

The image features a light green background on the left side, which contains a white rounded rectangular shape. The word "Chaum" is written in a dark blue, serif font within this white shape. Below the white shape, a dark blue horizontal bar extends across the width of the green area.

Chaum

Der Person: David Chaum

- Erfinder einiger kryptographischer Protokoll
- Fortentwicklung elektronischer Zahlungsmittel
- Gründer der *internationalen vereinigung fuer Kryptologie-Forschung*
- veröffentlicht “ *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* ”
1981, Erfindet den Mix-Verfahren

Motivation

- Privacy

Schutzziel von Mix-Verfahren

- Anonymisierung der Sender und Empfänger
- Schutz der Kommunikationsbeziehung

Anonymität

- Sender/Empfänger ist nicht identifizierbar innerhalb einer Menge von möglichen Sendern/Empfängern – der Anonymitätsgruppe.

Unbeobachtbarkeit

- Das Senden bzw. Empfangen von Nachrichten ist von Außenstehenden nicht feststellbar. Unbeobachtbarkeit gewährleistet Anonymität gegenüber Außenstehenden.

Unverkettbarkeit:

- Das Wissen über die Beziehungen von Objekten/Subjekten (Nachrichten, Sendern, Empfängern, Ereignissen etc.) ändert sich durch Beobachten des Systems nicht.

Was ist ein Mix ?

- Ein Mix ist ein Server im Netzwerk, der:
 - mehrfach verschlüsselte Nachrichten von Sendern entgegen nimmt
 - genau eine „Verschlüsselungs-Schale“ entfernt
 - mehrere Nachrichten in einem Schub (Batch) sammelt

Was ist ein Mix ?

- die Nachrichten eines Schubes umsortiert („mixt“)
- die bearbeiteten Nachrichten an den jeweiligen Empfängerweiterleitet

Grundfunktionen von Mix

- **Nachrichten Puffern**
- **Löschen von Duplikaten**
- **Umkodieren der Nachrichten**
- **Umsortieren der Nachrichten**

Nachrichten Puffern

- Sammeln der Nachrichten, bevor diese weiterverarbeitet werden.
- zwei Varianten des Puffers:
Batchbetrieb: m Speicherplätze für die Nachrichten vorgesehen; wenn diese Anzahl erreicht ist, wird der Puffer geleert.
Poolbetrieb: m Speicherplätze vorgesehen, trifft $(m+1)$ -te Nachricht ein, wird aus Pool zufällig eine Nachricht ausgewählt und weiterverarbeitet

Nachrichten Puffern

- Prüfen der Absender. es müssen genügend viele Nachrichten von genügend vielen verschiedenen Absendern vorhanden sein.
- Behandlung von Latenzzeiten: Möglichkeit der Vergabe von Zeitschranken für die Weiterverarbeitung bzw. Verzögerung der Nachrichten.

Duplikaten Löschen

- Um Angriffe durch Nachrichtenwiederholung zu verhindern, muß zu Beginn noch geprüft werden, ob eine eingehende Nachricht bereits gemixt wurde. Da ein Mix deterministisch umkodiert, würde eine Nachrichtenwiederholung z.B. in einem nächsten Schub zur Ausgabe der gleichen umkodierten Nachricht führen. Somit wäre eine Verkettung von Ein- und Ausgabe möglich.

Duplikaten Löschen

- Duplikaten Prüfen
 - Speicherung bereits gesendeter Nachrichten in einer Datenbank
 - Vergabe von Zeitstempeln für die Nachrichten

Umkodierung

- Verwendet asymmetrisches Verschlüsselungsverfahren, public Key und private Key
- Notation:
 - M: Message
 - K: public Key
 - K^{-1} : private Key
 - R: Zufallszahl

Nachrichten Umsortieren

- Der Mix sendet die Nachrichten zeitlich versetzt und in umsortierter Reihenfolge weiter, um eine Rückverfolgung zum Sender der anonymen Nachricht mittels Nachrichteneingangs und Nachrichtenausgangsüberwachung des Mixes zu verhindern.

