Privacy & PETs

Simone Fischer-Hübner

SWITS PhD course, 2012

1st Session, 3rd May 2012, KTH

Overview

I. Privacy - Definition
II. EU Directives & Basic Privacy Principles
III. Privacy Issues (LBS, Social Networks, RFID...)
IV. Introduction to PETs, Terminology
V. Mix-nets

I. Definition
Warren & Brandeis 1890

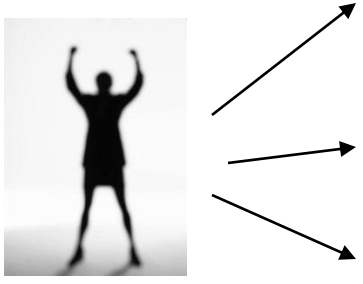
“The right to be let alone”

Definition- Alan Westin 1967

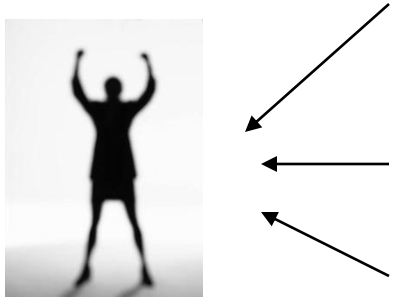
"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"

Privacy Dimensions

- Informational self-determination



- Spatial privacy



II. EU Directives

EU Data Protection Directive 95/46/EC

- **Objective:**
  - Protection of fundamental rights, freedom of individuals
  - Harmonsation of privacy legislation in Europe

- **Scope** (Art. 3): applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system.
  - Personal data: any information relating to an identified or identifiable natural person ('data subject')

  Does not apply for data processing for
  - defense, public/state security, criminal law enforcement
  - purely private or household activity (”household exemption”)

Basic Privacy principles
implemented in EU-Directive 95/46/EC

- Legitimisation by **law, informed consent** (Art. 7 EU Directive)
- **Data minimisation** and **avoidance** (Art. 6 I c,e)
  - Data must be adequate, relevant, not excessive & anonymised as soon as possible
- **Purpose specification** and **purpose binding** (Art. 6 I b)
  - ”Non-sensitive” data do not exist !

Example for Purpose Misuse

- Lidl Video Monitoring Scandal

Basic privacy principles (II)

- No processing of ”**special categories of data**” (Art. 8)
- **Transparency**, rights of data subjects
  - to be informed (Art.10)
  - to be notified, if data have not been obtained from the data subject (Art.11)
  - of access to data (Art.12 a)
  - of correction of incorrect data / erasure or blocking of illegally stored data (Art.12b)
  - to object to direct marketing (Art.14)

Basic privacy principles (III)

- Requirement of **security** mechanisms (Art.17)
- Sanctions (Art.24)
- Restricted personal data transfer from EU to third countries (Art. 25)

Basic privacy principles (IV)

- **Supervision** (Art. 28): Supervisory authorities
  - monitor compliance
  - act upon complaints
  - be consulted when drawing up data protection regulations
  - draw up regularly reports

Privacy Principles in Practice

Is it necessary to publish photos to the whole world (instead of having restricted access for parents, students, etc.)?

Purpose not well specified

Policy is not directly accessible and website did actually not exist!

KA

Kroppkärrs Skolområde

Samtycke till publicering av personuppgifter på Internet

Idag är Internet ett verktyg för information och kommunikation. Vi i vår verksamhet vill ha ett nyhetsflöde på varje enhets startsida för att visa aktuella bilder från vår verksamhet. Detta vill vi göra på www.karlstad.se på varje skola/förskola. Dessa bilder läggs ut i ett sådant format att det är svårt att förstora eller manipulera dem på annat sätt. Namn och annat som identifierar barnen publiceras bara om det finns ett syfte med detta.

Dessa uppgifter används enbart för registrering av samtycke i det administrativa systemet	
Barnets/elevens namn	Personnummer
Förskola/skola	Avdelning/klass
Vårdnadshavarens namn	
Vårdnadshavarens namn	

Jag tillåter att mitt barns foto och namn publiceras på www.karlstad.se.

Ja ☐ Nej ☐ Nej, jag har inte fått nog information ☐

Jag har också tagit del av informationen om hantering av personuppgifter på www.karlstad.se/bu/pul.

Underskrifter

EU Directive 2002/58/EC on privacy and electronic communications

- **Confidentiality of communications (Art.5):**
  - No interception/surveillance without the data subject's consent
  - Protection against cookies, spyware, web-bugs ("right to refuse")

EU Directive 2002/58/EC on privacy and electronic communications (cont.)

- **Traffic data (Art.6):**
  - Must be erased or made anonymous upon completion of transmission
  - Processing for billing purposes permissible
  - Processing for the purposes of value added services/marketing with the consent of the subscriber/user

EU Directive 2002/58/EC on privacy and electronic communications (cont.)

- **Location data other than Traffic data (Art.9):**
  - May only be processed when made anonymous, or with the informed consent of the user/subscriber
  - Where consent has been obtained, the user/subscriber must still have possibility of temporarily refusing the processing of location data

Problem: Also Location Data within Traffic Data can be very sensitive

EU Directive 2002/58/EC on privacy and electronic communications (cont.)

- **Unsolicited communications (Art.13):**

  Opt-in system for electronic mail for direct marketing (so-called "spam")

  Problem: US American CAN-SPAM Act of 2003 requires only Opt-out system, no SPAM legislation in most countries

Data Retention according to **EU Directives 2002/58/EC** and **2006/24/EC**

- **Art.15 of EU-Directive 2002/58/EC:**
  - allows member states to adopt laws for data retention for safeguarding security, defence, law enforcement
- **Data Retention Directive 2006/24/EC:**
  - Requires telco companies to retain traffic and location data for 6-24 months

Problems/Questions:

- Appropriate ?
  - Threat to online privacy: Traffic data contains mainly ”fingerprints” of non-criminal users
  - Criminals find ways ”around”
- Will anonymisation service providers be forced to collect more data than they would normally collect ?

New e-Privacy Directive, 2009/136/EC amending Directive 2002/58/EC

- Enacted on 18 Dec 2009, to be implemented by June 2011
- Main changes:
  - Privacy Breach Notification
  - Requirement to implement a security policy, adopt measures to restrict access to personal data, and to protect against data breaches
  - More strict SPAM legislation
  - Consent for the placement of cookies

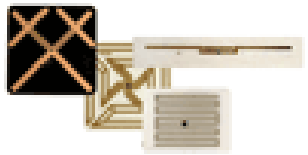
Newly proposed EU Data Protection Rules

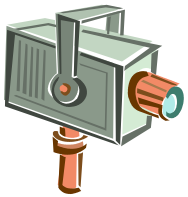
(Data Protection Regulation proposed 25 January 2012)

- **Single set of data protection rules**, valid across the EU, and if data are processed abroad by companies active in the EU market. **One DPA** in charge.
- **”Right to be forgotten”**
- Right to **”data portability”**
- **Easier exercising of data subject rights** (electronically, in relation to all recipients)
- **Explicitly** given **consent**, **more transparency** of data handling, easy-to-understand policies
- Increased **accountability,** privacy breach notification, **higher penalites** (up to 2% of global annual turnover)
- **Privacy impact assessment (PIA)**
- **Privacy by Design (PbD)**, Privacy by Default

III. Privacy Issues

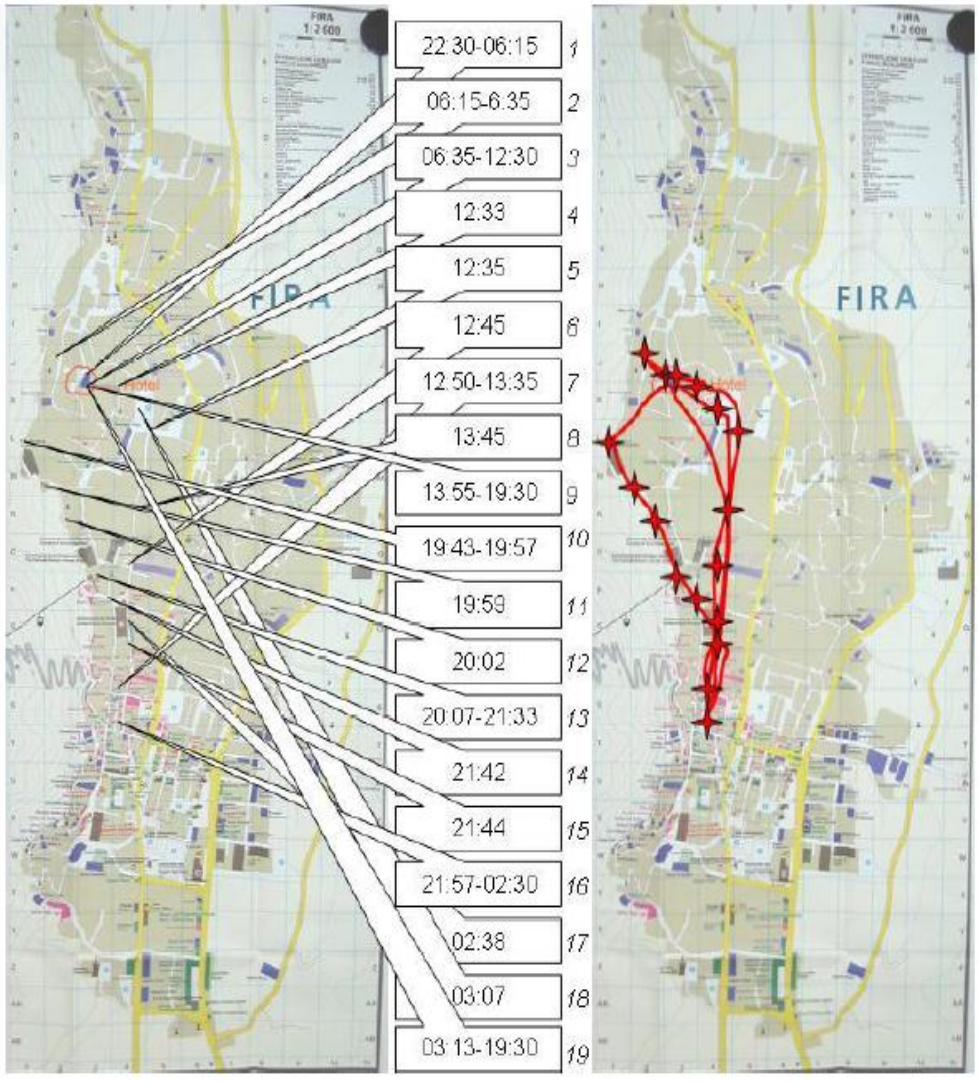
- Global networks, cookies, webbugs, spyware,...
- Location-based Services (LBS)
- Ambient Intelligence, RFID...
- Cloud Computing
- Social Networks
- Smart Grids
- Video Surveillance





