



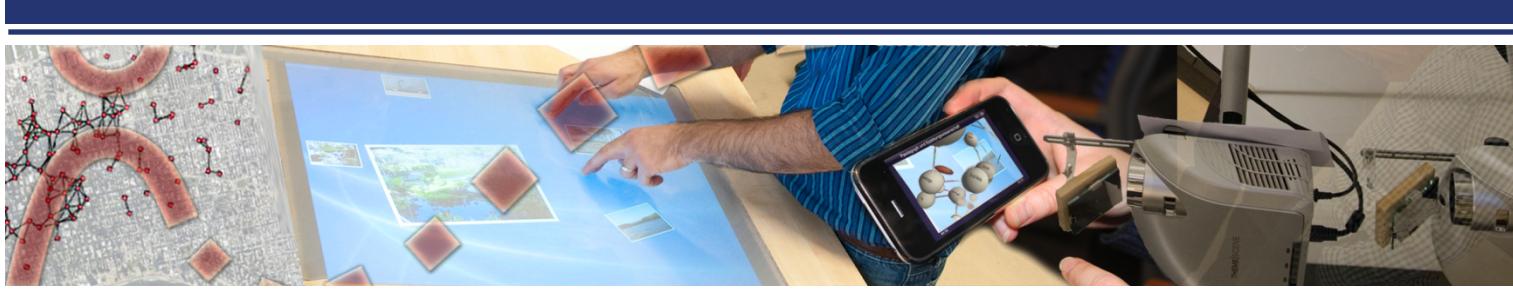
Telecooperation Lab
Prof. Dr. Max Mühlhäuser

TK3: Ubiquitous (& Mobile) Computing

Chapter ?: Privacy

Lecturer: Jörg Daubert

(based on slides by Stefan Schiffner)



PRIVACY - OUTLINE

- An Introduction to Privacy:
 - Definitions and Terminology
 - Privacy Enhancing Technologies
 - Case study: Smart Meter Privacy



Privacy – Dictionary Definition



TECHNISCHE
UNIVERSITÄT
DARMSTADT

1

- a : the quality or state of being apart from company or observation : seclusion
- b : freedom from unauthorized intrusion <one's right to privacy>

2

- archaic : a place of seclusion

3

- a : secrecy
- b : a private matter : secret

From Merriam Webster Online Dictionary

Not Really a basis for technical solutions



Informational self-determination



“The claim of individuals, groups and institutions to determine themselves, when, how and to what extent information about them is communicated to the others”

Privacy and Freedom:
Westin 1967

Information
about the
subject

Subj+ communicate +What? +ToWhom? +When?How?How much?

Verb

Direct Object

Indirect Object

Adverbial Adjuncts



What is Personal Data



EU Data Protection Directive (95/46/EC):

“personal data” shall mean any information relating to an **identified or identifiable** natural person ('Data Subject');

an identifiable person is one who can be **identified, directly or indirectly**, in particular by reference to an **identification number** or to one or more factors specific to his **physical, physiological, mental, economic, cultural or social** identity.

Personally Identifiable Information (PII)



