Privacy & Privacy-enhancing Technologies (PETs)

Simone Fischer-Hübner

COINS PhD Seminar 2013

Finse, 22nd April 2013

PriSec Research @ KAU - Related Projects

- EU FP7 IP **A4Cloud** (2012-2016)
- EU FP7 FET IP **Smart Society** (2013-2016)
- Google Research Award projects **”Usable Privacy & Transparency”** (2011-2013)
- **U-PrIM** project funded by KK-Foundation (in cooperation with Nordea & Gemalto, 2011-2012)
- **PETweb II** funded by NFR/Norway (2009-2013)
- Swedish IT Security Network (**SWITS**) funded by MSB
- **Towards Blocking-Resistant Communication on the Internet**, funded by Internetfonden

Previous EU projects: EU FP7 IP **PrimeLife,** FP6 projects PRIME, FiDIS, Bugyo,...

Overview

I. Privacy - Definition
II. EU Directives & Basic Privacy Principles
III. Privacy Issues
IV. Introduction to PETs & PbD
V. Anonymous Communication
VI. PrimeLife PETs

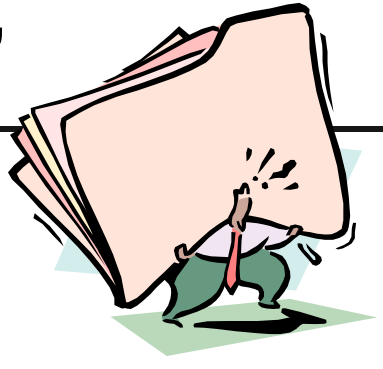
I. Definition
Warren & Brandeis 1890

"The right to be let alone"

HARVARD LAW REVIEW

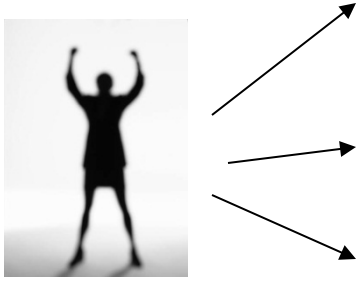
Definition- Alan Westin 1967

"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"

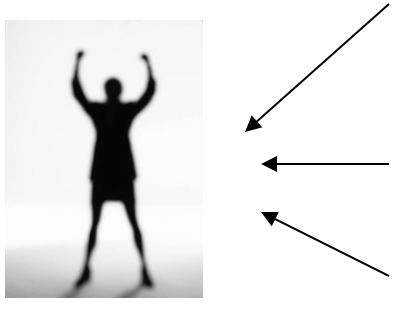


Privacy Dimensions

- Informational self-determination



- Spatial privacy



II. EU 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 ☐

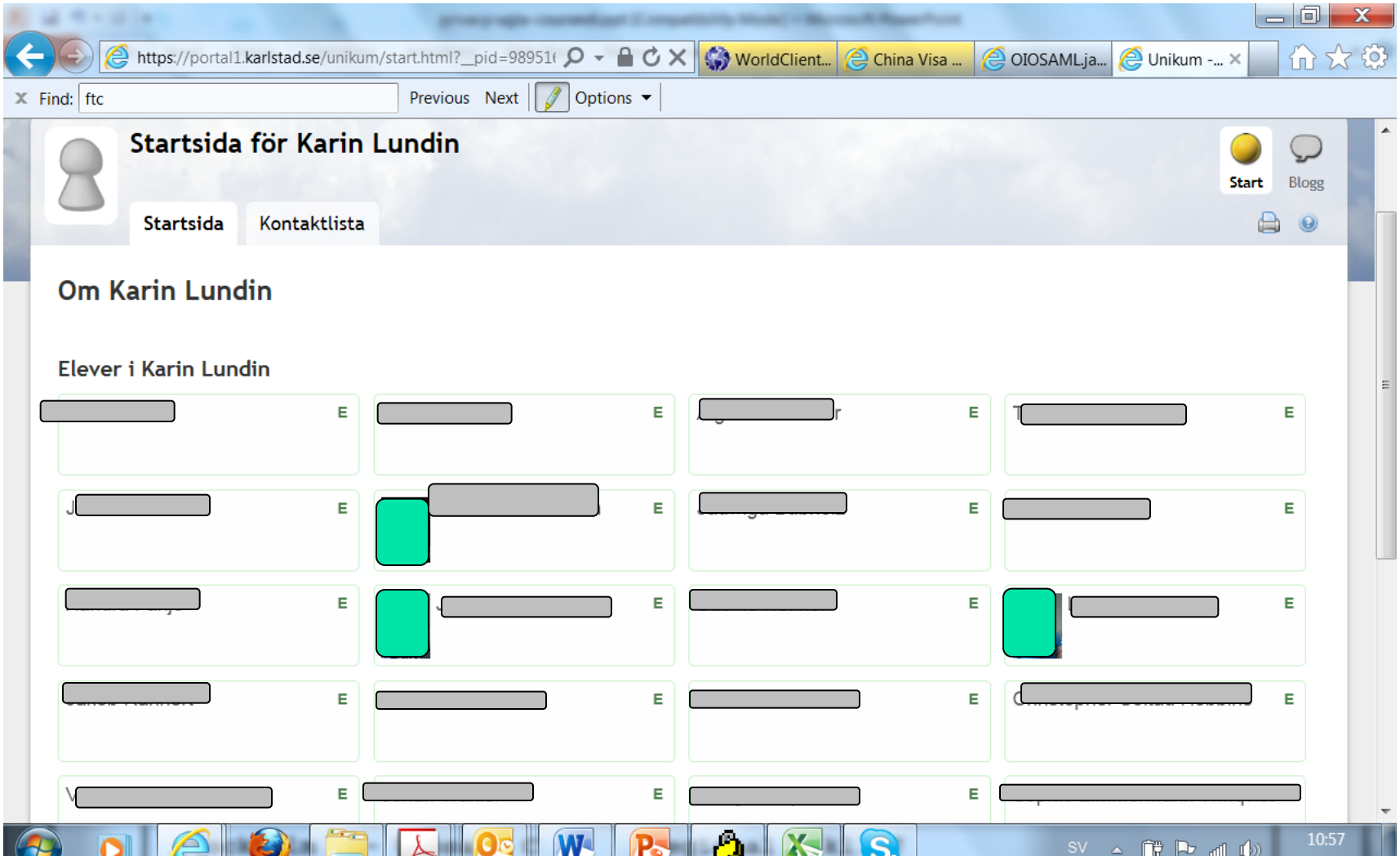
Jag har också tagit del av informationen om hantering av personuppgifter på www.karlstad.se/bu/pul.

Underskrifter

Unikum - Authentication

One factor authenticaton regarded as too insecure

Information about ethnic origin in Unikum



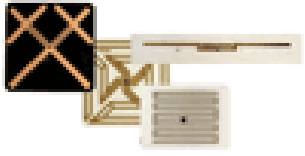
Newly proposed EU Data Protection Rules

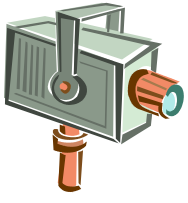
(Data Protection Regulation proposed 25 January 2012)

- **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

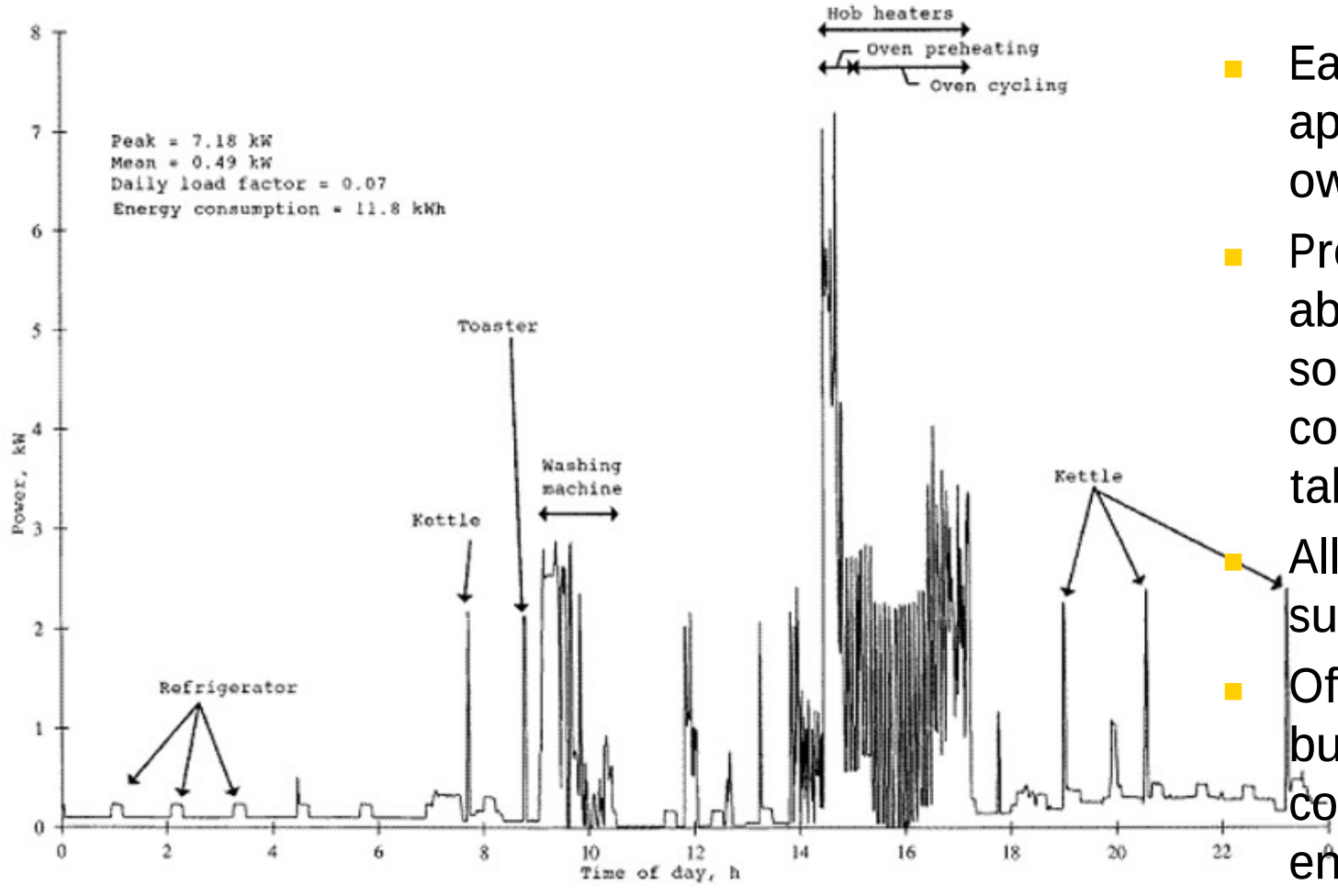
III. Privacy Issues

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





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

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
- .....

Mail Online

Facebook to switch off controversial facial recognition feature following data protection concerns

By DAILY MAIL REPORTER

German state bans Facebook 'Like' button

Posted on August 22, 2011 - 05:20 by **Emma Woollacott**

The German state of Schleswig-Holstein has ordered organizations to remove the Facebook 'Like' button from their websites and shut down fan pages.

The Independent Center for Privacy Protection (ULD) says it's taken the measure because information on 'Likes' is sent back to Facebook in the US and used to create a

IV. Introduction to PETs & PbD

- Law alone cannot sufficiently protect privacy
- PETs can implement legal privacy principles by technology
- Privacy by Design (PbD): ”Build it in” – as users have limited IT skills
  - Conduct PIA
  - Incorporate Privacy Protection into the overall system design (instead of using ”patches”)
  - Data minimisation as a key principle
  - ”Positive sum”

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,...

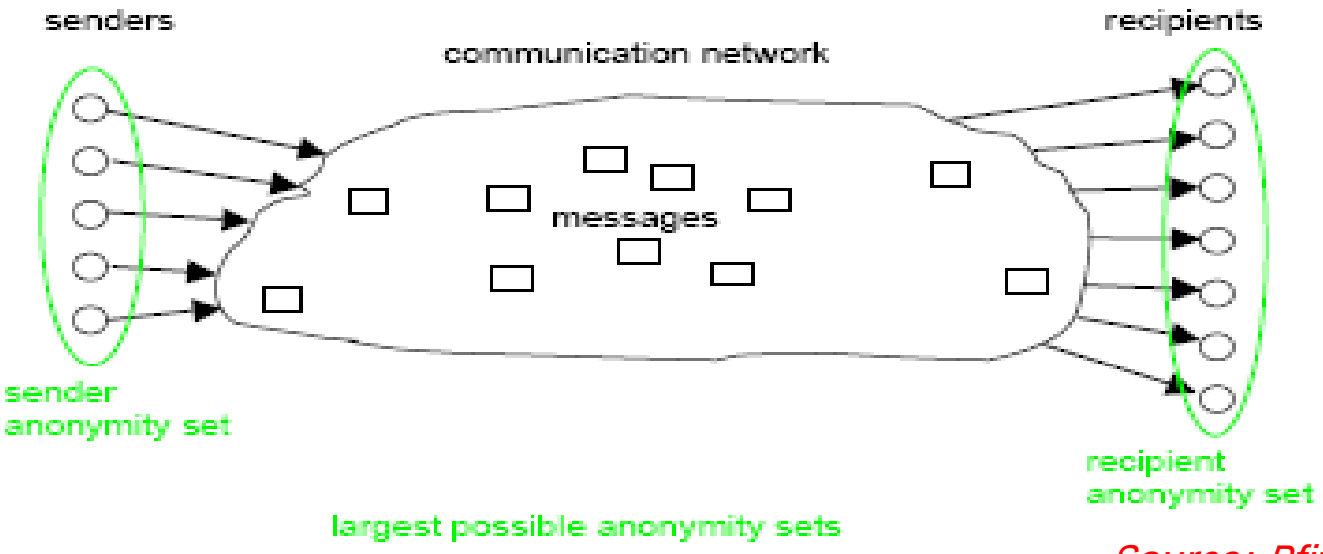
3. Combination of 1 & 2

- Privacy-enhancing Identity Management (PRIME, PrimeLife)