Mix in Mail System

- Mail System mit ein Mix

Ein Sender X sendet Nachrichten M via Mix1 an Empfänger Y mit Adress A_Y

Sender \rightarrow Mix1: $K_1(R_1, K_Y(R_0, M), A_Y)$

Mix1 \rightarrow Y: $K_Y(R_0, M), A_Y$

wobei R_0, R_1 die jeweils von Y und Mix1 generiert Zufallszahl

Mix in Mail System

- Problem: Sollten zwei genau identische Nachrichten beim Mix eintreffen, so wird die Unverkettbarkeit zwischen Sender und Empfänger verletzt.
- Lösung: Duplikanten Prüfung oder kombiniere Time-stamp mit Zufallszahl R

Mix Kaskade

- Warum mehr als ein Mix?

Die Schutzziel: Die kommunikations-
beziehung sollt auch vor Mix verbogen sein.

Ein einzelner Mix sowohl den Sender als
auch den Empfänger.

Mix Kaskade

- Sender -> Mix 1:

$K_1(R_1, K_2, (R_2, \dots, K_{n-1}(R_{n-1}(K_n(R_n, K_Y(R_0, M)), A_Y)))) \dots A_2)$

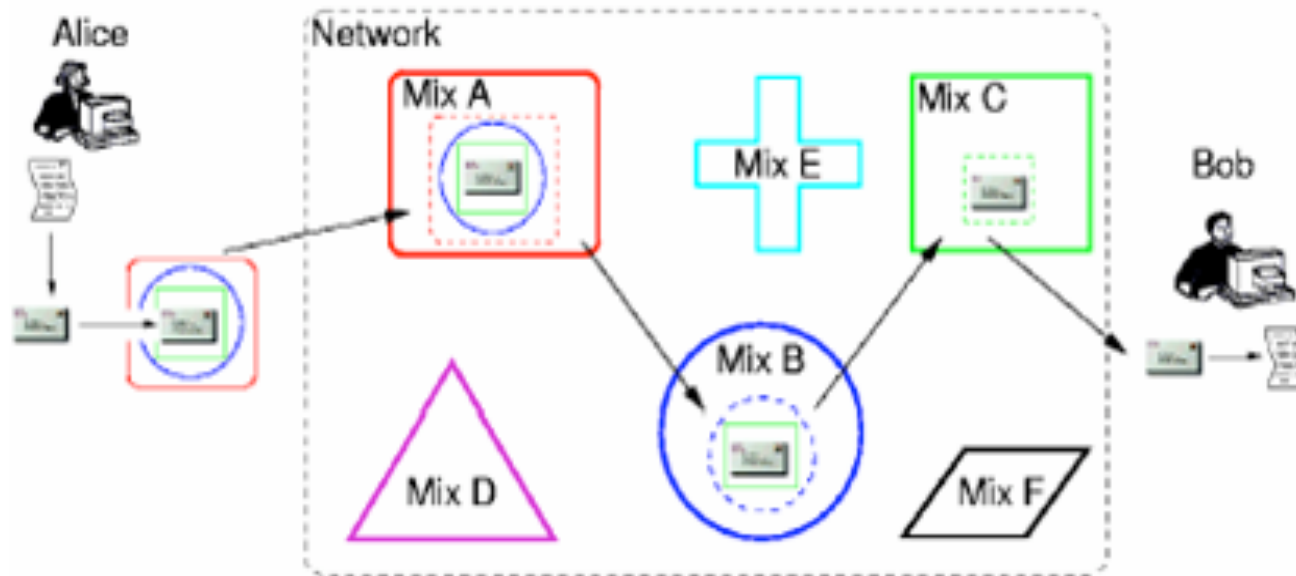
- Mix 1 -> Mix 2 :

$K_2, (R_2, \dots, K_{n-1}(R_{n-1}(K_n(R_n, K_Y(R_0, M)), A_Y)))) \dots A_3)$

.....