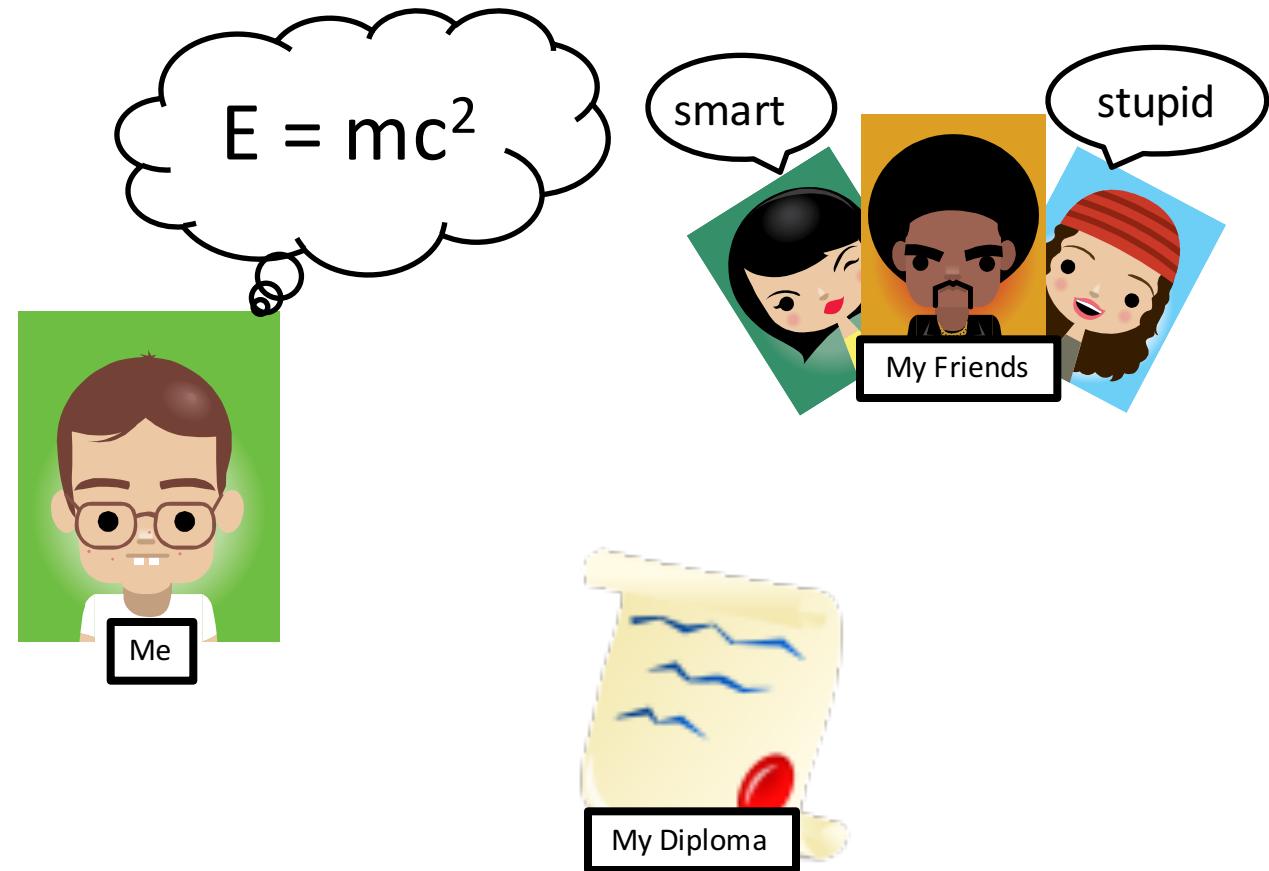
Who I am?



TECHNISCHE
UNIVERSITÄT
DARMSTADT



My Car





How to enforce my right to informational self-determination?

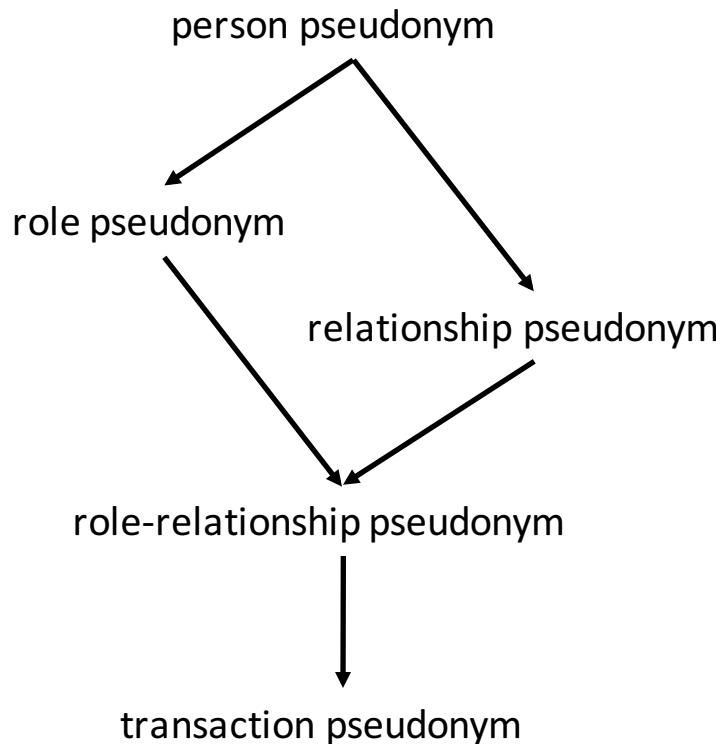
- Protect legal privacy principles using technology
 - minimizing or avoiding personal data
 - safeguarding of lawful data processing