PRIME
Privacy and Identity Management for Europe

Definitions - Anonymity

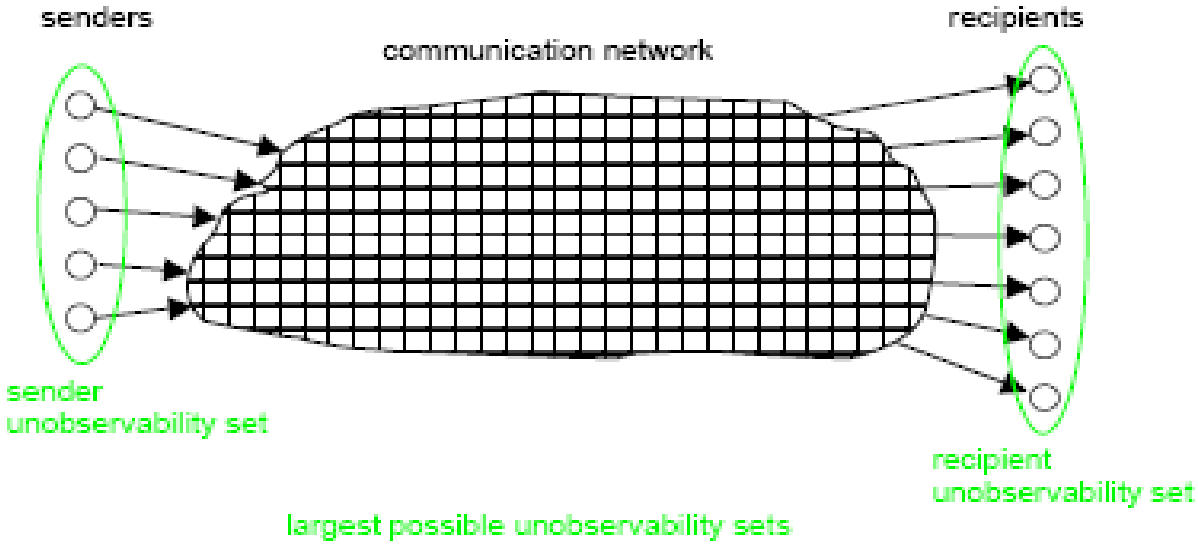
- *Anonymity:* The state of being not identifiable within a set of subjects (e.g. set of senders or recipients), the anonymity set



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



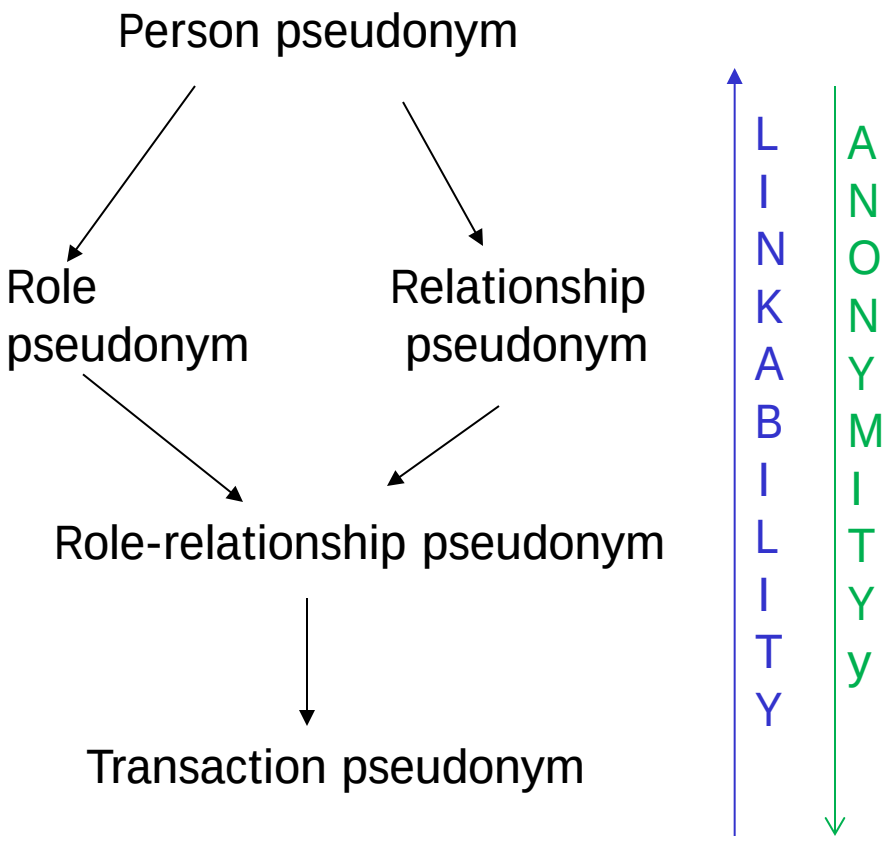
Source: Pfitzmann/Hansen

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

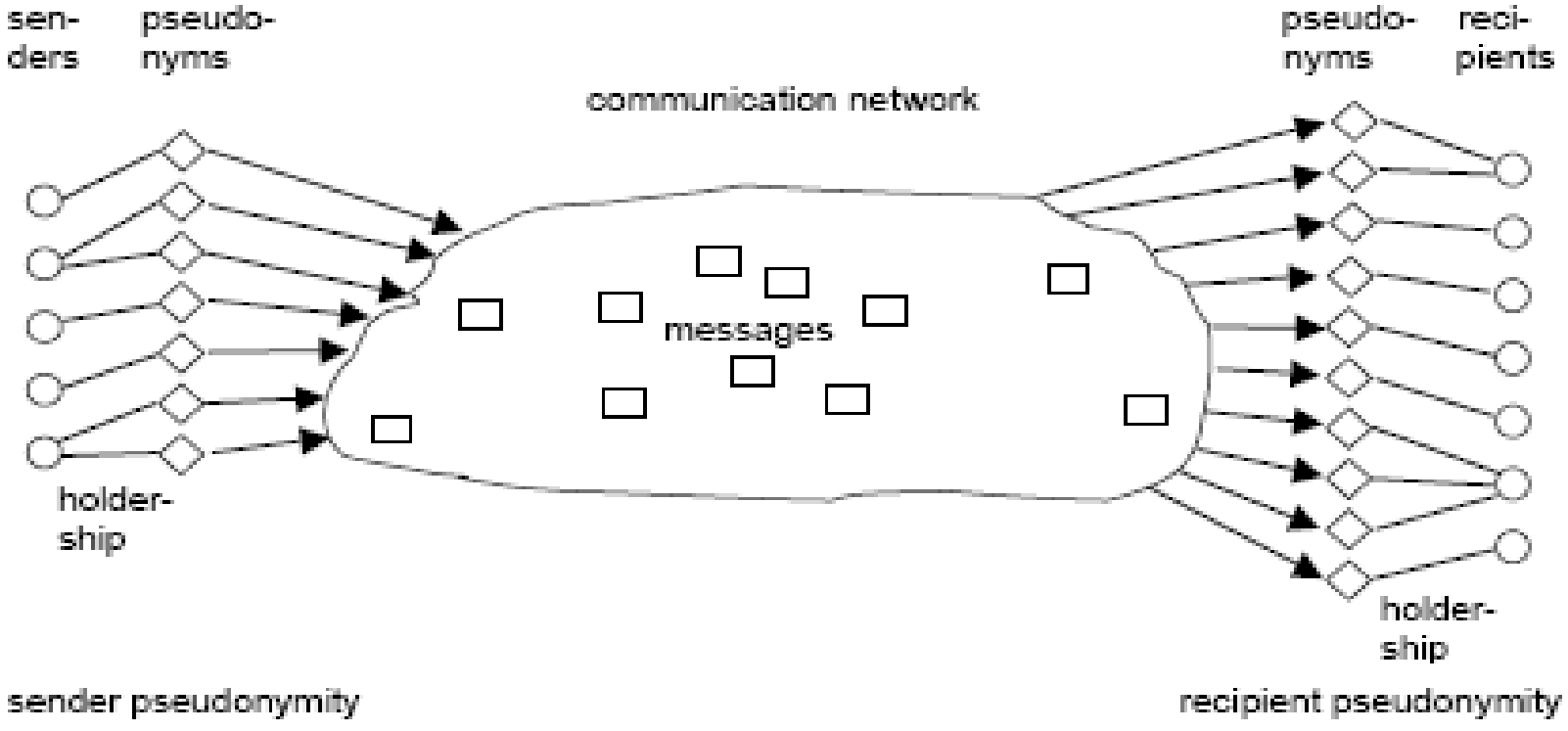
Definitions - Pseudonymity

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



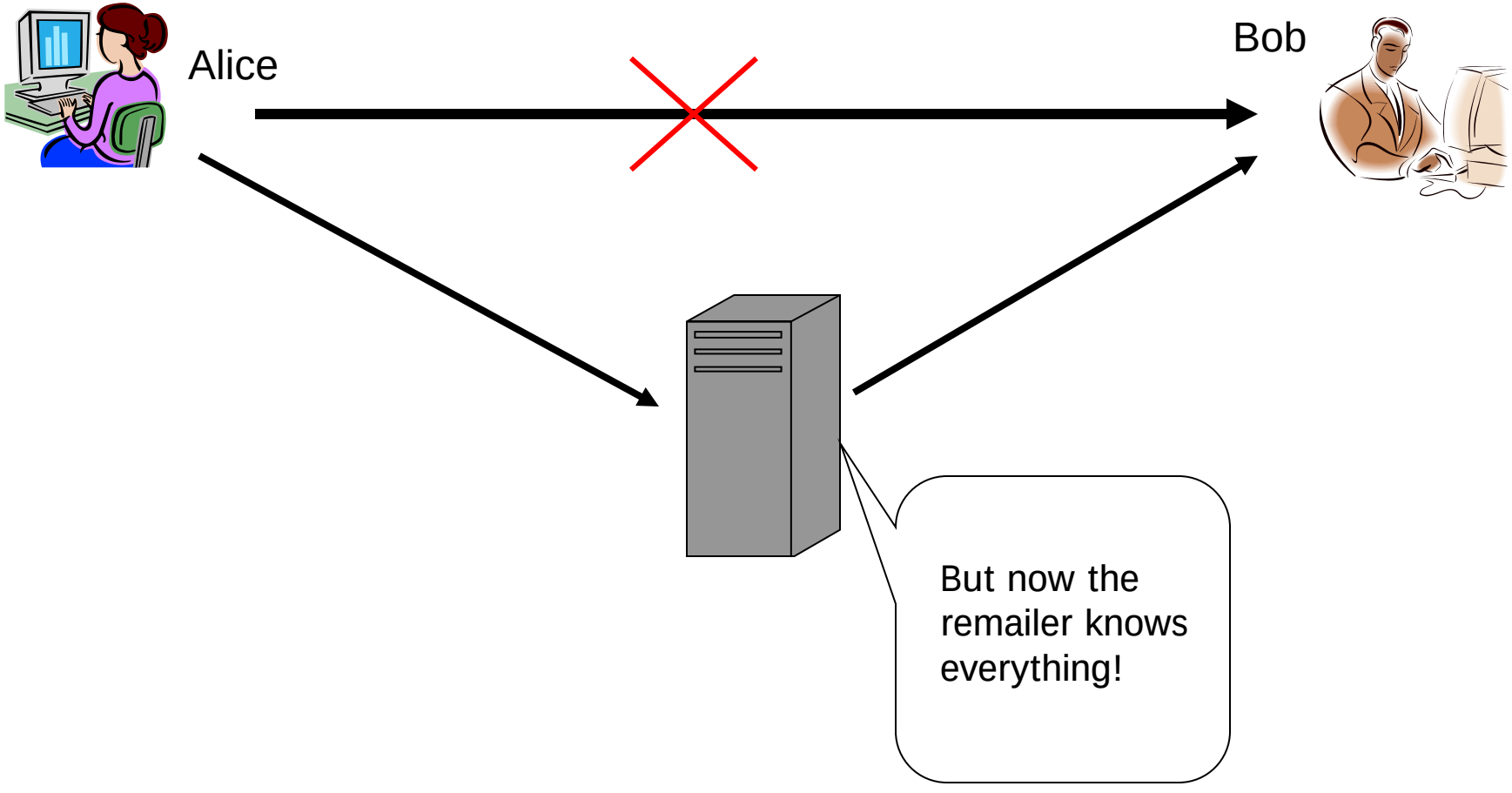
Source: Pfitzmann/Hansen

Definitions - Pseudonymity (cont.)