Mix Kaskade

- Mix $n \rightarrow Y$:
 $K_Y(R_n, M)$



Eigenschaften der Mix-Kaskade

- Nur der erste Mix kennt den Sender
- Nur der letzte Mix kennt den Empfänger
- Alle anderen kennen nur ihre beiden Nachbarn
- Vertraulichkeit wird durch Verschlüsselung erreicht: Verschlüsselung in “Zwiebelschalen” für jeden Mix

Längentreue Kodierung

- Da jeder Mix aus der weiterzuleitenden Nachricht den Teil entfernt, in dem seine Adresse enthalten ist, zumindest aber die Zufallszahl, die er nicht ausgeben darf, erfolgt eine Verkürzung der Nachricht auf ihrem Weg durch die Mixe.
- Rückschlüsse aufgrund der Verkürzung der Nachrichten fordert die *längentreu* Umkodierung.

Längentreue Kodierung

- Jeder Mix muss zufällige Bitketten in die Nachricht eingefügen, so daß die Länge erhalten bleibt.
- Sender -> Mix 1:
 $[K_1(R_1, A_2)], [R_1^{-1}(K_2(R_2, A_3))], \dots,$
 $[R_1^{-1} R_2^{-1} \dots R_{n-1}^{-1} K_n (R_n, A) \dots],$
 $[R_1^{-1} (R_2^{-1} \dots (R_n^{-1}(M_1)))] , \dots,$
 $[R_1^{-1} (R_2^{-1} \dots (R_n^{-1}(M_z)))]$

Längentreue Kodierung

- Mix 1 -> Mix 2:

$$[K_2(R_2, A_3)], [R_2^{-1}(K_3(R_3, A_4))], \dots,$$

$$[R_2^{-1}(R_3^{-1} \dots (R_{n-1}^{-1} K_n(R_n, A)) \dots)],$$

$$[R_2^{-1}(R_3^{-1} \dots (R_n^{-1}(M_1)))]], \dots,$$

$$[R_2^{-1}(R_3^{-1} \dots (R_n^{-1}(M_z)))]],$$

$$[R_1(J_1)]$$

Längentreue Kodierung

- Mix n -> Empfänger:
[M_1], [M_2], ..., [M_z],
[$R_n R_{n-1} \dots R_1(J_1) \dots$], ...,
[$R_n(J_n)$]

Rückadresse

- Wie kann Y eine Nachrichten zurück senden, wenn X vor Y anonym bleibt?
- Lösung: betten A_x in Nachrichten ein
- Format: $K_1(R_1, A_x), K_x$
wobei K_x vorläufige public Key von X,
 R_1 von X generiert Zufallszahl

Rückadresse

Beispiel:

- X -> Mix:

$K_1(R_1, K_Y(R_0, M_1), A_Y), K_1(R_1, A_X), K_X$

- Mix -> Y:

$K_Y(R_0, M_1), K_1(R_1, A_X), K_X$

- Y -> Mix:

$K_1(R_1, A_X), K_X(R_2, M_2)$

Rückadresse

- Mix \rightarrow X:

$$R_1(K_x(R_2, M_2))$$

Bemerkung:

- mit R_1 kann I/O Korrespondenz geschützt werden
- A_x ist in Nachrichten eingebettet
- die Rückantwort sieht ganz anderes als die originale Nachrichten

Rückadresse in Mix Kaskade

die Adress Teile:

- $X \rightarrow$ Mix 1:

$$K_1(R_1, K_2(R_2, \dots, K_{n-1}(R_{n-1}, K_n(R_n, A_x)) \dots)), \\ K_x(R_0, M)$$

- Mix 1 \rightarrow Mix 2:

$$K_2(R_2, \dots, K_{n-1}(R_{n-1}, K_n(R_n, A_x)) \dots), R_1(K_x(\\ R_0, M))$$

.....