Pseudonyms



ID in a certain context



- **Increasing Anonymity support**
- **Linkability**
 - Separate pseudonyms might be linkable by context, e.g., used IP address
 - Can lead to re-identification, e.g., several linkable transaction pseudonyms can be seen as a role-relationship pseudonym

The internet is not made for unlinkable pseudonymous communication



PETs for Data Minimization

- Anonymous Communication
 - MIXes
 - DC-Nets
- Controlled Disclosure
 - Anonymous credentials
 - Anonymous payment systems
 - Voting systems
- Privacy enhanced ID Management Systems
 - Ecosystems that use the above



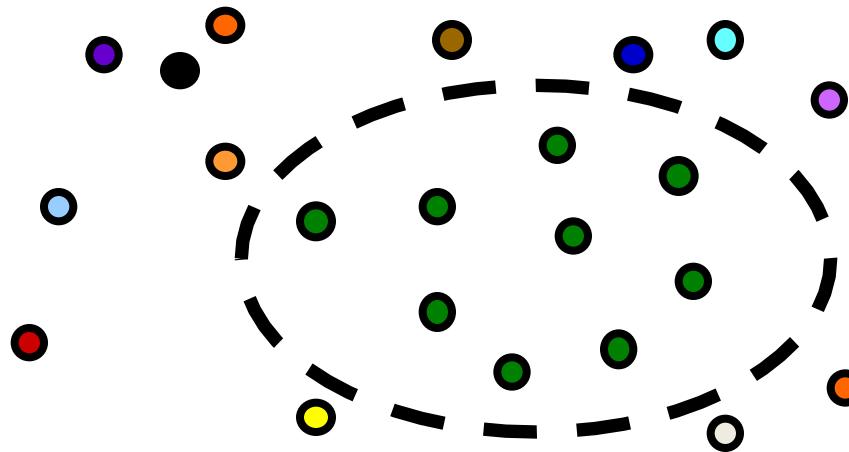


Anonymity



- Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set