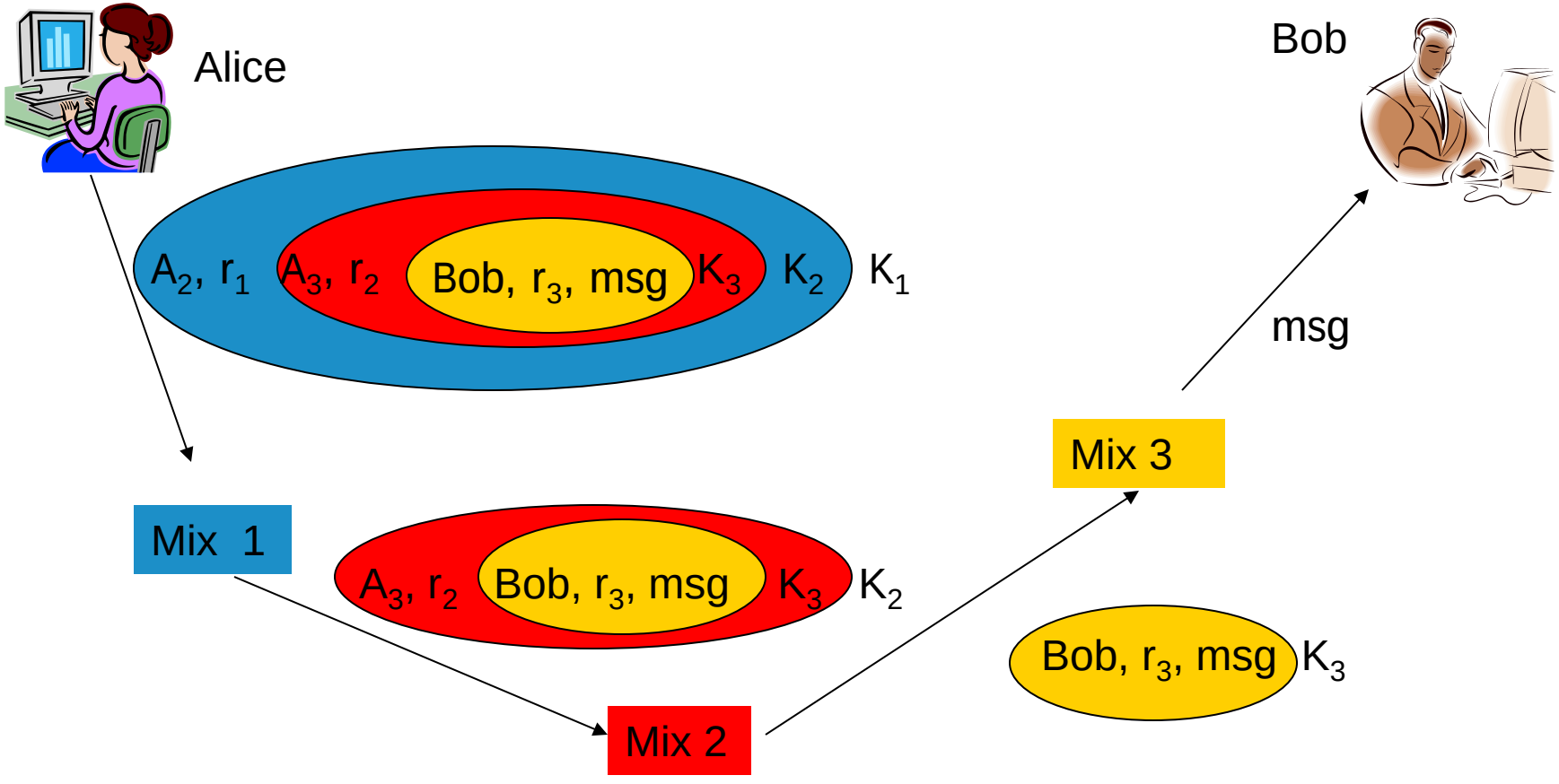


Source: Pfitzmann/Hansen

V. Anonymous Communication Technologies

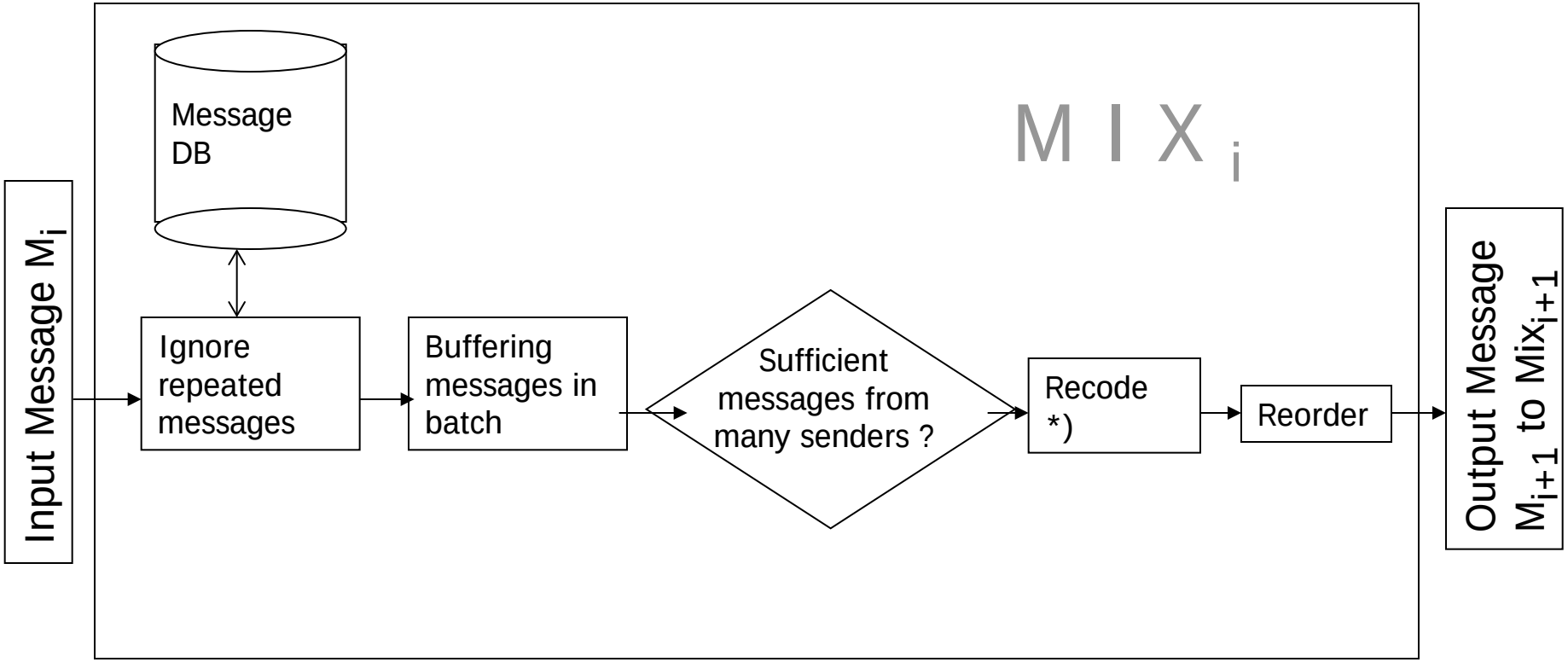


Mix-nets (Chaum, 1981)



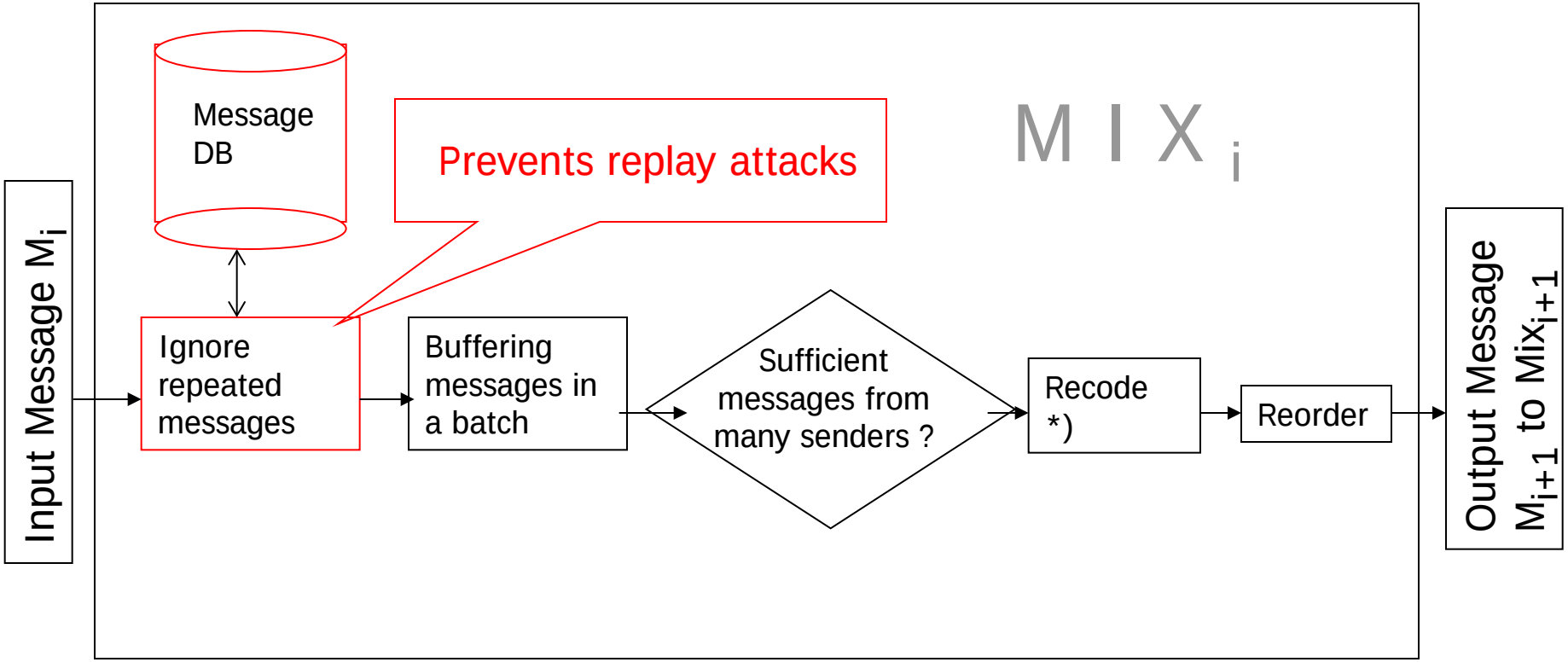
K_i: public key of Mix_i, r_i: random number, A_i: address of Mix_i

Functionality of a Mix Server (Mix_i)



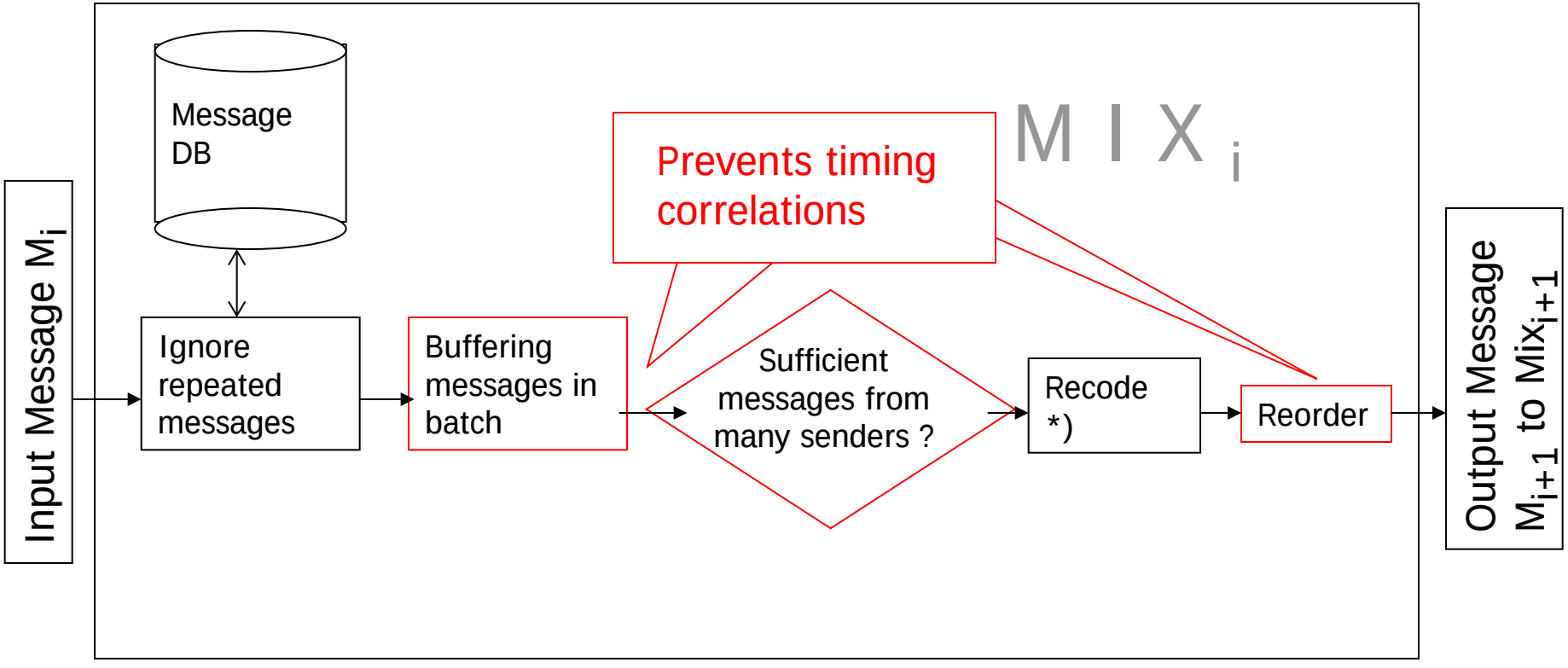
*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

Functionality of a Mix Server (Mix_i)



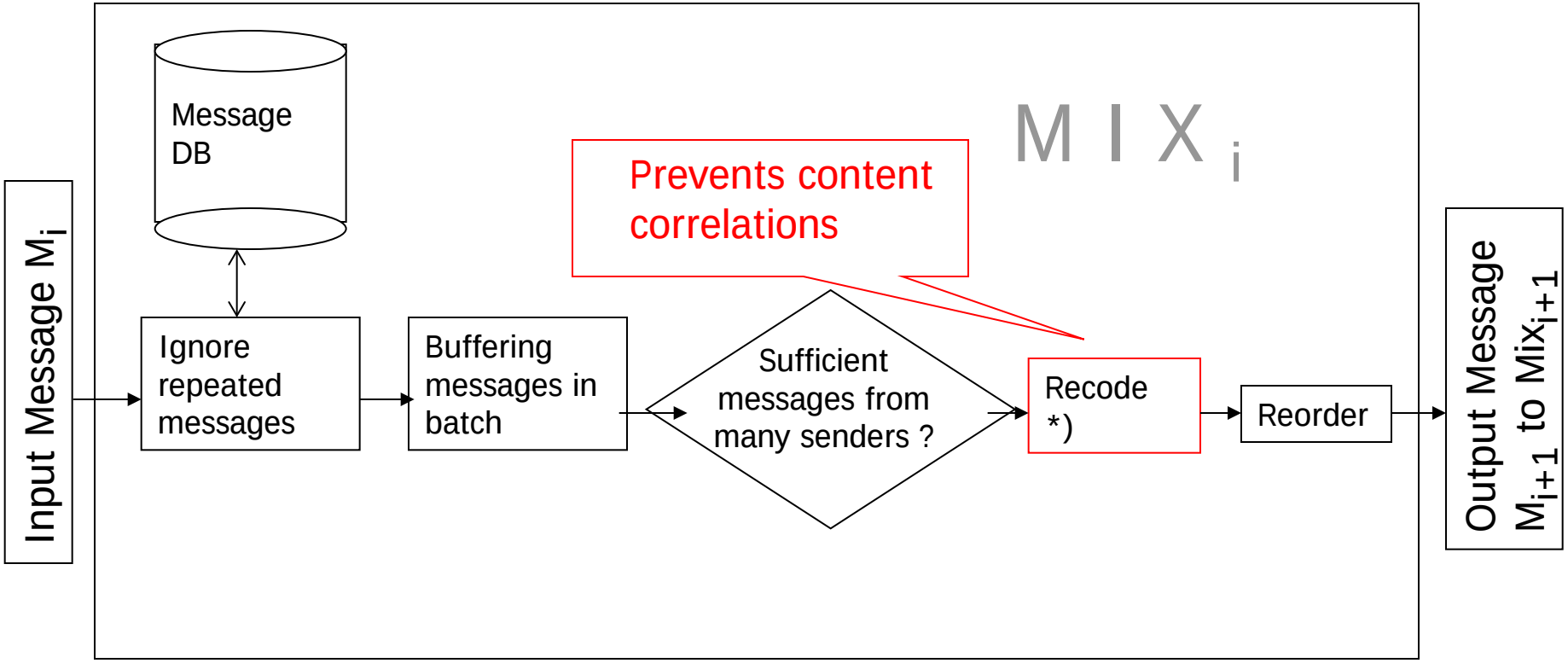
*) decrypts $M_i = E_{Ki}[A_{i+1}, r_i, M_{i+1}]$ with the private key of Mix_i,
ignores random number r_i,
obtains address A_{i+1} and encrypted M_{i+1}