Digital Pseudonyms

- Weitere Anwendungen vorgestellt von Chaum sind die sogenannte “*Digital Pseudonym*” und “*Elektronic Voting*”.
- Der public Key der teilnehmer wird als seine Digital Pseudonym gesehen.
- Ein Authority hat ein list von public Key.
- Teilnehmer stellt eine Anwendungsfrage an Authority anonym, eingebettet mit seinem public Key.

Digital Pseudonyms

- Der Authority vergleicht den Public Key mit der Einträge von dem Pseudonym-List und trifft die Entscheidung.
- Die Entscheidung wird mit *Return Adress* an dem Teilnehmer zurückgeschickt.

Elektronic Voting

- Nur registrierter Wähler darf an der Wahl teilnehmen, d.h. seiner public Key K muss auf dem Pseudonym-List stehen.
- Mit einem Mix, sieht der Stimmzettel so aus:
$$K_1(R_1, K, K^{-1}(C, V))$$
wobei K_1 public Key von Mix, V die Wahlstimme

Elektronic Voting

- Mit Mix Kaskade, hat der Stimmzettel die Form:

$$K_1(R_1, \dots, K_{n-1}(R_{n-1}, K_n(R_n, K, K^{-1}(C, V))) \dots)$$

Technik zur Verbesserung :

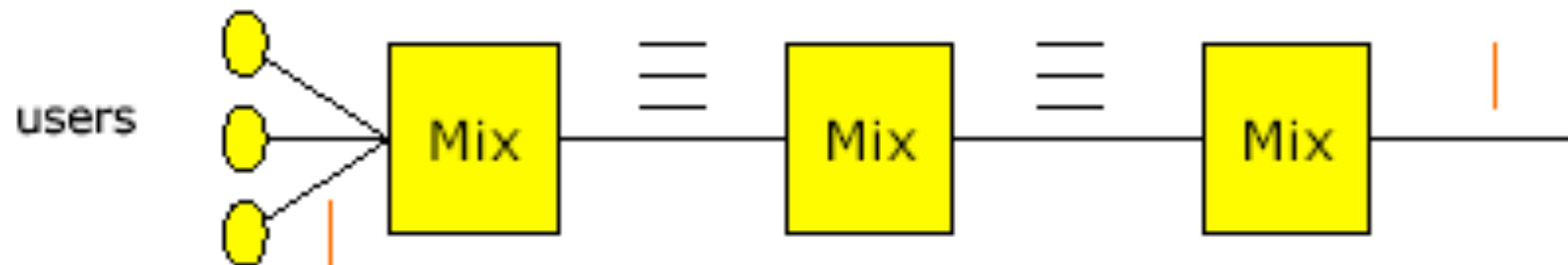
- Manchmal wird der Schub beim Nachrichten sammeln nicht voll, weil zu wenige Teilnehmer Nachrichten senden möchten
- Mann kann entweder warten, bis weitere Nachrichten eintreffen (führt zu weiteren Verzögerungen), oder Akzeptieren, dass Anonymitätsgruppe klein bleibt
- Lösung: Dummy traffic

Technik zur Verbesserung :

- **Dummy traffic:** Ein Nutzer sendet ständig Daten. Wenn er keine (verschlüsselten) Nachrichten zu senden hat, sendet er Zufallszahlen, die nicht unterscheidbar sind von echten verschlüsselten Nachrichten.
- Ziel: Verkehrsaufkommen in Situationen niedrigen Verkehrs künstlich erhöhen, um Anonymitätsgruppe zu vergrößern