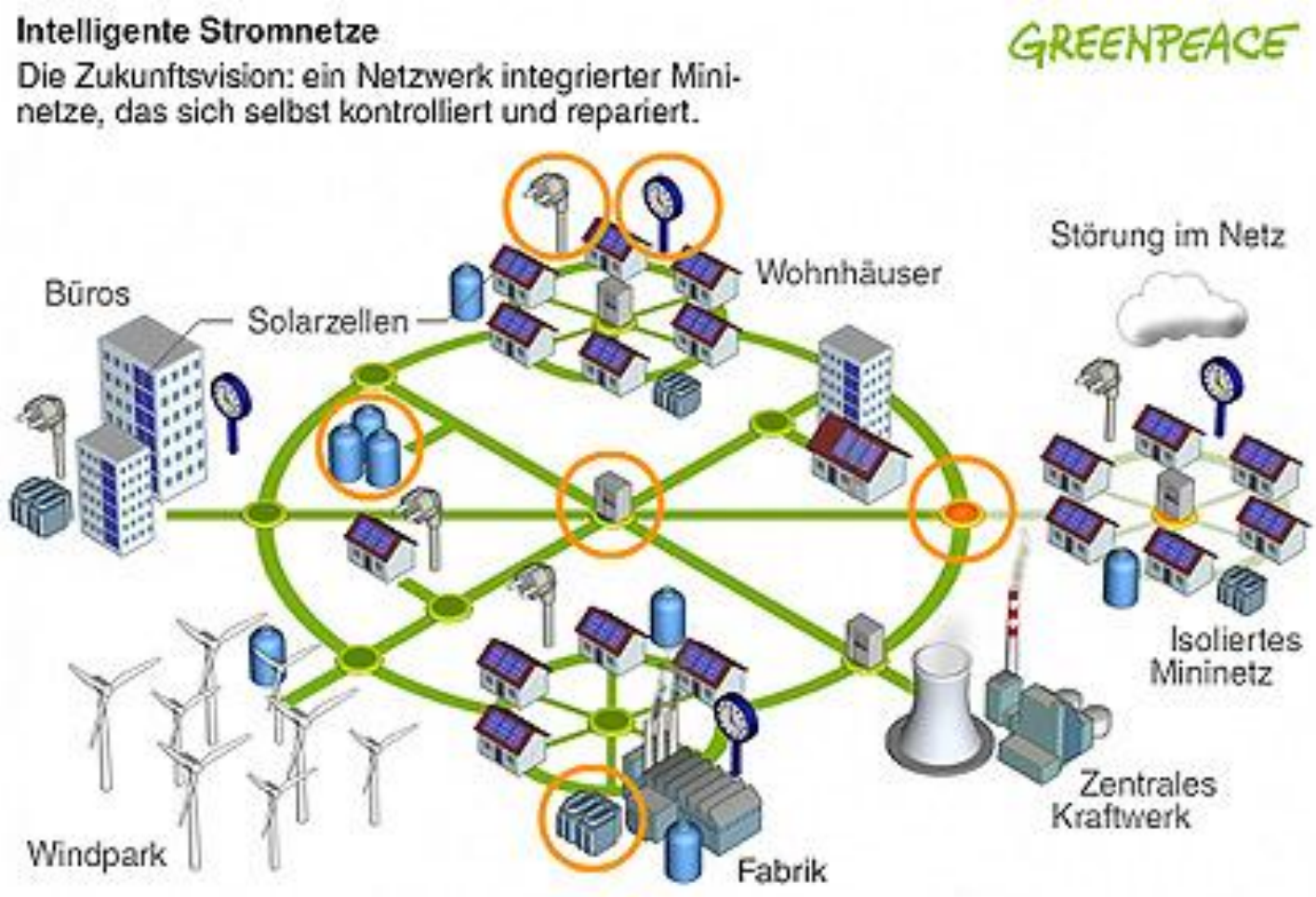
LBS - Risks

- Unsolicited tracking of user's position, movements
- Unsolicited Profiling
- Disclosure of the user's current context
- Disclosure of social networks



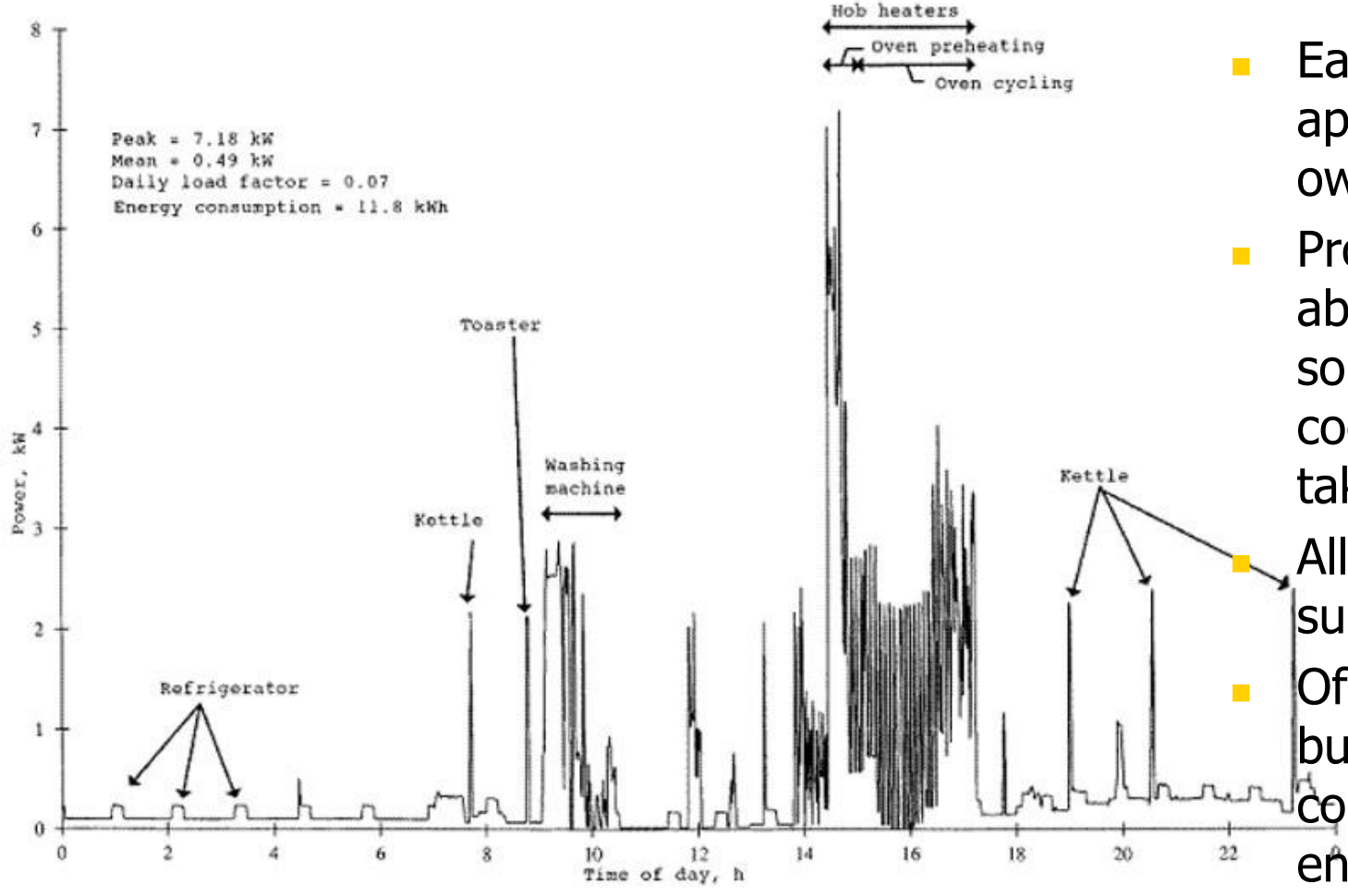
Source: Lother Fritsch & Rannenberg, GUF