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}

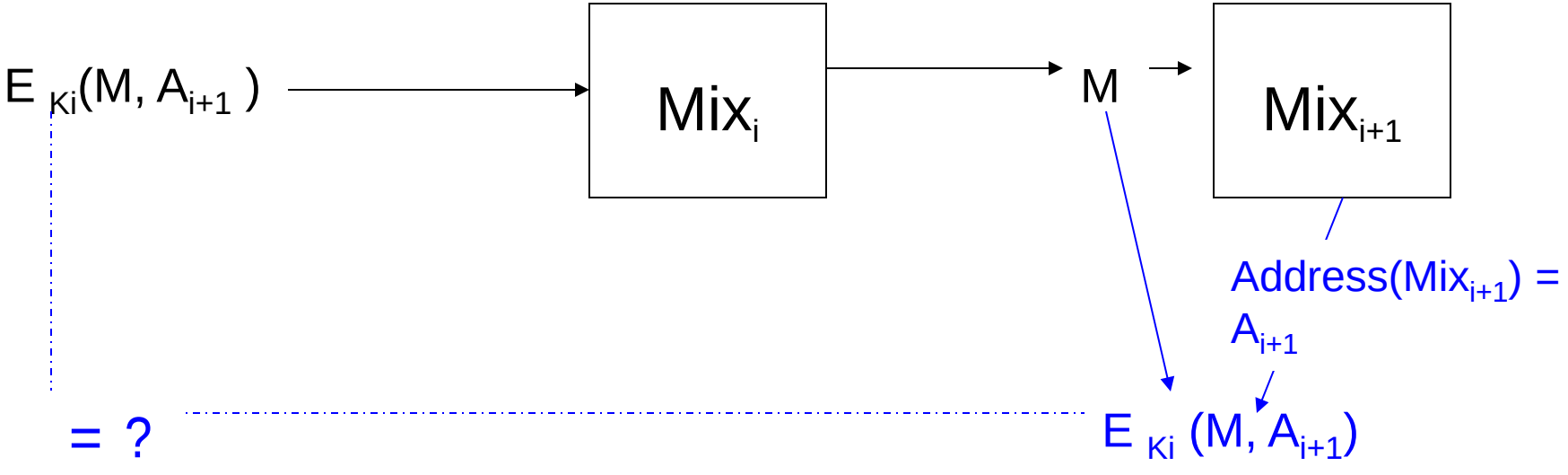
Functionality of a Mix Server (Mix_i)



*) 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}

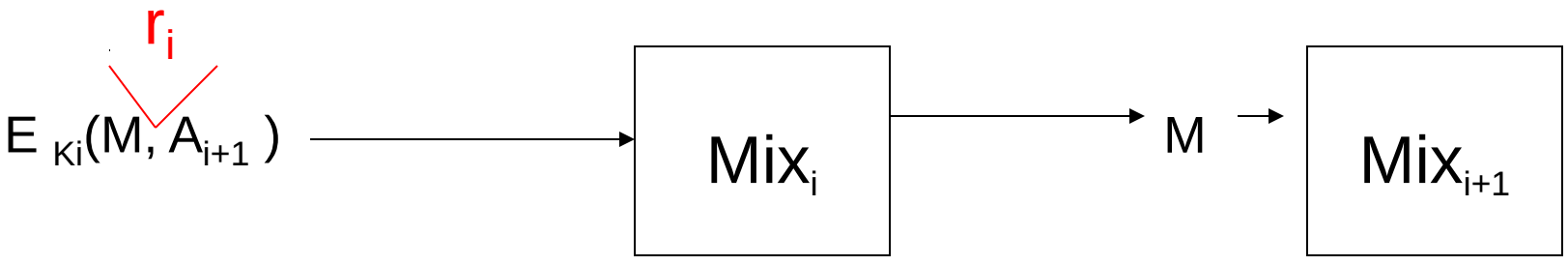
Why are random numbers needed ?

If no random number r_i is used :



Why are random numbers needed ?

If no random number r_i is used :



Protection properties & Attacker Model for Mix nets

- Protection properties:
  - Sender anonymity against recipients
  - Unlinkability of sender and recipient

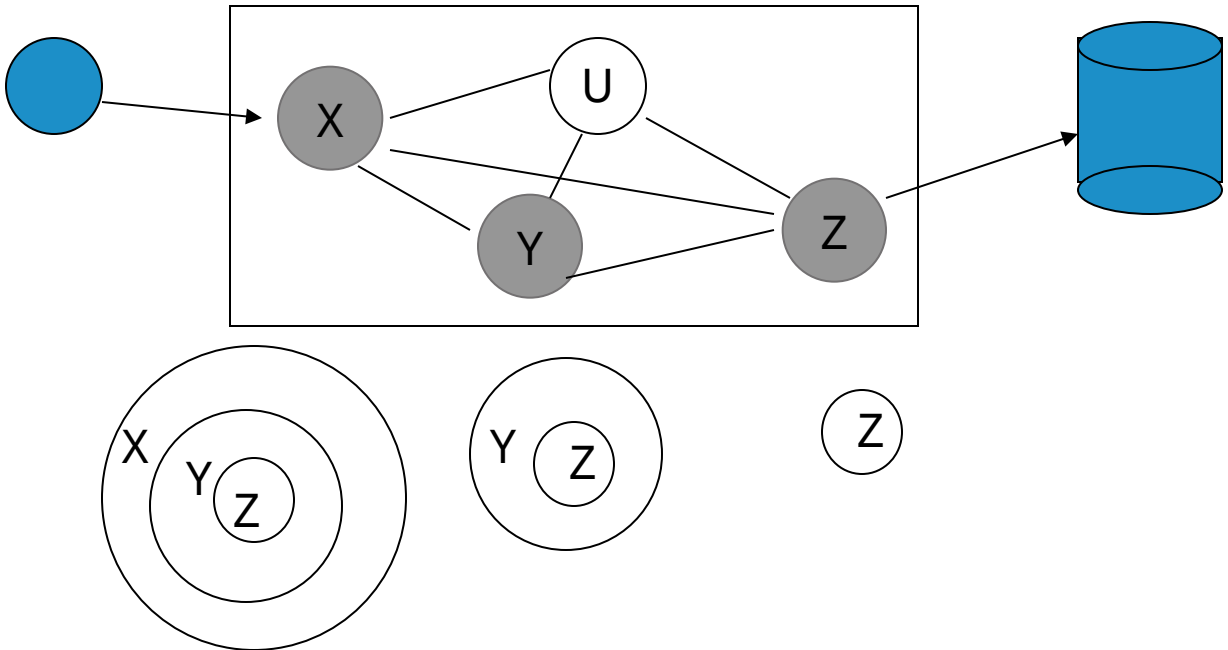
- Attacker may:
  - Observe all communication lines
  - Send own messages
  - Delay messages
  - Operate Mix servers (all but one...)
- Attacker cannot:
  - Break cryptographic operations
  - Attack the user's personal machine

Existing Mix-based systems for HTTP (real-time)

- Simple Proxies (remailers)
  - Anonymizer.com
  - ProxyMate.com
- Mix-based Systems considering traffic analysis:
  - Onion Routing (Naval Research Lab)
  - Tor (Free Haven project)
  - JAP (TU Dresden)

First Generation of Onion Routing

- Onion = Object with layers of public key encryption to produce anonymous bi-directional virtual circuit between communication partners and to distribute symmetric keys
- Initiator's proxy constructs “forward onion” which encapsulates a route to the responder
- (Faster) symmetric encryption for data communication via the circuit



Onion Routing - Review

- Functionality:
  - Hiding of routing information in connection oriented communication relations
  - Nested public key encryption for building up virtual circuit
  - Dummy traffic between Mixes (Onion Routers)
- Limitations:
  - No forward secrecy
  - First/Last-Hop Attacks by
    - Timing correlations
    - Message length (No. of cells sent over circuit)

Tor (2nd Generation Onion Router – www.torproject.org)

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis

Learn more about Tor »

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.

Get involved with Tor »

Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.

Activists

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on corruption.

Media

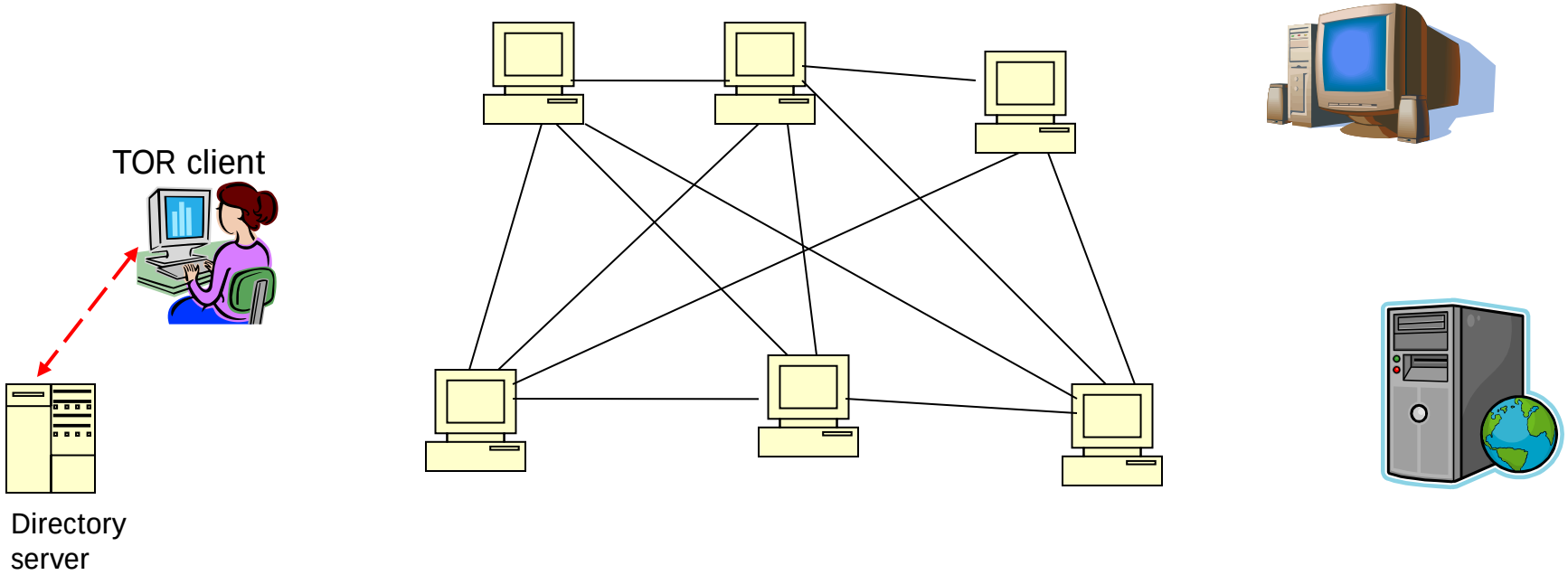
Journalists and the media use Tor to protect their research and sources online.

Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications,

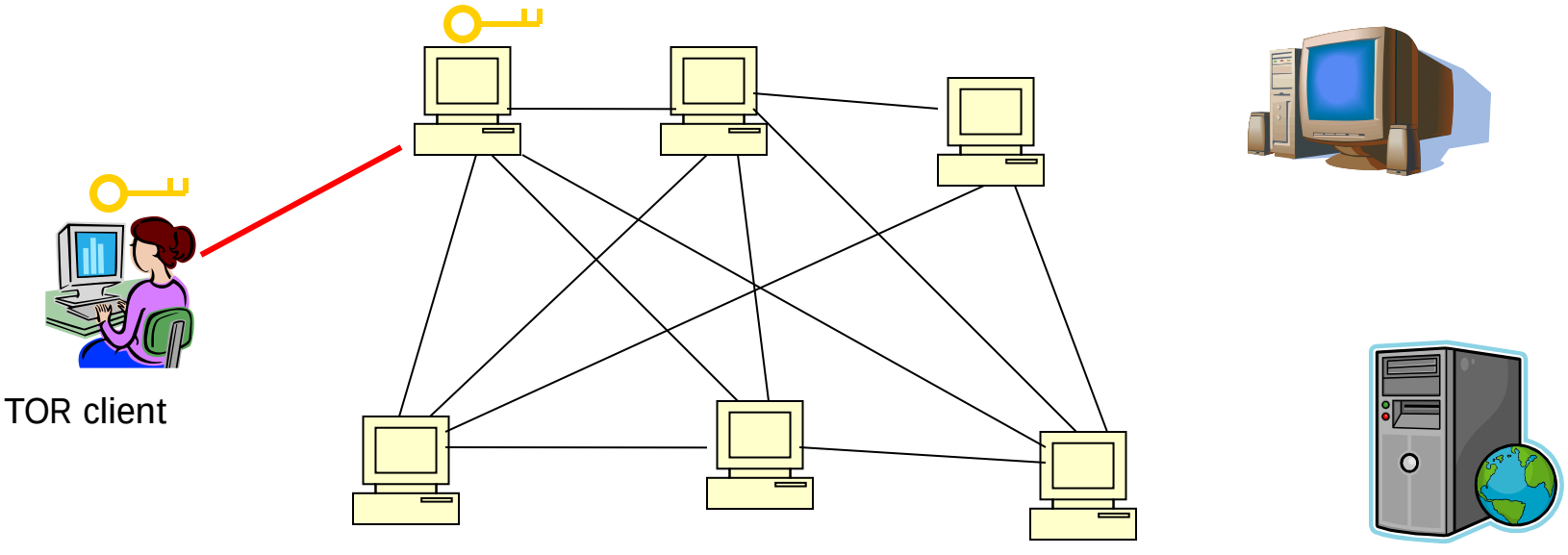
First Step

- TOR client obtains a list of TOR nodes from a directory server
- Directory servers maintain list of which onion routers are up, their locations, current keys, exit policies, etc.



