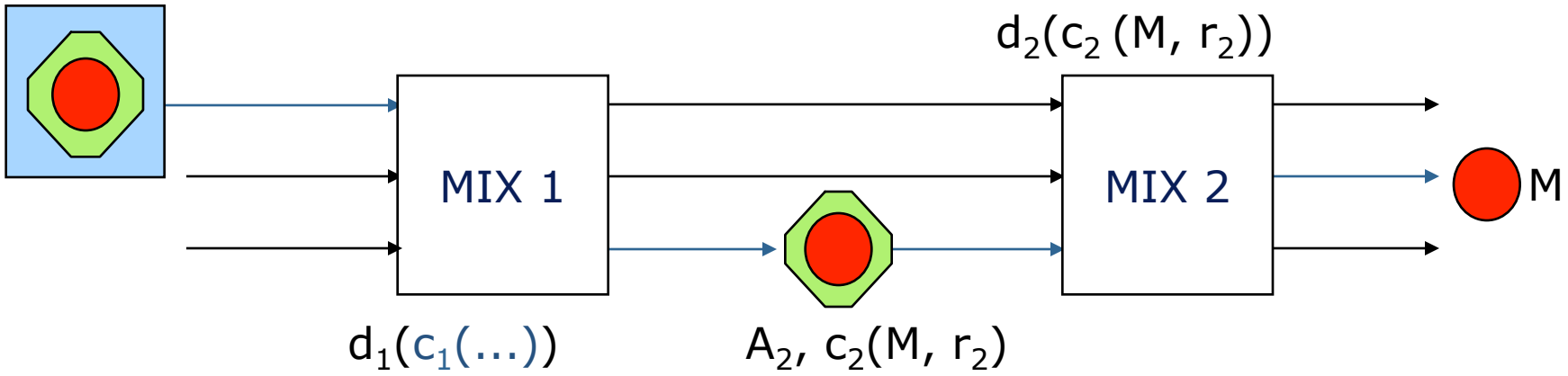


Kryptographische Operationen eines Mix

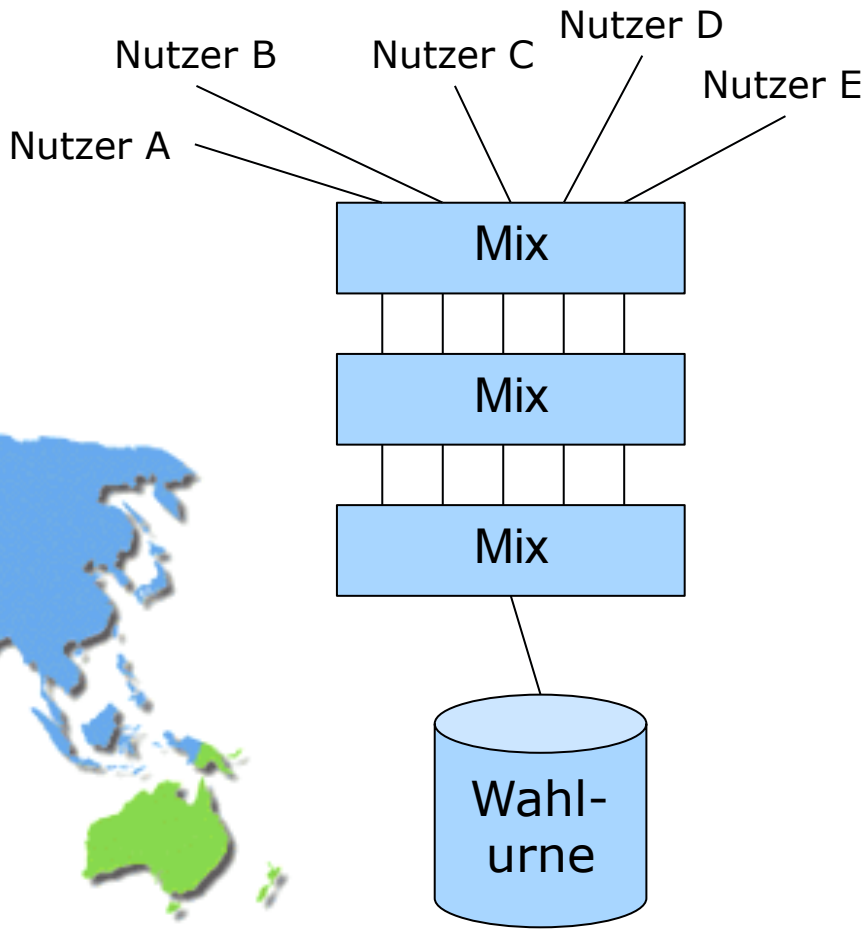
Chaum, 1981

- Verwendet asymmetrisches Verschlüsselungssystem
  - $c_i(...)$ Verschlüsselungsfunktion für Mix i
    - Jeder kann den öffentlichen Schlüssel c_i verwenden
  - $d_i(...)$ private Entschlüsselung von Mix i
    - Nur Mix i kann entschlüsseln
  - A_i Adresse von Mix i
  - r_i Zufallszahl (verbleibt im Mix, wird »weggeworfen«)
  - M (verschlüsselte) Nachricht für Empfänger (inkl. seiner Adresse)