Smart Grids



Picture source: Wikipedia

Smart Metering – Privacy Risks

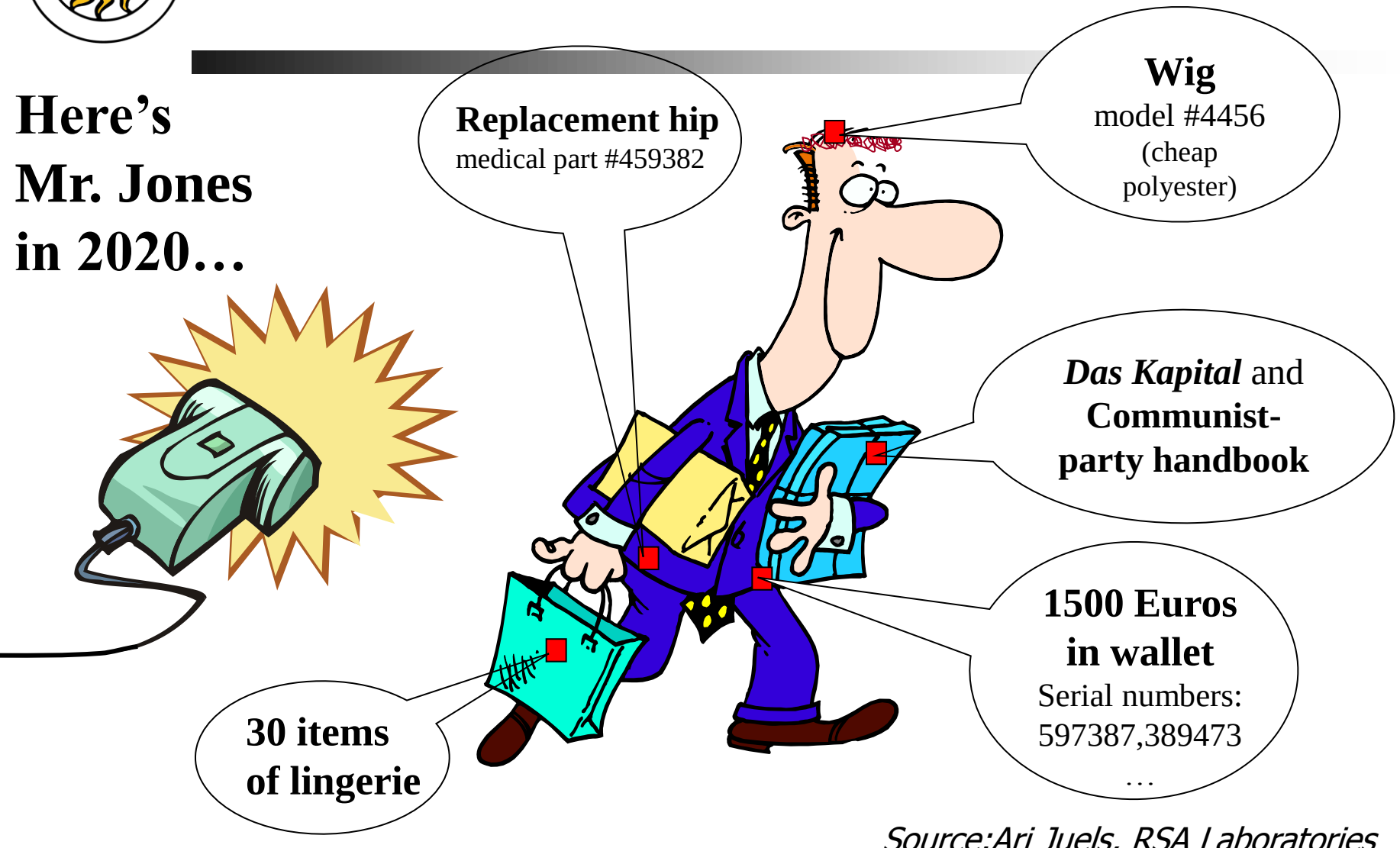


- Each electrical appliance has its own fingerprint
- Provides information about when someone is at home, cooks, watches TV, takes a shower, etc.
- Allows real-time surveillance
- Of interest for burglars, insurance companies, law enforcement,…

Source: Smart Metering & Privacy, Elias Leake Quinn, 2009

The RFID consumer privacy problem

Here's Mr. Jones in 2020…



Source:Ari Juels, RSA Laboratories

…and the tracking problem

- Mr. Jones pays with a credit card; his RFID tags now linked to his identity
- Mr. Jones attends a political rally; law enforcement scans his RFID tags
- Mr. Jones wins Turing Award; physically tracked by paparazzi via RFID

Privacy Risks of Social Networks

Uppdaterad 2007-10-25 19:01 Skriv ut Skicka

Enisa, det europeiska organet för nätverkssäkerhet, går i dag ut med en varning till dem som är med i nätverken på internet. Bland annat varnar man för att tagga, ansiktsidentifiera, sina vänner och anhöriga på bilder.

Facebook äger dig

"Det är ett slavkontrakt"

Samtliga 400 000 svenskar som registrerat sig på Facebook har skrivit över rättigheterna till sina bilder och hemligheter på det amerikanska företaget – för all evighet.

De har själva godkänt detta i ett 13-sidigt kontrakt

FACEBOOK ÄGER

- Dina mejl
- Dina bilder
- Dina intressen
- Dina filmer
- Dina kontaktuppgifter

- Intimate personal details about social contacts, personal life, etc.
- The Internet never forgets completely....
- Not only accessible by ”friends”

Freddi Staur (ID fraudster)

Identity Theft – ”Face Rape”

Politikers identitet stals på Facebook

KARLSTAD: "Plumpt och dumt"

Karlstadspolitikerna Robert Warholm (FP) och Lill Nilsson (V) har fått sina identiteter kapade på Facebook.
– I sitt eget namn kan skämta hur mycket man vill om mig. Men att göra det i mitt namn är att gå över gränsen, säger Robert Warholm.

”Anders Knape hade inga trosor på sig i dag”. Det är det senaste inlägget på vad man skulle kunna tro är kultur- och fritidsnämndens vice ordförande Robert Warholms personliga fansida på Facebook. I andra inlägg som har gjorts på sidan den senaste månaden förespråkar den påstådde Robert Warholm bland annat också barnaga.

Robert Warholms personliga fansida? Nej, sidan är en bluff. [Förstora]

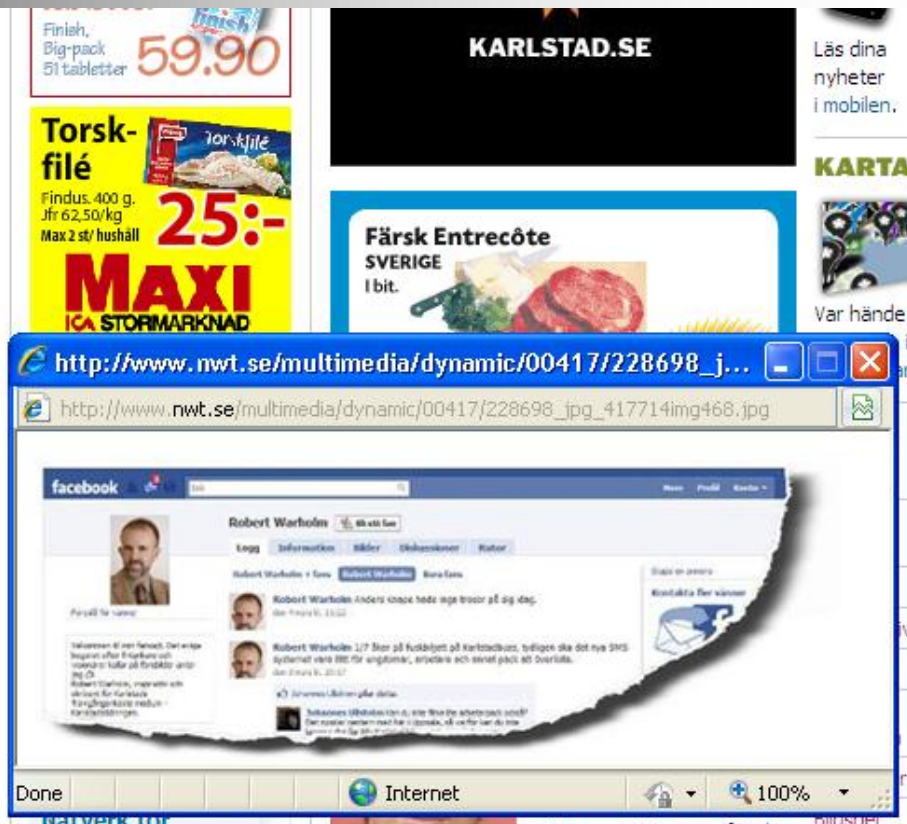
Men sidan är en bluff. Den verklige Robert Warholm har anmält det hela till Facebook, och även till Folkpartiets säkerhetsansvarige.

– Det är klart att det inte är bra att folk går in och stjäl andras identiteter. Samtidigt är det ju politiker som sticker ut som riskerar sådana här saker, så man får nästan ta det som en komplimang. Men naturligtvis ska det inte vara på det här viset, säger Robert Warholm till NWT.

Robert Warholm (FP) [Förstora]

Kultur- och fritidsnämndens ordförande Lill Nilsson har också fått sin identitet kapad. Någon har skapat en falsk profilsida i hennes namn. Den verkliga Lill Nilsson tar dock inte så allvarligt på det inträffade.

– Jag tycker att det är ganska oförargligt än så länge, det är så uppenbart bluff att det inte är något att göra



Privacy Risks of Social Networks – Social Network Analysis

Social Network Analysis/Profiling by:

- Employers
- Schools/Universities
- Tax authorities
- Law Enforcement
- Insurances
- Hackers
- .....

Art.29 Data Protection Working Party – Opinion 5/2009 on online social networking

- Who is the data controller?
  - SNS providers
  - Users ?
    - No: if "household exemption" applies
    - Yes:
      - If SNS is used beyond a purely personal/houshold activity (e.g., as a collaboration platform for a company)
      - When access to profile information extends beyond self-selected "friends" (e.g., access is given to all SNS members) – unless exemptions apply for journalistic purposes
- What are obligations of data controllers?
  - Appropriate technical and organisational security measures
    - SNS should offer privacy-friendly default settings
  - Informed consent by other individual concerned
  - Information to be provided by SNS
    - Information about the SNS identity, purposes (Art.10 EU Directive)
    - SNS users should be advised by SNS to obtain informed consent before uploading information/pictures about others

IV. Introduction to Privacy-Enhancing Technologies (PETs)

- Law alone is not sufficient for protecting privacy in our Network Society
- PETs needed for implementing Law
- PETs for empowering users to exercise their rights

Classifications of PETs

1. PETs for minimizing/ avoiding personal data
(-> Art. 6 I c., e. EU Directive 95/46/EC)
(providing Anonymity, Pseudonymity, Unobservability, Unlinkability)

- At communication level:
  - Mix nets, Onion Routing, TOR
  - DC nets
  - Crowds,…
- At application level:
  - Anonymous Ecash
  - Private Information Retrieval
  - Anonymous Credentials,…