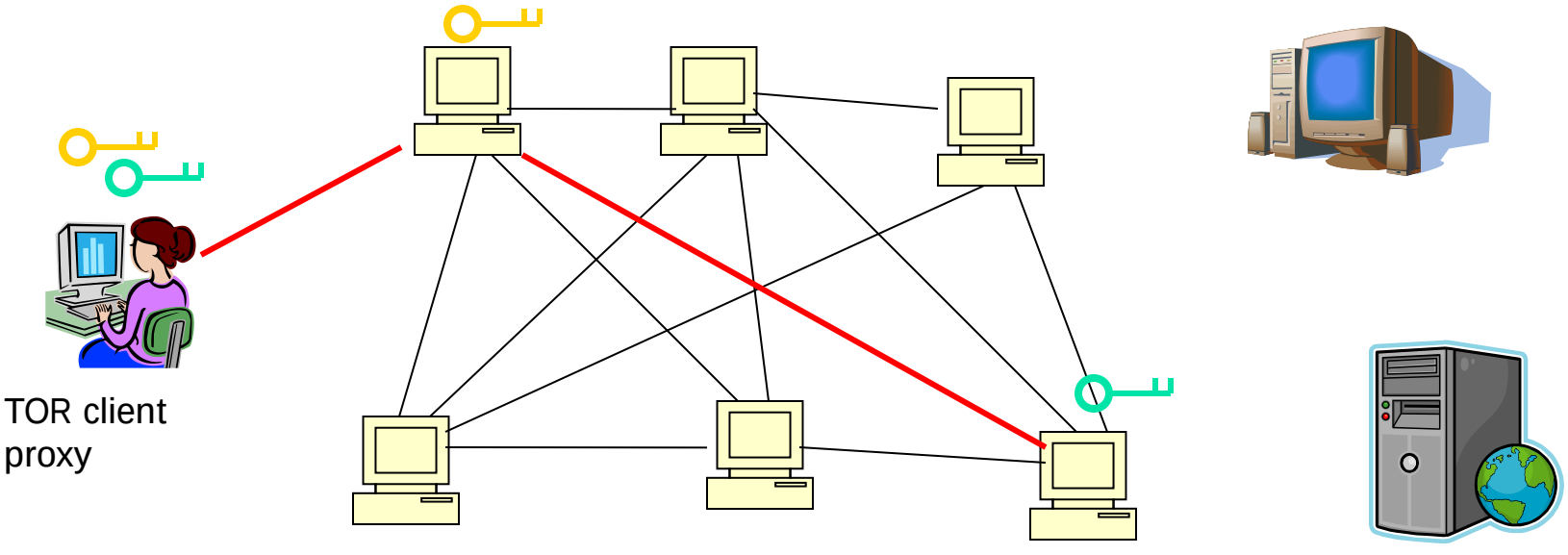
TOR circuit setup

- Client proxy establishes key + circuit with Onion Router 1



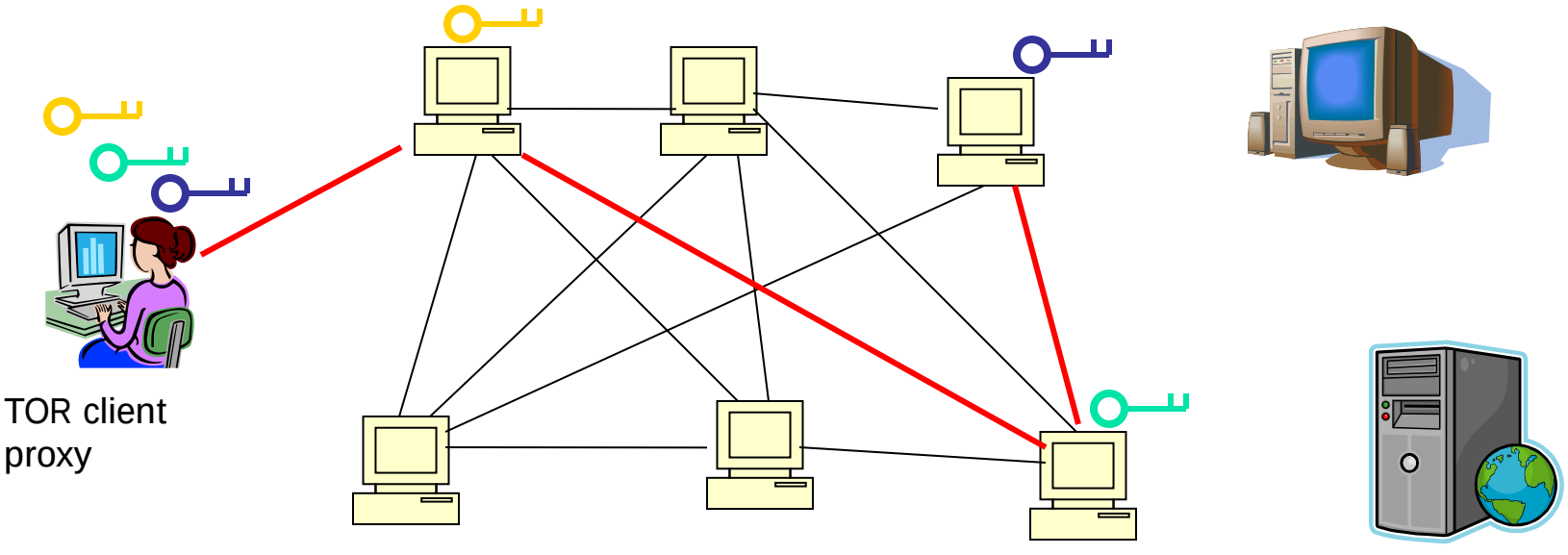
TOR circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2



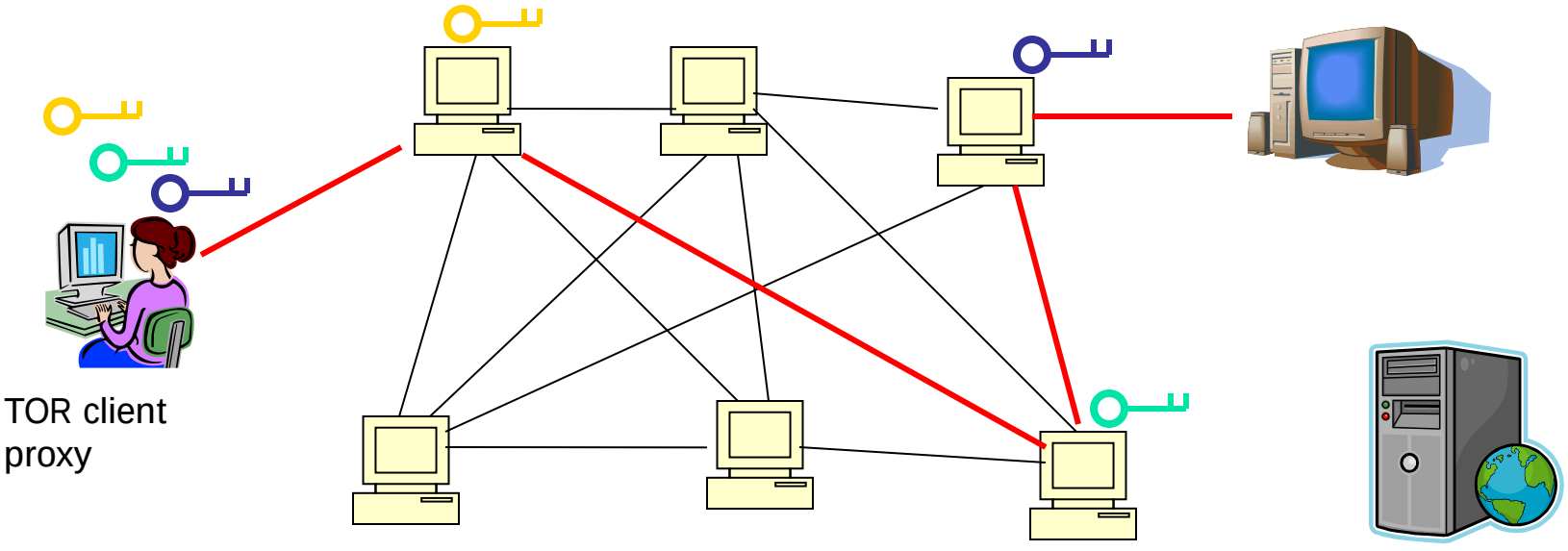
TOR circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.



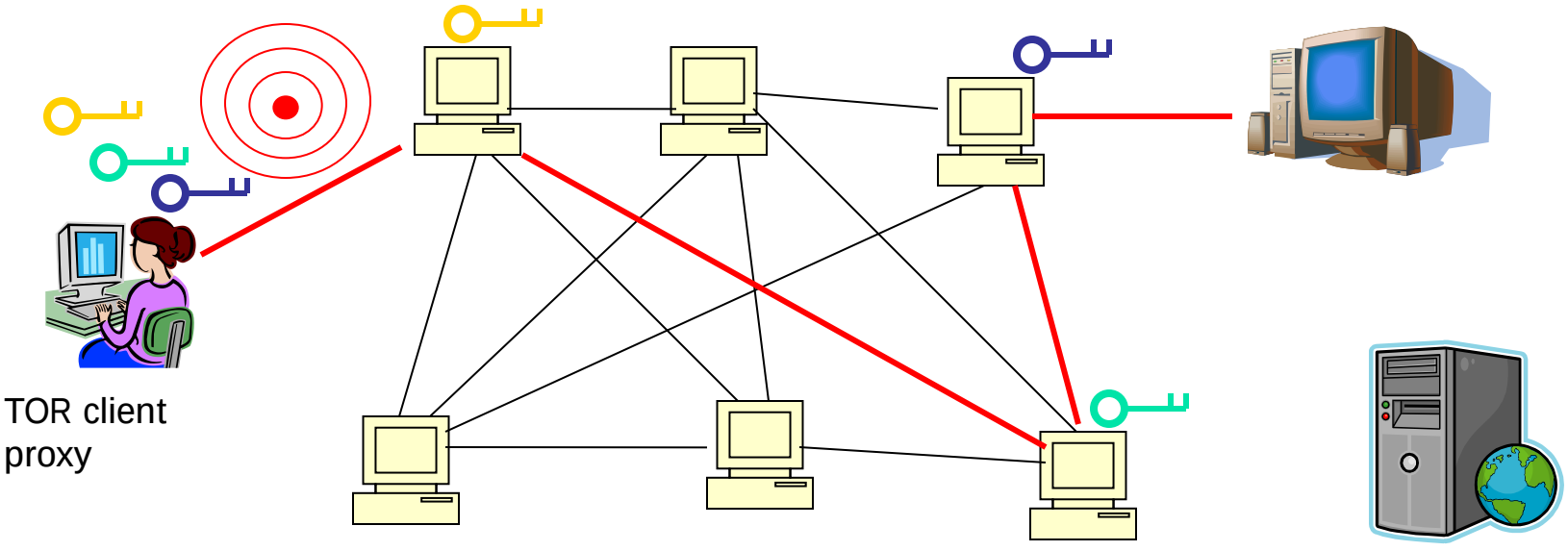
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



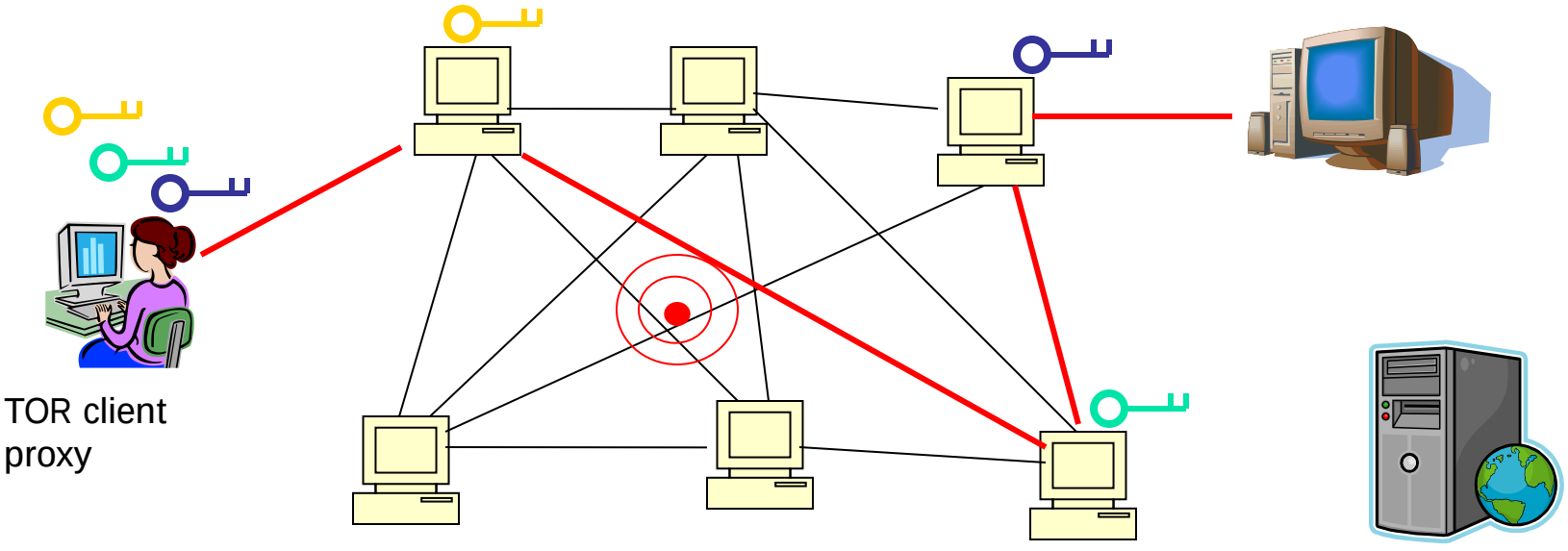
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