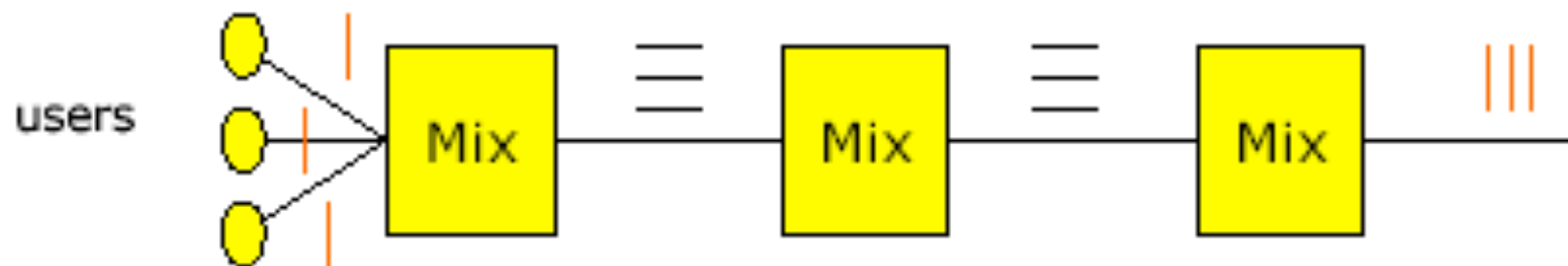
Technik zur Verbesserung :

- Dummy traffic nur zwischen Mixen reicht nicht aus





Technik zur Verbesserung :

- Dummy traffic muss Ende-zu-Ende generiert werden



Grenz von Mix

- durch drei Möglichkeiten wird eine Kommunikationsbeziehung aufgedeckt :
 -  Alle Mixe, die von einer Nachricht durchlaufen wurden, arbeiten zusammen.
 -  Alle anderen Sender und Empfänger der in allen Mixen gleichzeitig gemixten Nachrichten arbeiten zusammen.

Grenz von Mix

3. Ein Angreifer verfügt über unbegrenzte Rechenleistung (nicht komplexitätstheoretisch beschränkter Angreifer).

Anwendungsgebiet von Mix

- Mixe sind gut geeignet für wenig zeitkritische Dienste: E-Mail
- Für Echtzeitkommunikation (http, ftp) sind Modifikationen nötig:
 - Nachrichten sammeln führt zu starken Verzögerungen, da der Mix die meiste Zeit auf andere Nachrichten wartet

Anwendungsgebiet von Mix

- Nachrichtenlängen und Kommunikationsdauer variieren bei Verbindungsorientierten Diensten stark

Angriffe auf Mix-Netze

Replay-Angriffe:

- bereits bearbeitete Pakete werden wieder „eingespielt“, Angreifer sucht nach bekanntem Paket im Ausgabe-Schub und lernt so die Zuordnung
- Maßnahmen:
Gültigkeitsdauer für Pakete
Datenbank bearbeiteter Pakete

Angriffe auf Mix-Netze

N-1 Angriff

- Nachrichten von „ $n-1$ “ Nutzern werden durch Nachrichten des Angreifers ersetzt
- Angreifer erkennt die einzige ihm unbekannte Nachricht im Ausgabe-Schub und lernt so die Zuordnung

Angriffe auf Mix-Netze

- Maßnahmen:
 - Broadcast bearbeiteter Pakete, wobei jeder Nutzer überprüft, ob seins noch dabei ist
 - Ticketmethode: Pakete enthalten „Ticket“, an Hand dessen der Mix entscheiden kann, von wie vielen unterschiedlichen Nutzern die Pakete stammen

Angriffe auf Mix-Netze

DoS-Angriffe:

- Senden von (geschickt gewählten) „ungültigen“ Paketen
- Überlastung des Dienstes mit sinnlosen (zufällig gewählten) Paketen
- „Social engineering“ - Angriffe: Erzwingen der Einstellung des Dienstes durch Mißbrauch des Dienstes

Angriffe auf Mix-Netze

- Maßnahmen:
 - Aufdeckverfahren: Sender von „ungültigen“ Paketen kann ermittelt werden
 - eventuell Einsatz von Paketfiltern / Firewalls

Weitere Entwicklung von Mix

- 1991 ISDN-Mixes
- 1995 Mixmaster
- 1996 MIXes in mobile communications
- 1996 Onion Routing
- 1998 Stop-and-Go (SG) Mixes
- *2000 AN.ON/JAP Anonymizer*
- 2004 TOR