2. PETs for the safeguarding of lawful processing
(-> Art. 17 EU Directive 95/46/EC)

- P3P, Privacy policy languages
- Encryption,…

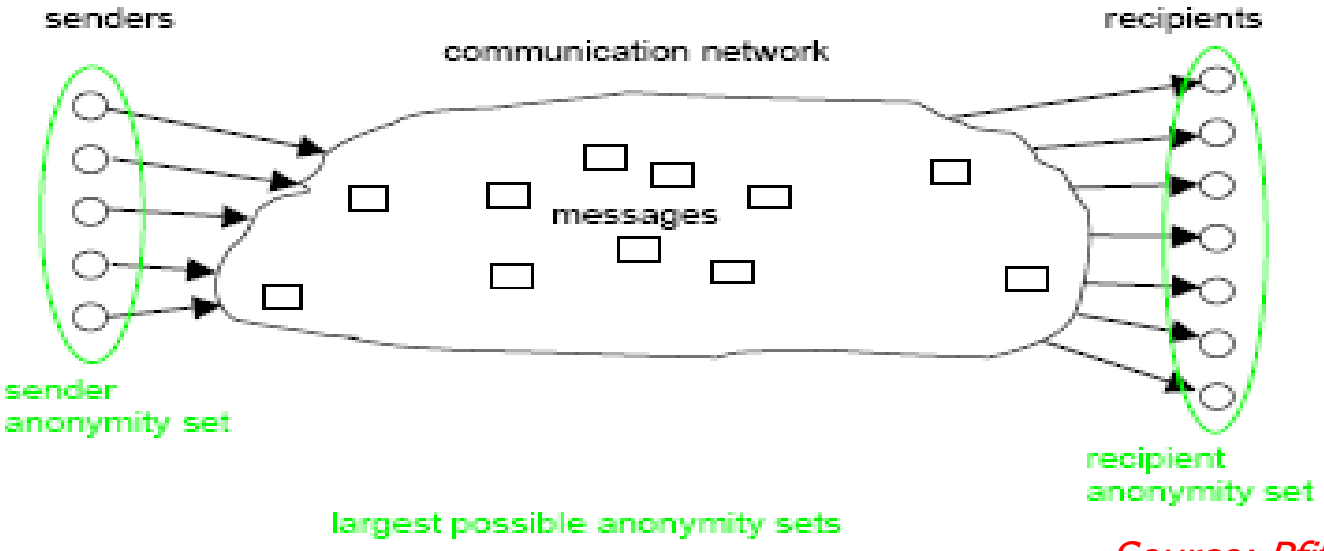
3. Combination of 1 & 2

- Privacy-enhancing Identity Management (PRIME, PrimeLife)

Privacy and Identity Management for Europe

Definitions - Anonymity

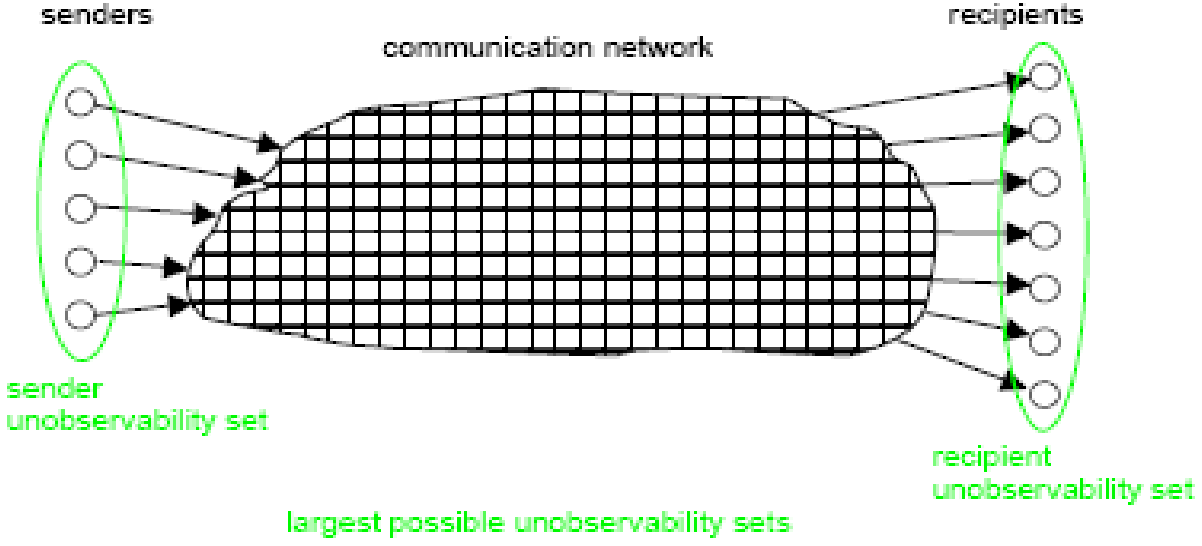
- *Anonymity:* The state of being not identifiable within a set of subjects (e.g. set of senders or recipients), the anonymity set



Source: Pfitzmann/Hansen

Definitions - Unobservability

- *Unobservability* ensures that a user may use a resource or service without others being able to observe that the resource or service is being used



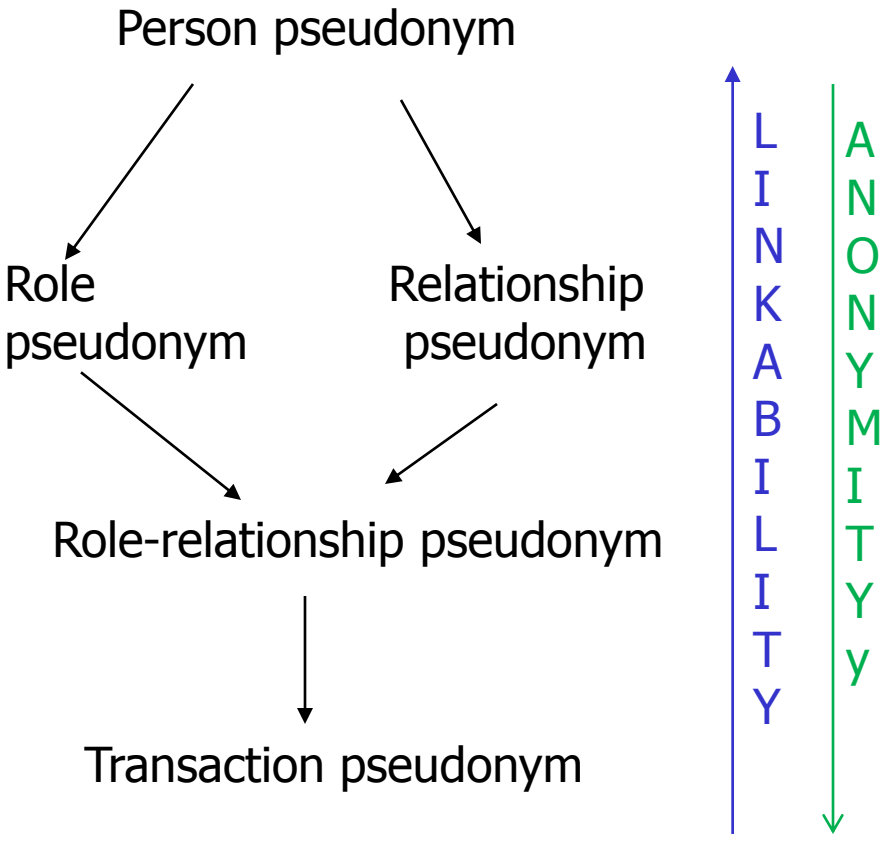
Source: Pfitzmann/Hansen

Definitions - Unlinkability

- *Unlinkability* of two or more items (e.g., subjects, messages, events):
  - Within the system, from the attacker's perspective, these items are no more or less related after the attacker's observation than they were before
- Unlinkability of sender and recipient (relationship anonymity):
  - It is untraceable who is communicating with whom

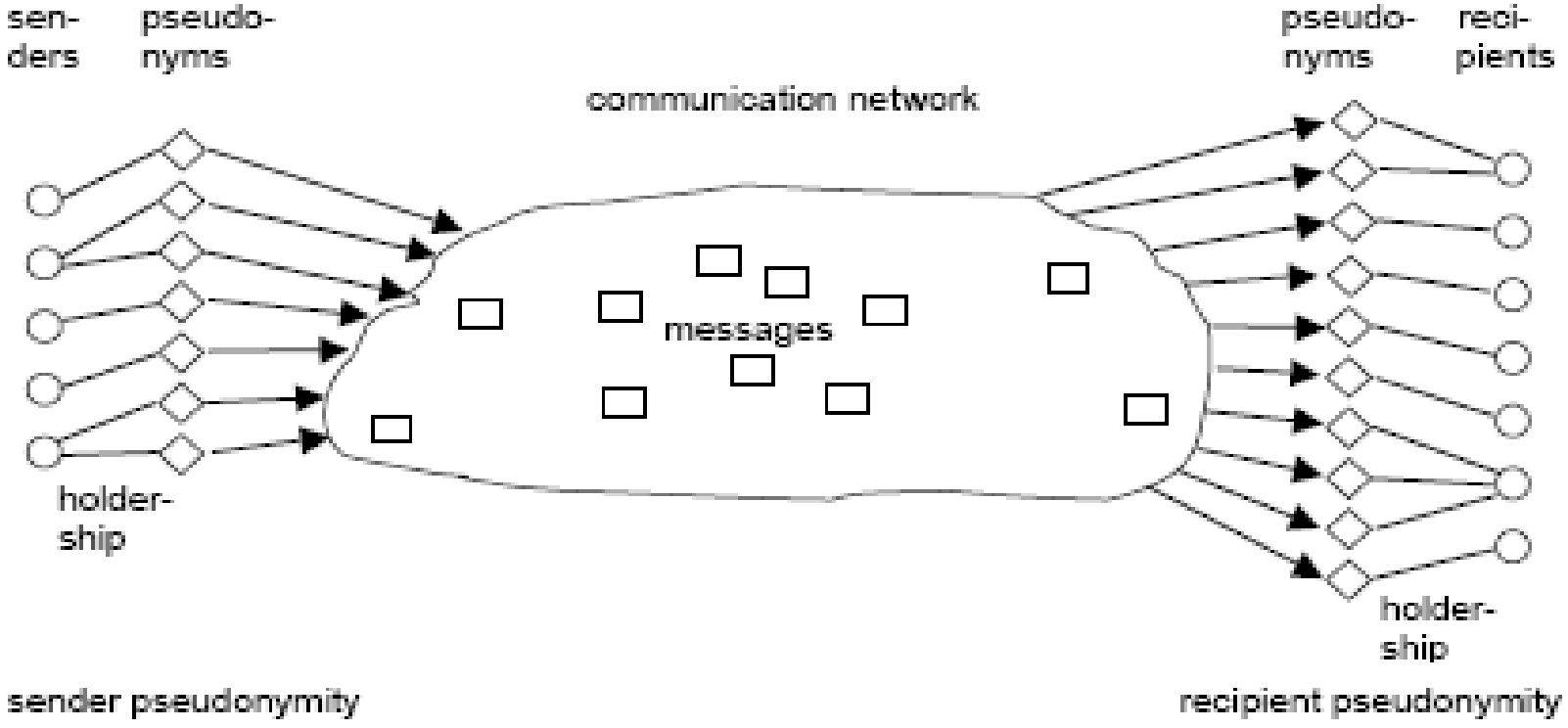
Definitions - Pseudonymity

- *Pseudonymity* is the use of pseudonyms as IDs
- Pseudonymity allows to provide both privacy protection ***and*** accountability