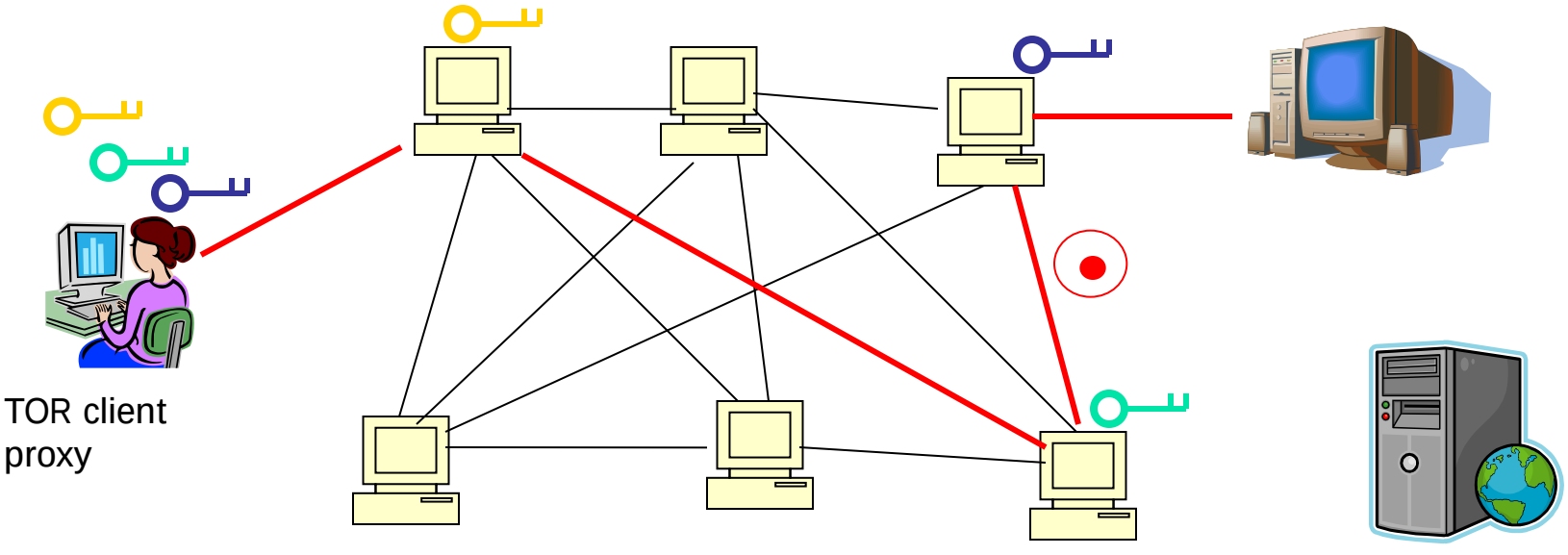
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



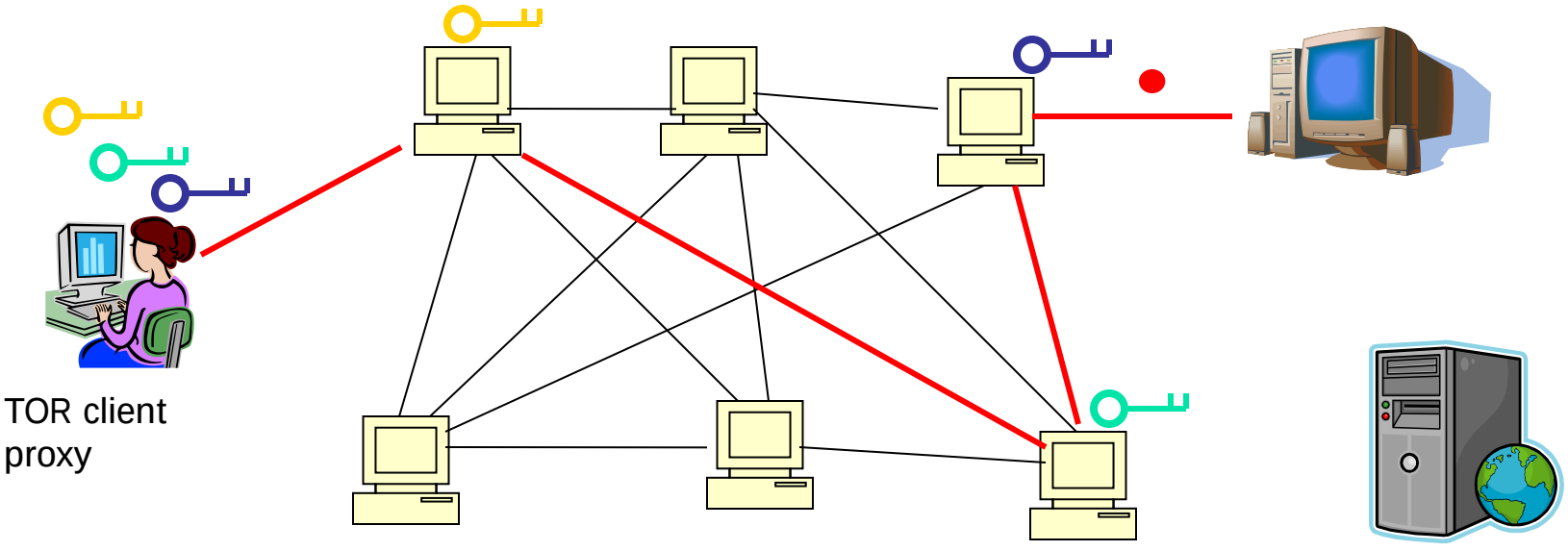
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



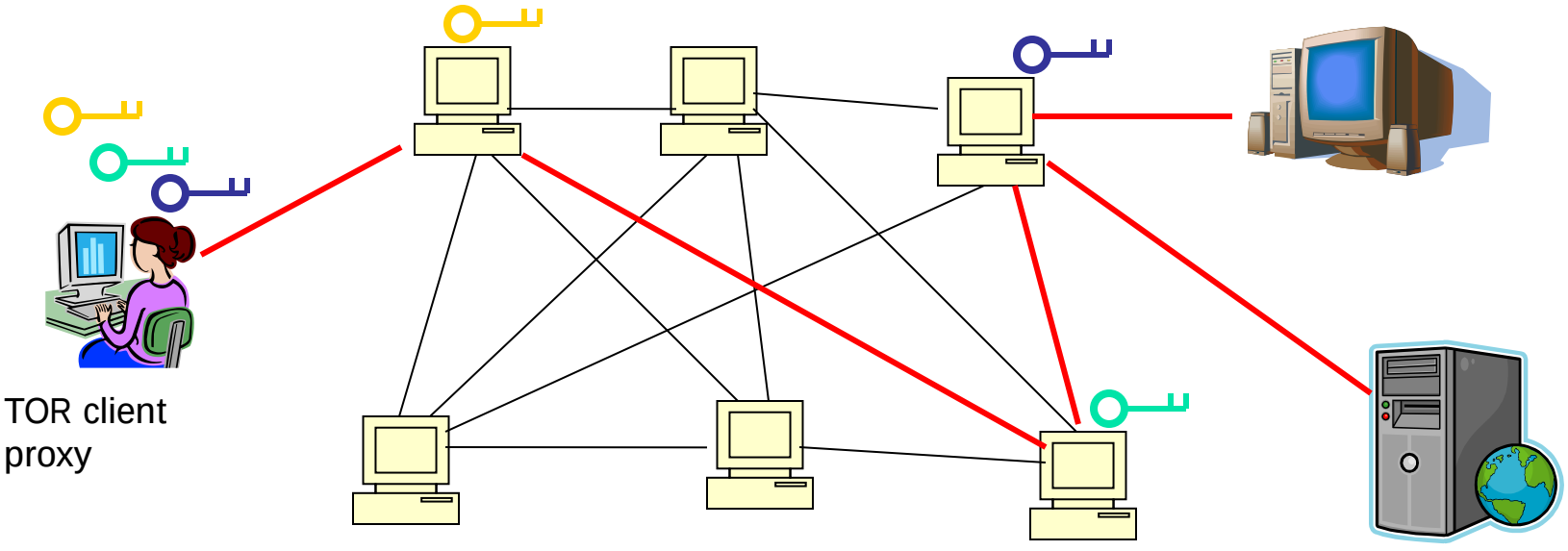
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



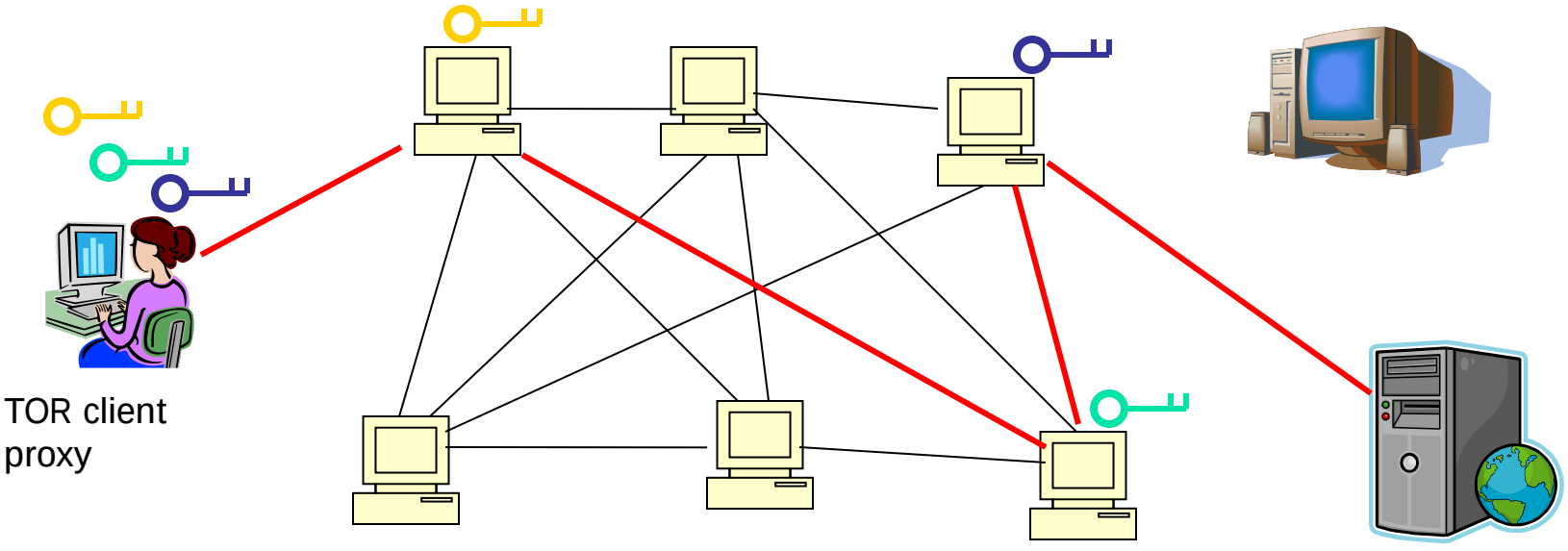
Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit

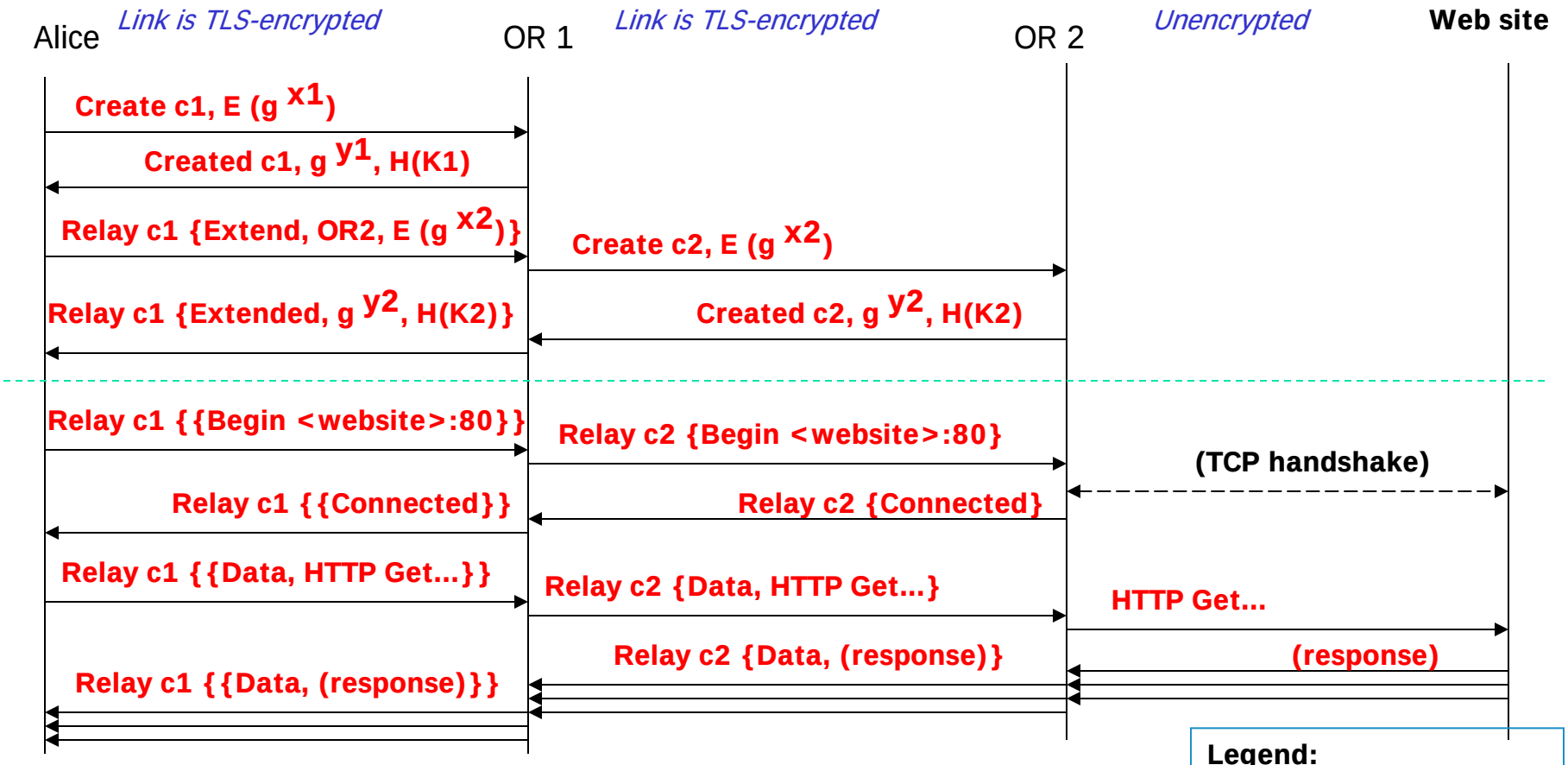


Tor circuit setup

- Client proxy establishes key + circuit with Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc.
- Client applications connect and communicate over TOR circuit