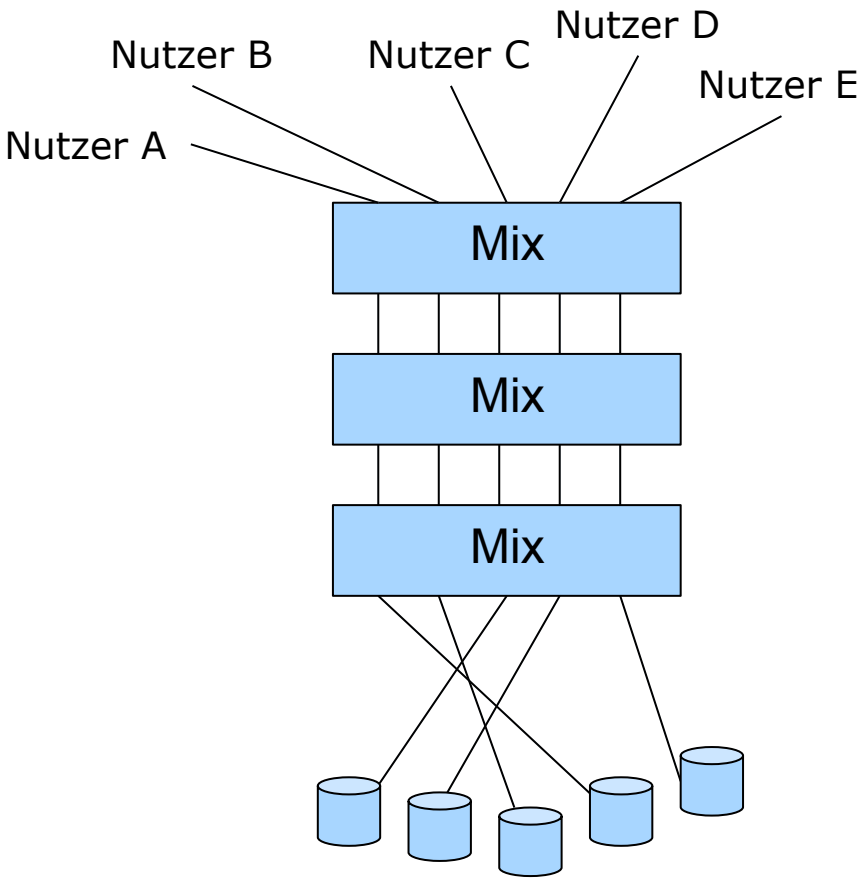
$A_1, c_1(A_2, c_2(M, r_2) , r_1)$



- Fördern der Nutzung von Techniken zum Schutz der Vertraulichkeit und Anonymität für demokratische Prozesse
  - z.B. Elektronische Wahlen



- Implementierung eines Dienstes zum anonymen Internetzugriff
- Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation
  - beruht auf Erweiterungen des Mix-Verfahrens von Chaum
  - Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)
- Schutz des Einzelnen vor Überwachung und Profilierung seiner Internetaktivitäten auch durch private Organisationen



Juristische Sicht

- Telemediengesetz (TMG, vormals Teledienstedatenschutzgesetz TDDSG)
  - § 13 Abs. 6 TMG: 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.

Nicht immer nur der Staat hat die Überwachungsmöglichkeiten

- Beispiele
  - Payback, Google, Facebook

- Die Wirtschaft und private Organisationen sammeln heute mehr Daten denn je
  - freiwillige Preisgabe
  - Verbesserung des Service (Customer Relationship Management)
  - illegal (weil kaum nachweisbar und unauffällig) oder in rechtlicher Grauzone (z.B. international handelnde Unternehmen)
- Was kann der Einzelne tun?
  - Zurückhaltung, Skepsis bei Datenweitergabe, technische Schutzmöglichkeiten nutzen (z.B. Verschlüsselung, Anonymisierer)

Historische Entwicklung

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
1999	Zeroknowledge Freedom Anonymizer
2000	AN.ON/JAP Anonymizer
2004	TOR

Grundverfahren
Anwendung

Tor (ursprünglich: Onion Routing)

Ziele:

Freier Informationszugang, voll dezentrale Strukturen

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

OpenSource

www.torproject.org

BROWSER BUNDLE

AN.ON (Software: JAP/JonDonym)

Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

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

OpenSource

www.anon-online.de

Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
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