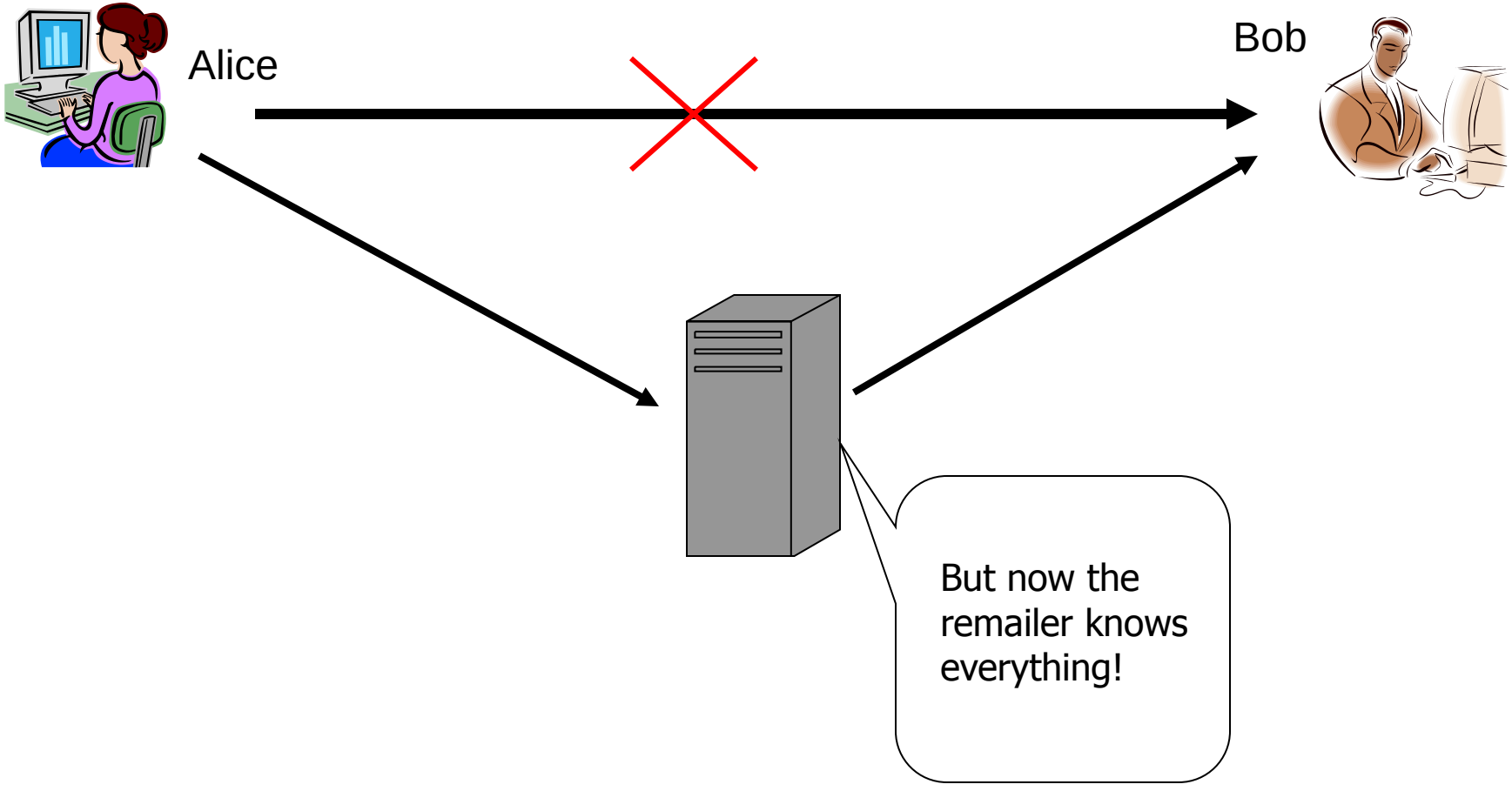
Source: Pfitzmann/Hansen

Definitions - Pseudonymity (cont.)