Tor: Building up a two-hop circuit and fetching a web page



Legend:
E(x): RSA encryption
{X}: AES encryption
cN: a circuit ID

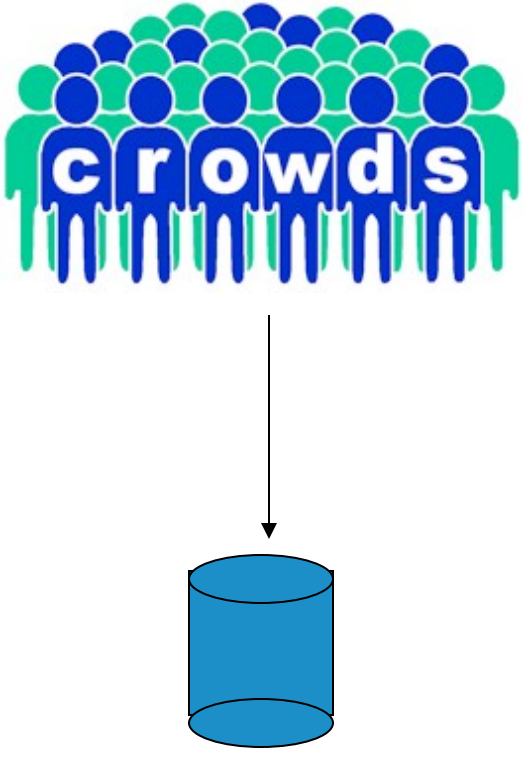
Tor - Review

- Some improvemnets in comparision with Onion Routing:
  - Perfect forward secrecy
  - Resistant to replay attacks
  - Many TCP streams can share one circuit
  - Seperation of ”protocol cleaning” from anonymity:
    - Standard SOCKS proxy interface (instead of having a seperate application proxy for each application)
    - Content filtering via Privoxy
  - Directory servers
  - Variable exit policies
  - End-to-end integrity checking
  - Hidden services
- Still vulnerable to end-to-end timing and size correlations

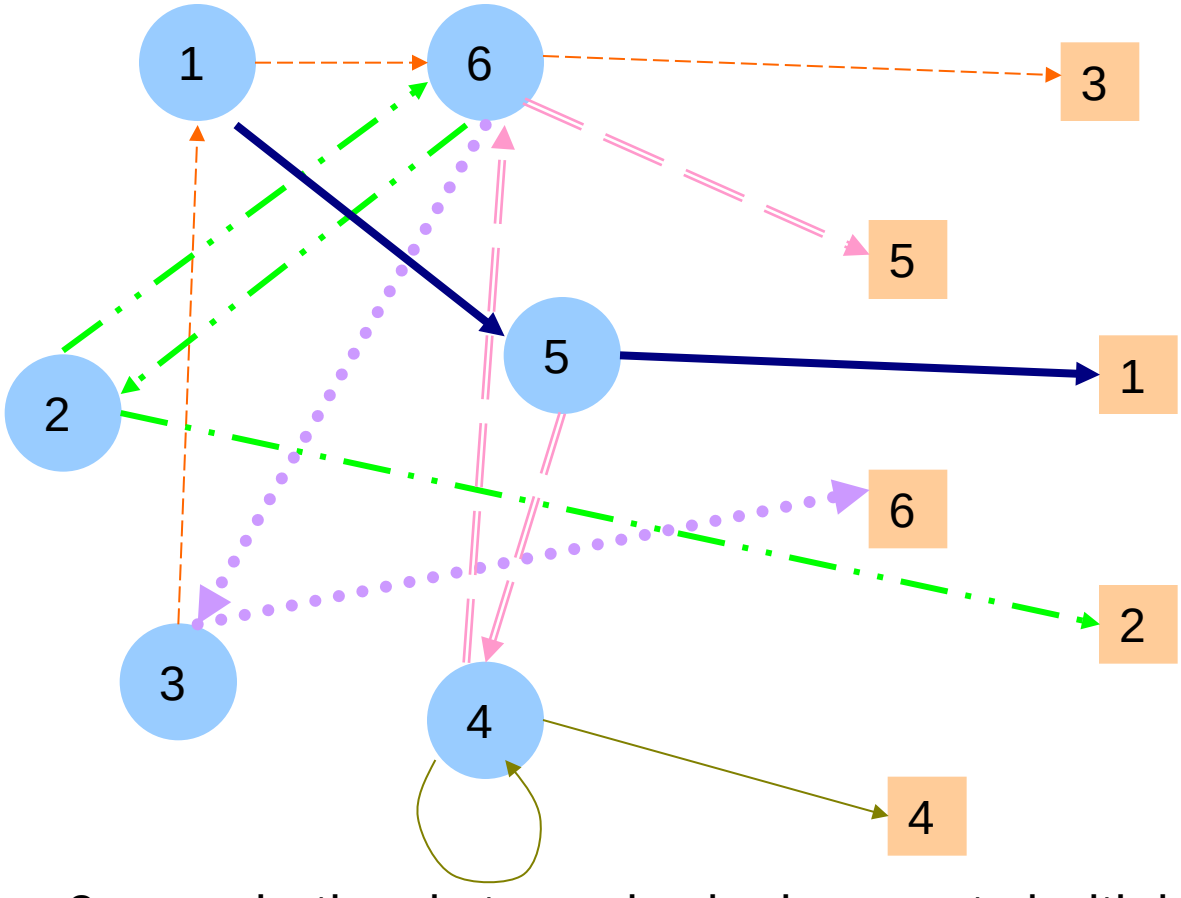
Crowds for anonymous Web-Transactions

1. User first joins a "crowd" of other users, where he is represented by a "jondo" process on his local machine
2. User configures his browser to employ the local jondo as a proxy for all new services
3. User´s request is passed by the jondo to a random member of the crowd
4. That member can either submit the request directly to the web server or forward it to another randomly (with pf> 1/2) chosen user.

-> Request is eventually submitted by a random member



Communication Paths in Crowds

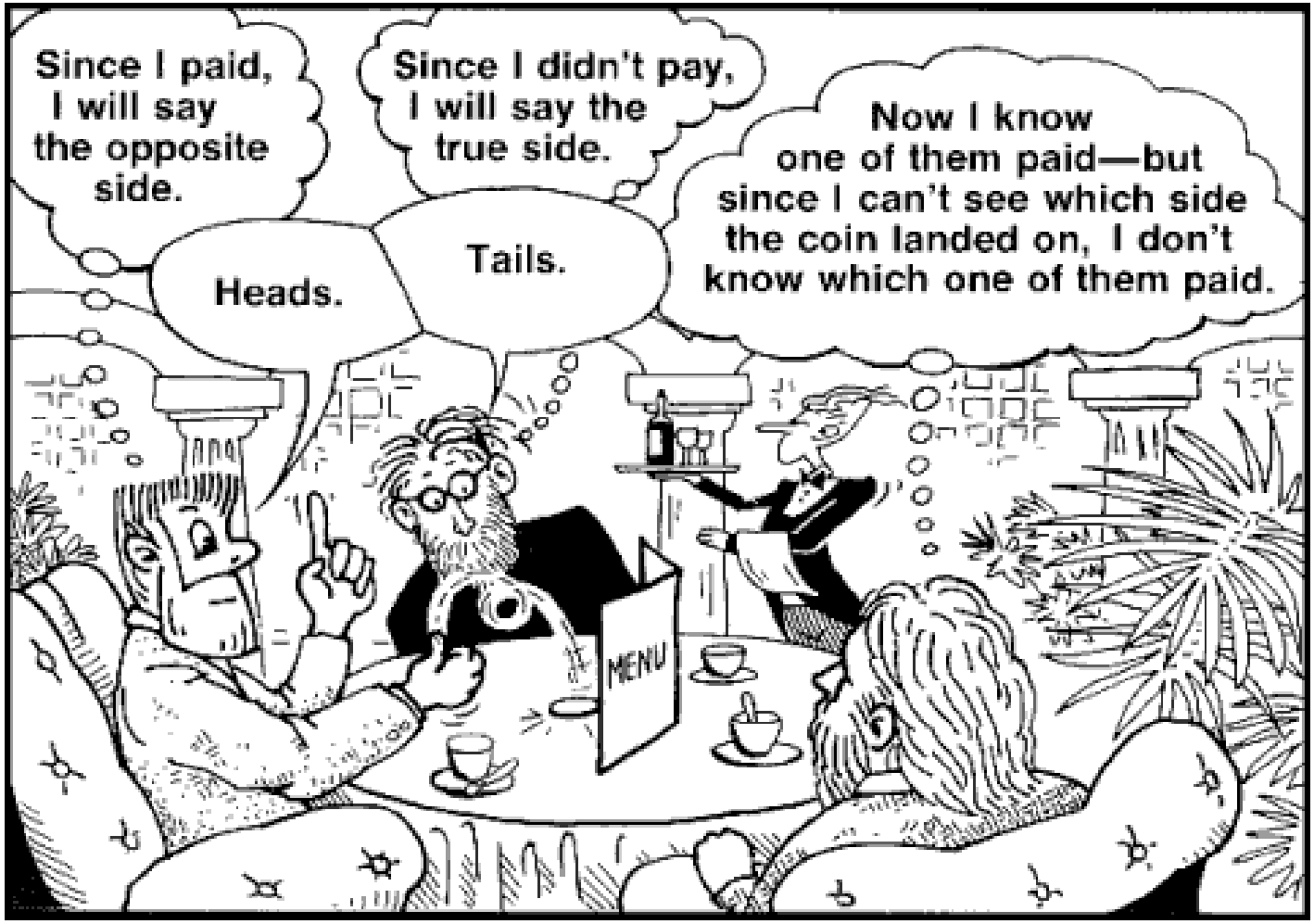


Communications between jondos is encrypted with keys shared between jondos

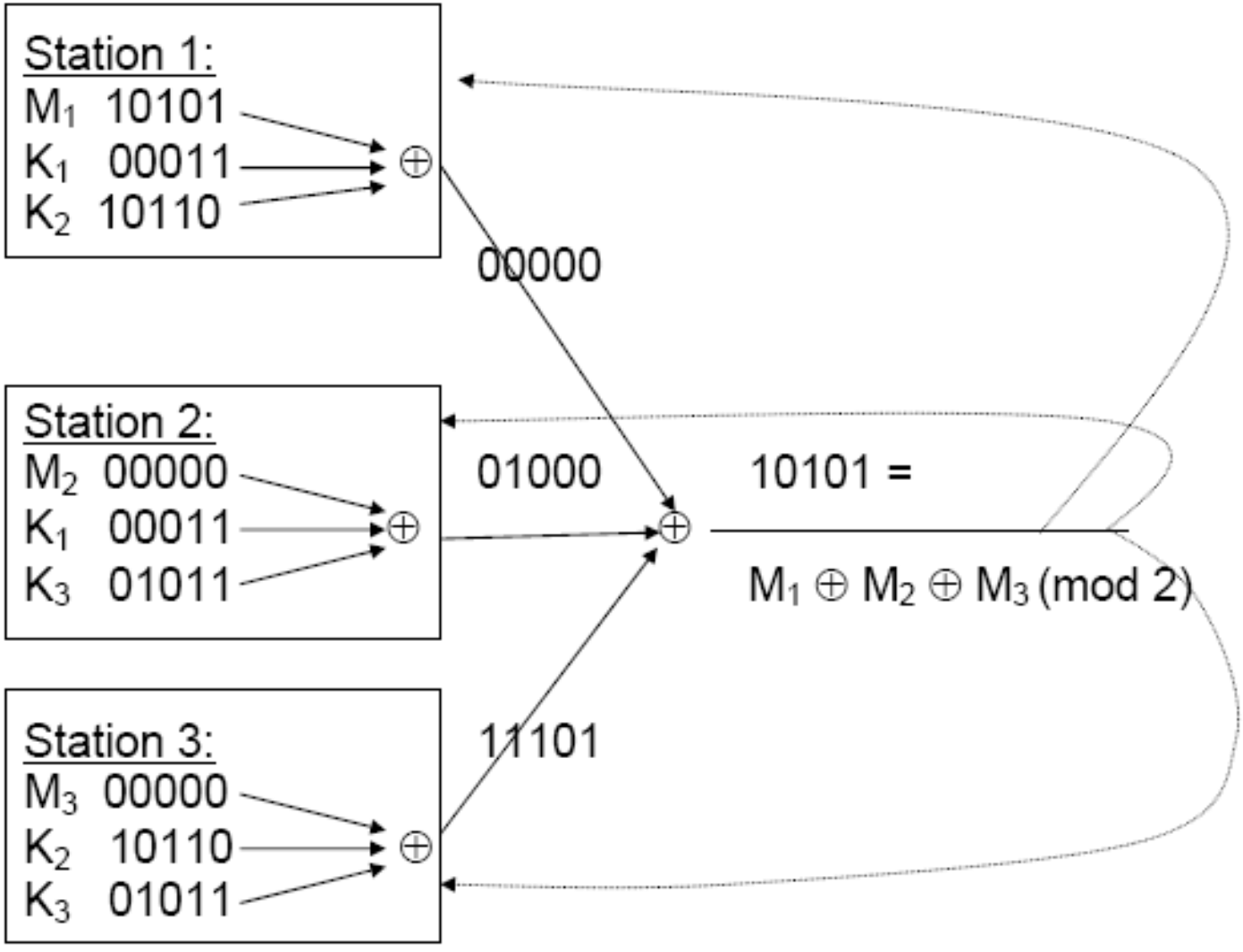
Crowds -Review

- **Sender anonymity against:**
  - end web servers (“beyond suspicion”)
  - other Crowd members
  - eavesdroppers
- **Limitations:**
  - No protection against “global” attackers, timing/message length correlation attacks
  - Web server´s log may record submitting jondo´s IP address as the request originator´s address
  - Request contents are exposed to jondos on the path
  - Anonymising service can be circumvented by Java Applets, Active X controls
  - Performance overhead (increased retrieval time, network traffic and load on jondo machines)
  - No defend against DoS-attacks by malicious crowd members