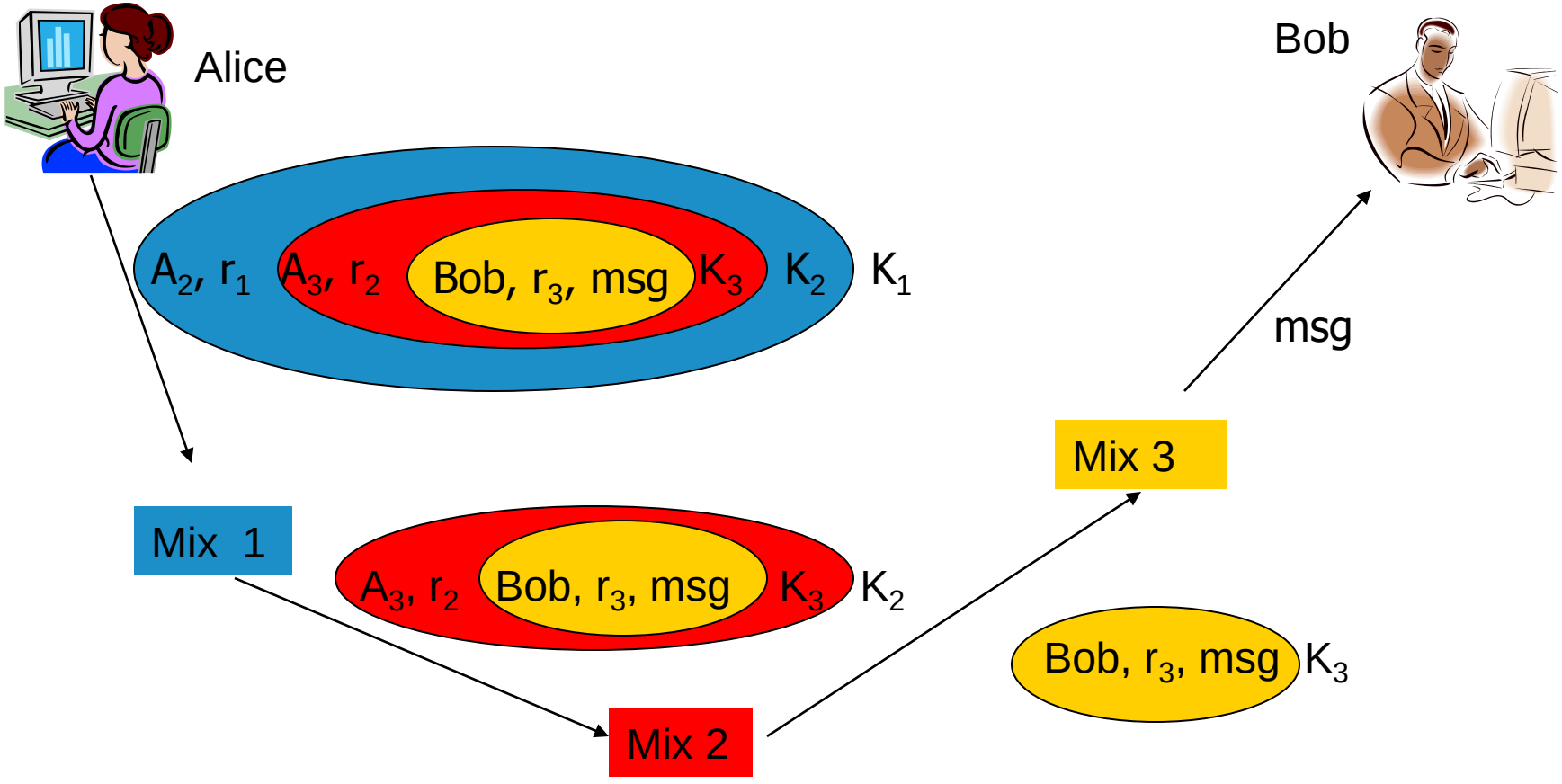


Source: Pfitzmann/Hansen

V. Anonymous Communication Technologies – Mix-nets

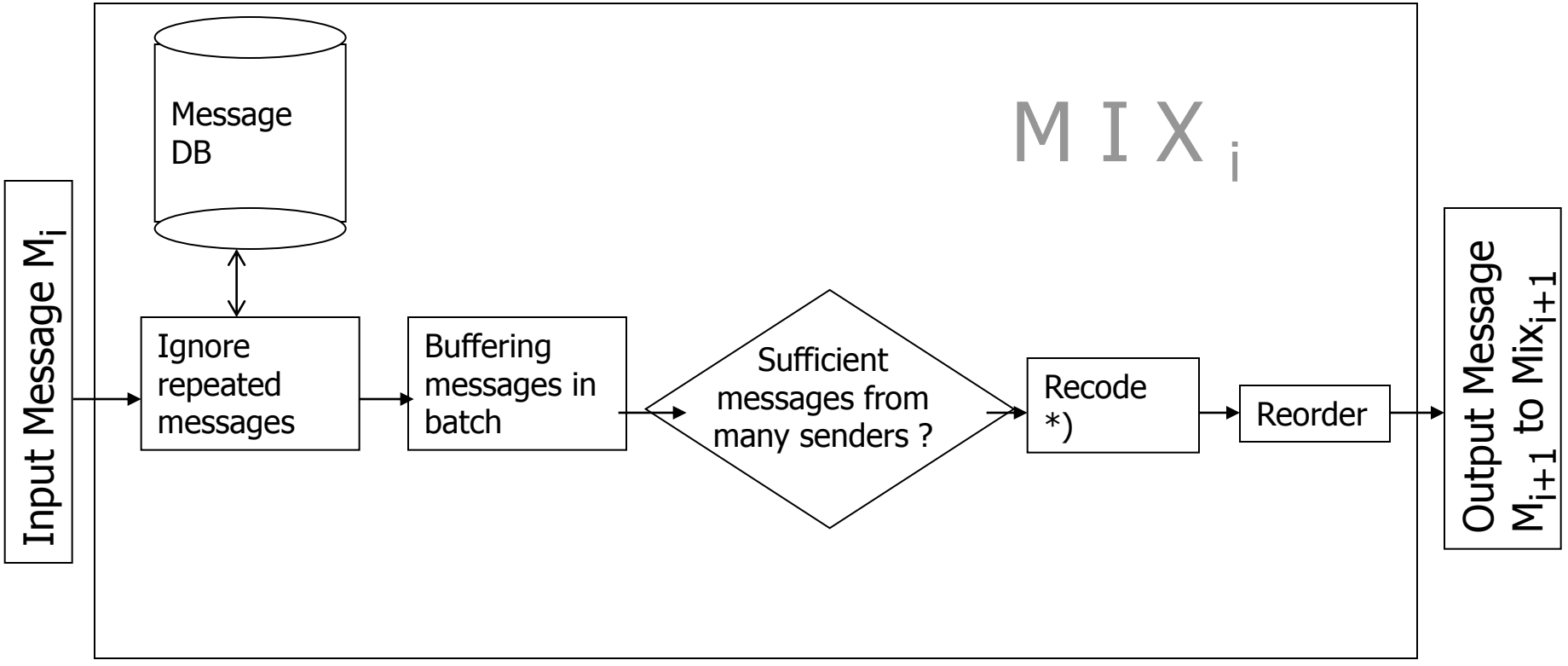


Mix-nets (Chaum, 1981)



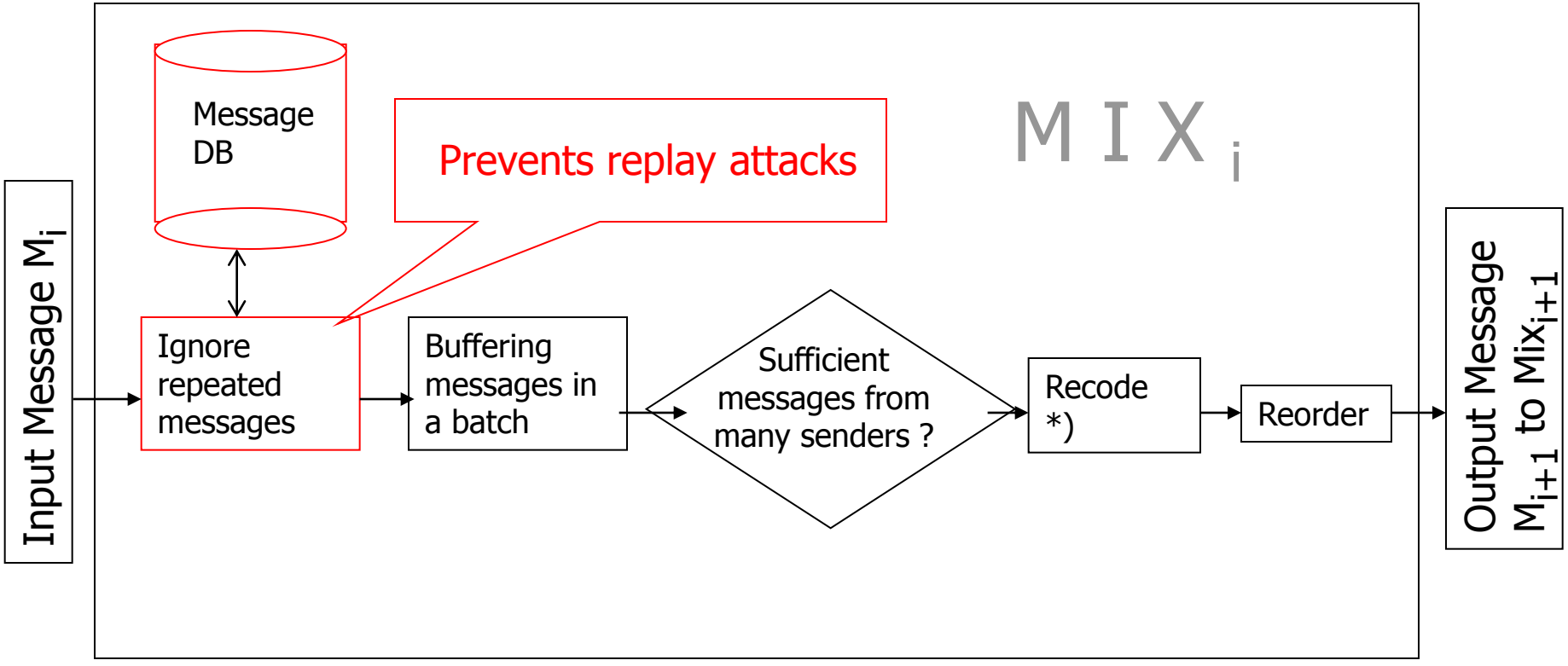
K_i: public key of Mix_i, r_i: random number, A_i: address of Mix_i

Functionality of a Mix Server (Mix_i)



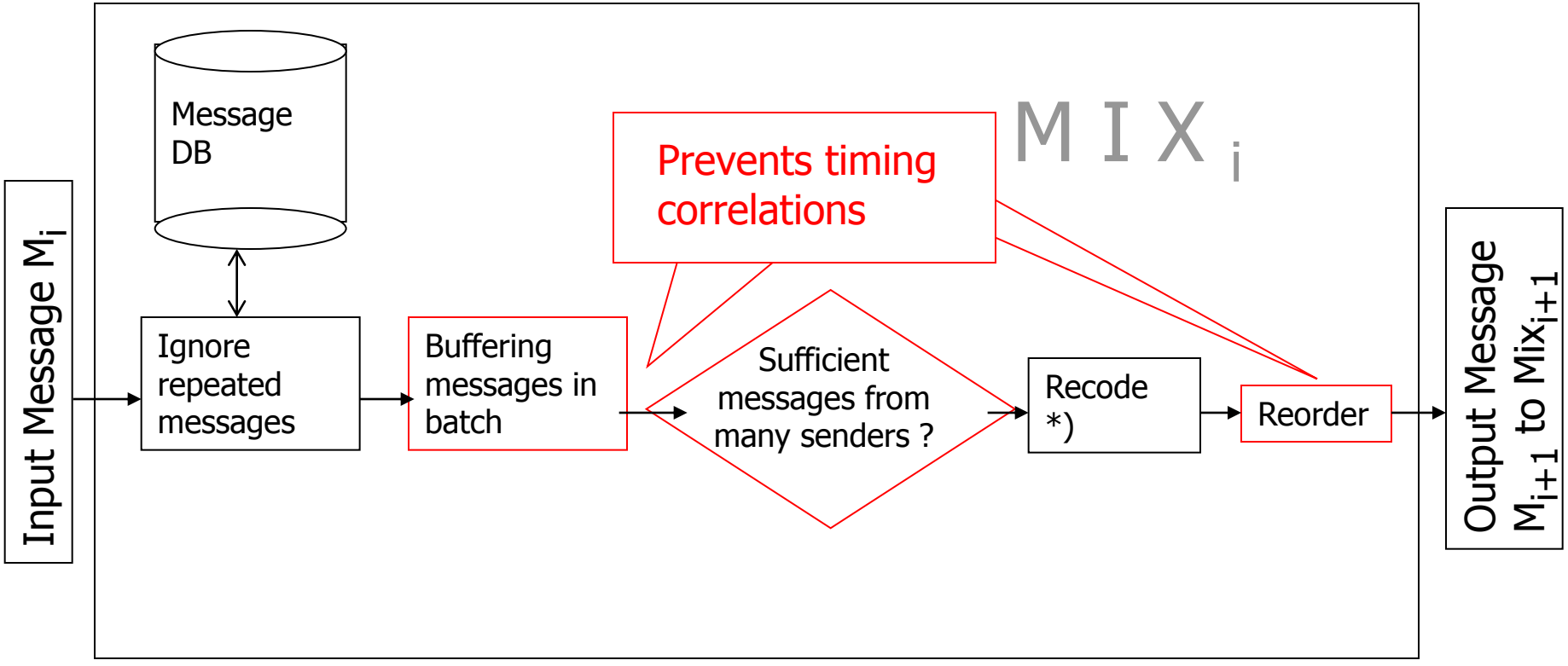
*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

Functionality of a Mix Server (Mix_i)



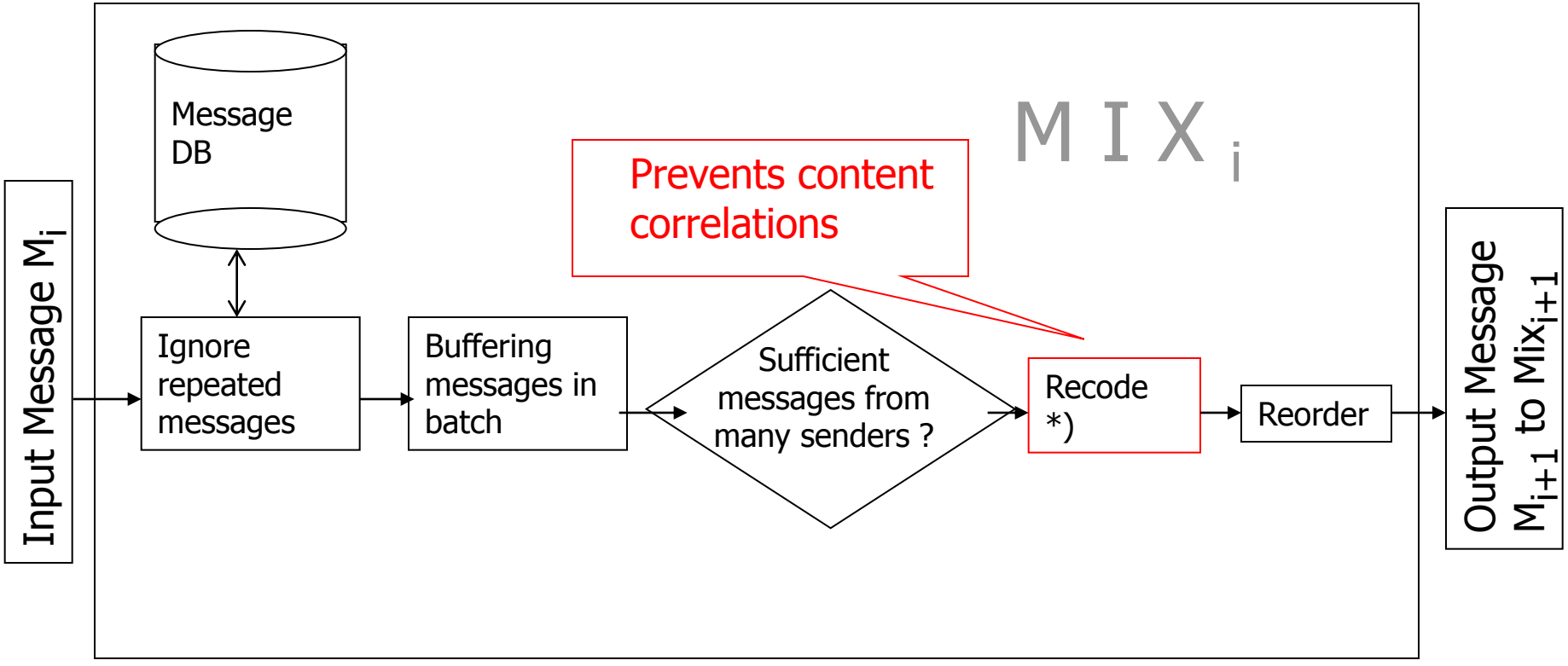
*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

Functionality of a Mix Server (Mix_i)



*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

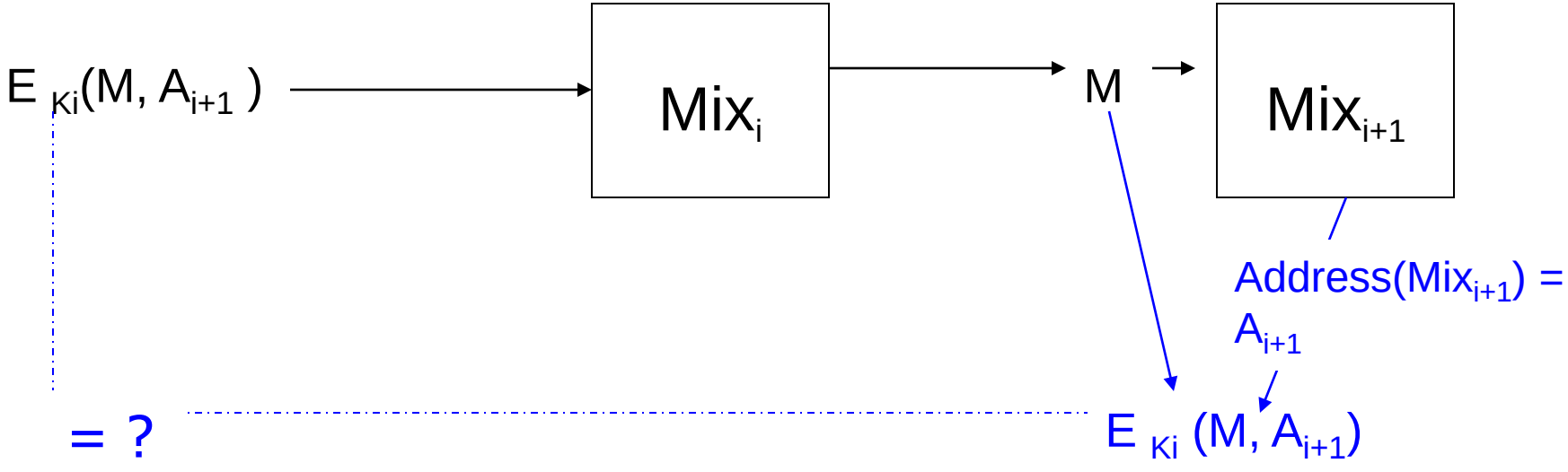
Functionality of a Mix Server (Mix_i)



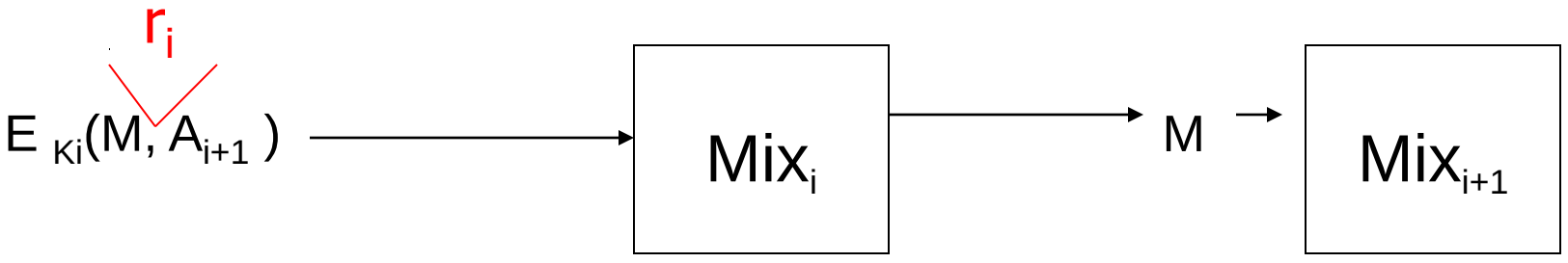
*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

Why are random numbers needed ?

If no random number r_i is used :



Why are random numbers needed ?



Sender Anonymity with Mix-nets

Sender (Alice) chooses Mix-Sequence Mix_1, ….., Mix_n, Mix_{n+1}.
Mix_{n+1} = recipient (Bob).

A_i (i =1..n+1): address of Mix_i
k_i (i=1..n+1): public key of Mix_i
z_i: random bit strings
M: message for recipient
M_i: message that Mix_i will receive

Sender prepares her message:

$$M_{n+1} = E_{Kn+1}(M)$$
$$M_i = E_{ki}(z_i, A_{i+1}, M_{i+1}) \quad \text{for } i=1\ldots n$$

and sends M_1 to Mix_1

Sender Anonymity with Mix-nets (cont.)

Sender (Alice)

$E_{k1}(z_1, A_2, M_2)$

Mix$_1$ Mix$_2$ Mix$_3$

Recipient (Bob)

$E_{kn+1}(M)$

Each Mix$_i$ decrypts:

$E_{ki}(z_i, A_{i+1}, M_{i+1})$ -> A_{i+1}: address of next Mix

M_{i+1}: $E_{ki+1}(z_{i+1}, A_{i+2}, M_{i+2})$, encoded message for Mix$_{i+1}$,

z_i: random string, to be discarded

and forwards M_{i+1} to Mix$_{i+1}$

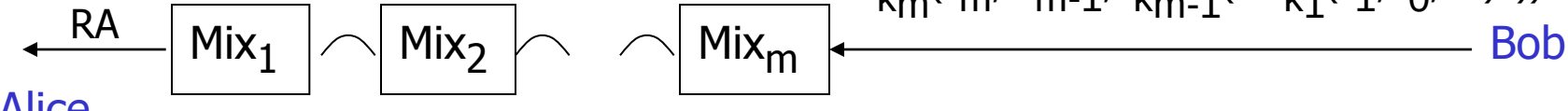
Recipient Anonymity with Mix-nets

Recipient Bob chooses Mix-Sequence Mix_1, ….., Mix_m.
Mix_0 = Sender Alice.
and creates anonymous return address RA:

$$R_{m+1} = e$$
$$R_j = E_{kj}(c_j, A_{j+1}, R_{j+1}) \quad \text{for } j=1..m$$
$$RA = (c_0, A_1, R_1)$$

e : label of return address
c_j: symmetric key, used by Mix_j to encode message on the return path
A_j (j =0..m): address of Mix_j
k_j (j=1..m): public key of Mix_j
z_j: random bit strings

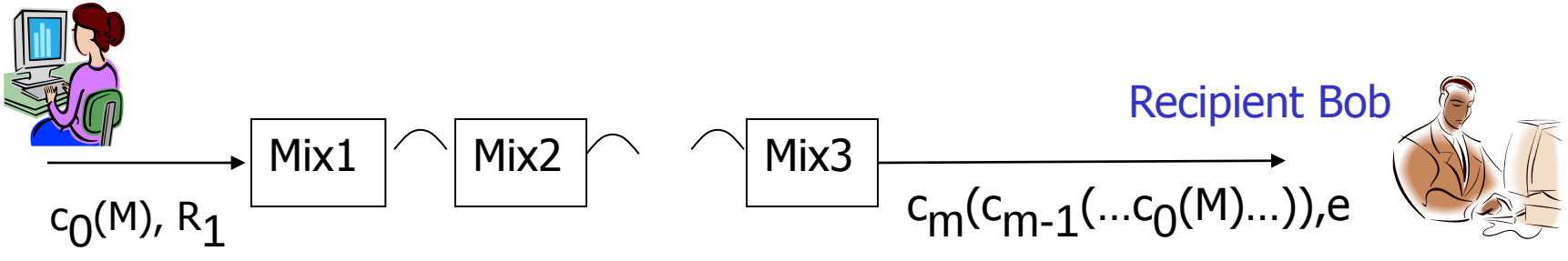
Recipient Bob sends RA anonymously to Sender Alice:



Recipient anonymity with Mix- nets (cont.)