DC (Dining Cryptographers) nets [Chaum 1988]



DC-nets: Perfect sender anonymity through Binary superposed sending and broadcast



DC nets - Review

- Protection properties:
  - Perfect sender anonymity through superposed sending (message bits are hidden by one-time pad encryption)
  - Message secrecy through encryption
  - Recipient anonymity through broadcast and implicit addresses (addressee is user who can successfully decrypt message)
- Problems:
  - Denial of Service attacks by DC-net participants (Defense: trap protocols)
  - Random key string distribution

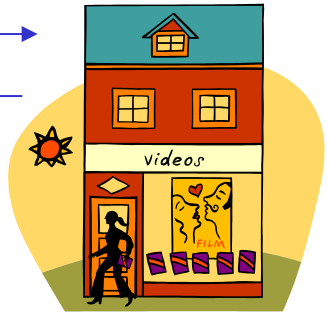
VI. PrimeLife PETs:
Anonymous Credentials (Idemix)

Relying Party

Service request

Data request

(unlinkable) selective disclosure



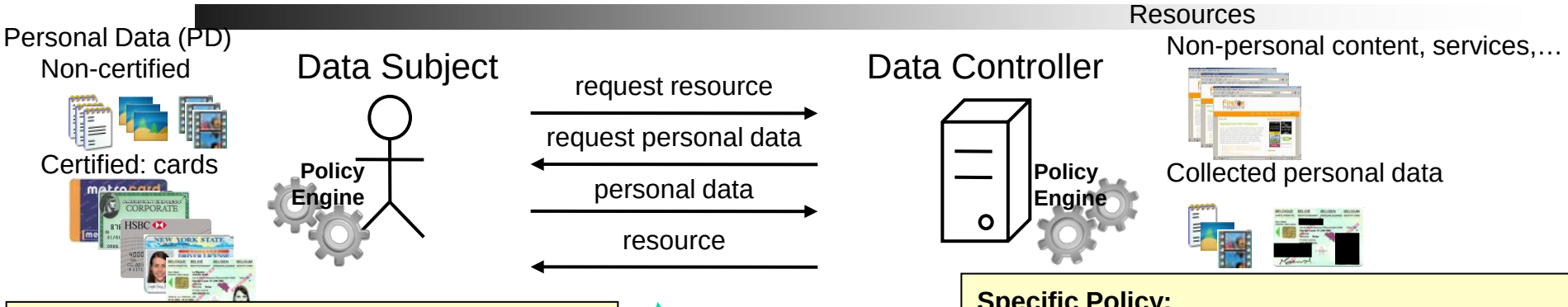
Issues credentials

Identity Provider

Advantages:

- Data Minimisation
- Unlinkability of Transactions (Idemix)
- No Profiling by IdPs or Relying Parties

PrimeLife Policy Language PPL (Neven et al.)



Specific Policy:

over specific personal data (e.g. birth date)

- **Access control policy (ACP):**
  who can access (e.g. PrivacySeal silver)
- **Data handling preferences (DHPrefs):**
  how is to be treated when revealed
  - **Authorizations** (e.g. marketing purposes, forwarded to PrivacySeal gold)
  - **Obligations** (e.g. delete after ≤2y)

Generic Preferences:

DHPrefs over implicitly revealed personal data (e.g. IP address, cookies,…)

- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after ≤2y)

SAML

XACML

Specific Policy:

over specific resource (e.g. BuyService)

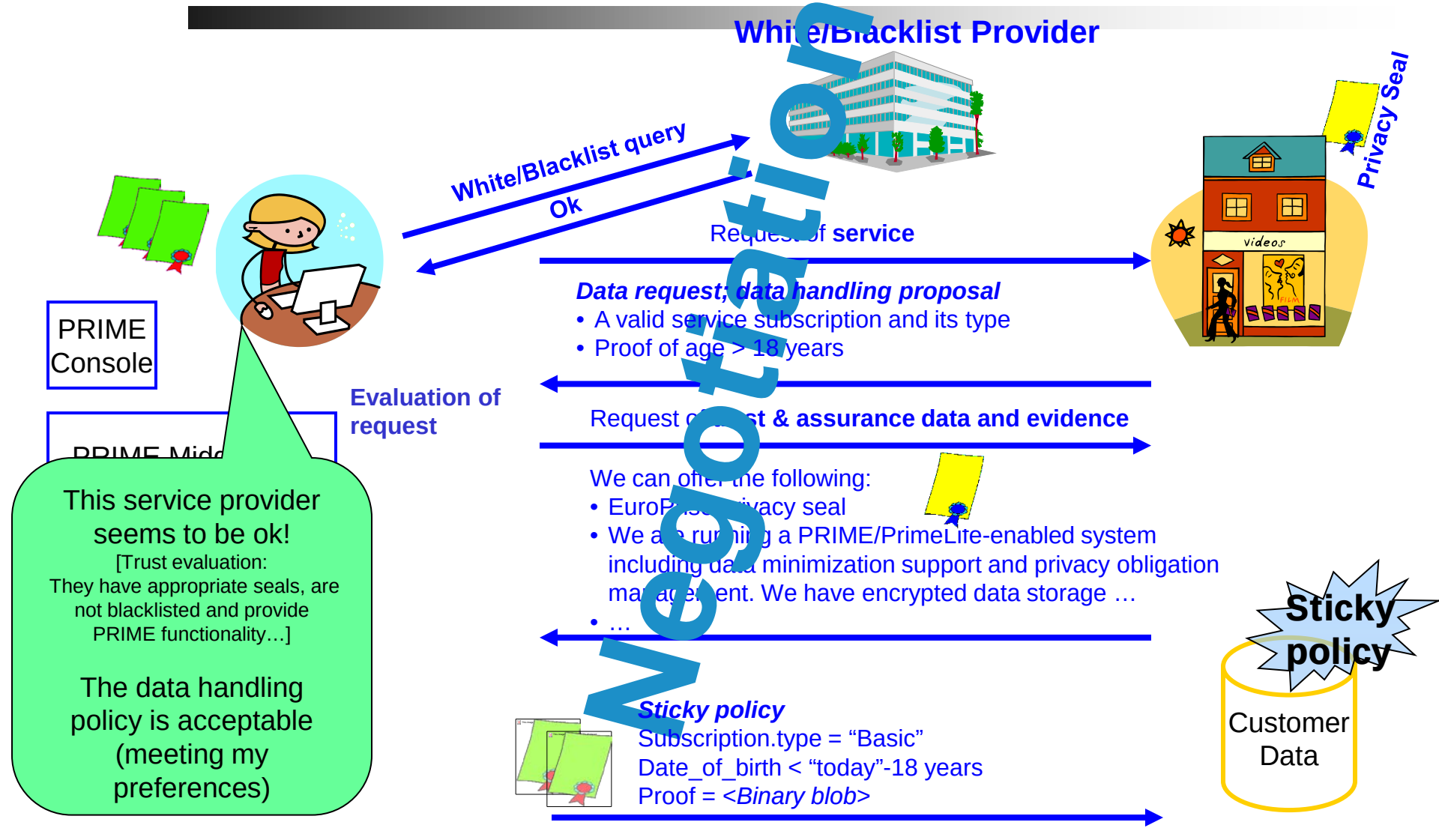
- **Access control policy (ACP):**
  who can access
  - cards to possess (e.g. ID card)
  - personal data to reveal (e.g. nationality)
  - conditions to satisfy (e.g. age>18)
- **Data handling policy (DHP):**
  how revealed personal data will be treated
  - **Authorizations** (e.g. marketing purposes)
  - **Obligations** (e.g. delete after 1y)

Generic Policy:

DHP over implicitly revealed personal data (e.g. IP address, cookies,…)

- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after 1y)

PrimeLife architecture



Questions ?

http://www.cs.kau.se/~simone/

Further reading

- Andreas Pfitzmann, Marit Hansen, Anonymity. Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version v0.34, August 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
- D.Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24 (2). 1981, pp. 84-88, http://world.std.com/~franl/crypto/chaum-acm-1981.html
- D.Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", Journal of Cryptology, 1, 1988
- P. M.Reiter, A.Rubin, "Anonymous Web Transactions with Crowds", Communications of the ACM, Vol.42, No.2, February 1999, pp. 32-38.
- TOR: Anonymity Online, http://www.torproject.org/
- Roger Dingledine, Nick Mathewson, Paul Syverson, TOR: The Second-Generation Onion Router, Proceedings of the 13th Usenix Security Symposium, August 2004, http://www.torproject.org/svn/trunk/doc/design-paper/tor-design.pdf
- Simone Fischer-Hübner, "IT-Security and Privacy - Design and Use of Privacy-Enhancing Security Mechanisms", Springer Scientific Publishers, Lecture Notes of Computer Science, LNCS 1958, May 2001, ISBN 3-540-42142-4 (chapter 4)
- PrimeLife project, http://primelife.ercim.eu/

Repetition: Diffie-Hellman Key exchange

<u>Global Public Elements:</u>

q: prime number

α: $\alpha < q$ and α is a primitive root of q

[If α is a primitive root of prime number p, then the numbers:

α mod p, α^2 mod p,…, α^{p-1} mod p
are distinct and are a permutation of {1..p-1}.

For any integer b<p, primitive root α of prime number p, one can find

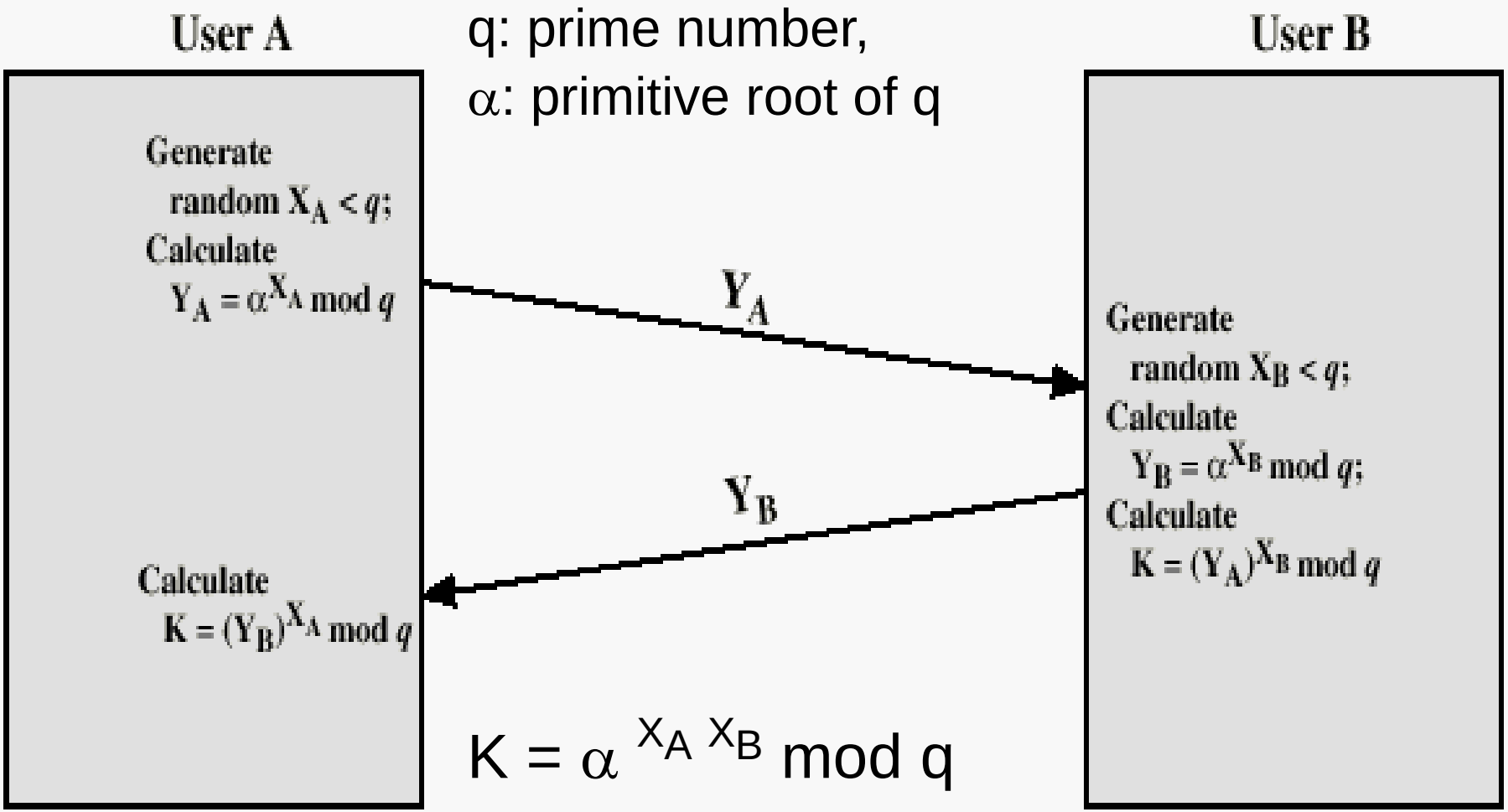
unique exponent i (discrete logarithm),

such that b= α^i mod p, $0 \leq i \leq (p-1)$

For larger primes, calculating discrete logarithms is considered as practically infeasible]

Diffie-Hellman Key Exchange

q: prime number,
α: primitive root of q



$$K = \alpha^{X_A X_B} \bmod q$$