Alice has received anonymous return address RA = (c_0, A_1, R_1)

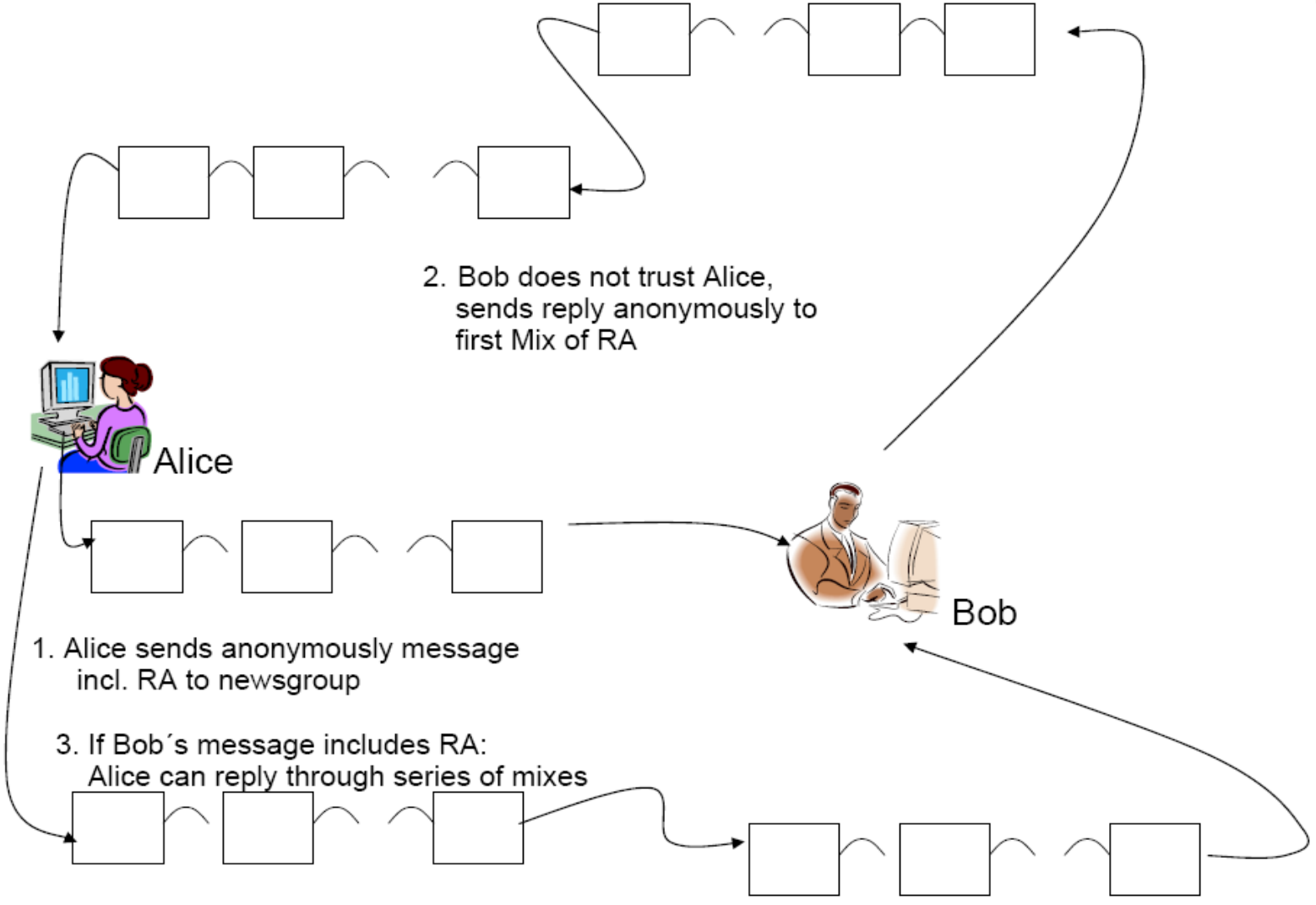
Sender Alice replies (without knowing recipient Bob):



Each Mix_j receives: $c_{j-1}(\ldots c_0(M)..)$, R_j,
decrypts: $R_j = E_{kj}(c_j, A_{j+1}, R_{j+1})$ -> (c_j, A_{j+1}, R_{j+1}),
forwards: $c_j(c_{j-1}(\ldots c_0(M)\ldots))$, R_{j+1} to Mix_{j+1}

Label e indicates Bob which $c_0,..,c_m$ he has to use to decrypt M

Two-Way Anonymous Conversation



Protection properties & Attacker Model for Mix nets

- Protection properties:
  - Sender anonymity against recipients
  - Recipient anonymity against senders
  - Unlinkability of sender and recipient
- Attacker may:
  - Observe all communication lines
  - Send own messages
  - Delay messages
  - Operate Mix servers (all but one...)
- Attacker cannot:
  - Break cryptographic operations
  - Attack the user's personal machine

Questions?

Backup Slides

(in case that there will be time left)

Length-preserving Coding
(for preventing message tracing by decreasing sizes)

Messages are sent through Mix sequence $Mix_1,\ldots, Mix_m$.
Each message has fixed length of b blocks.

Creation of return address:
R_{m+1} = [e] ([ ] = block limits)
$R_j = [\, k_j\,(c_j, A_{j+1})], c_j(R_{j+1})$
$j=1,..,m$
e: label , c_i: symmetric keys,

k_i: public keys, d_i: private keys of Mix_i

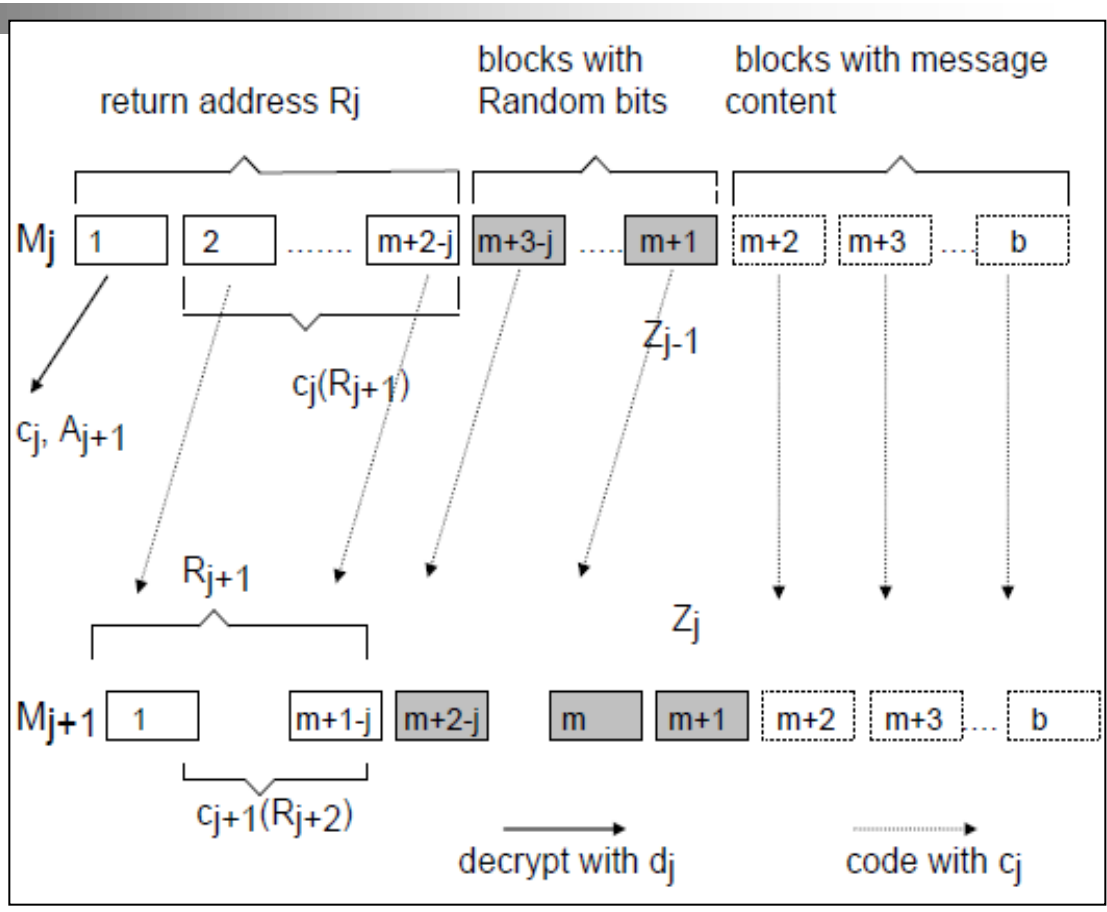


Figure according to Pfitzmann

Each Mix_j decrypts first block $k_j(c_j, A_{j+1})$ -> c_j, A_{j+1}, deletes first block, encrypts rest of M_j with c_j, inserts Z_j before message blocks, forwards M_{j+1} to Mix $_{j+1}$

Length-preserving Coding providing Sender Anonymity

Recipient does not know symmetric keys $c_1,..,c_m$

-> Sender has to encrypt message with all c_i and to create R_1

Sender creates H_1MC_1 with (MC: message content)

$$H_1 = R_1$$
$$MC_1 = c_1(c_2...(c_m(k_{m+1}(MC)))..)$$

k_{m+1}: public key of recipient

Each Mix_i *decrypts* message blocks with c_i

Lehgth-preserving Coding providing Recipient Anonymity

Sender does not know symmetric keys $c_1,..,c_m$

Sender receives RA = (c_0, A_1, R_1), encrypts MC with c_0, and thus creates H_1MC_1 with

$H_1 = R_1$
MC1 = c_0(MC)

Each Mix_i *encrypts* message blocks with c_i