Pfitzmann 2000



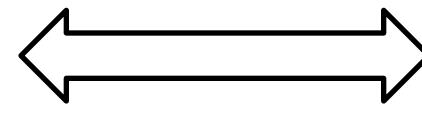
the anonymity set



- Anonymous communication between peers

- Attacker Model

- How resource attacker is
- Active
- Passive



- Global Attacker

- Dolev-Yao threat model
- All communication
- Some nodes



- Local Attacker

- Some communication
- Some nodes



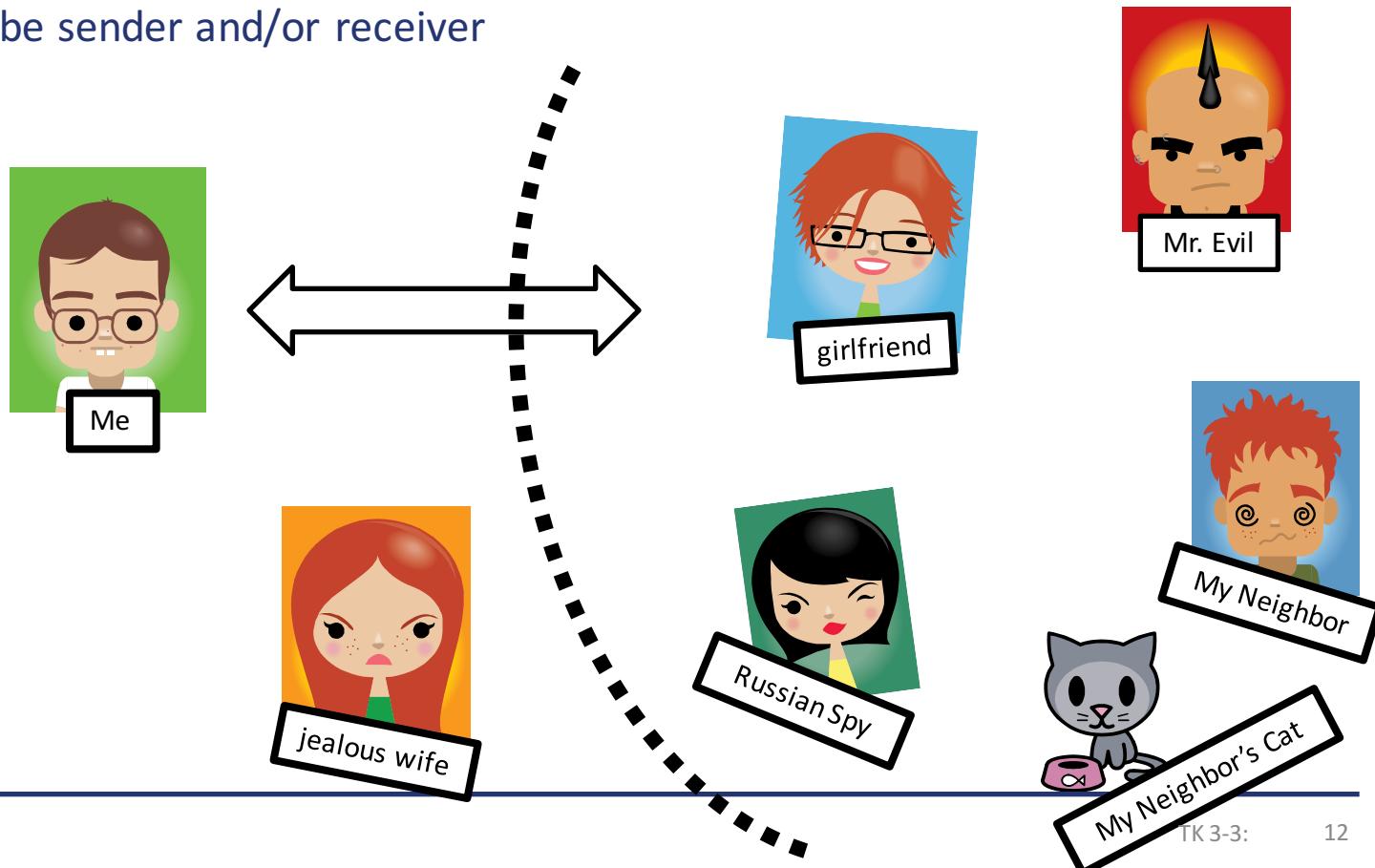
Anonymous Communication



TECHNISCHE
UNIVERSITÄT
DARMSTADT

■ Basic Idea:

- Every message can be sent by anyone
- ~can be received by anyone
- Attacker can be sender and/or receiver



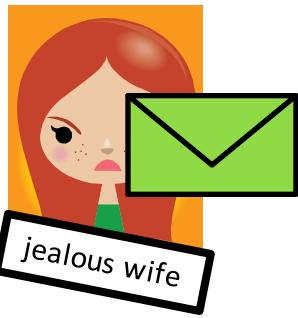


1. Collects messages
2. Deletes doublets
3. Re-Codes
4. Shuffles
5. Forwards





Replay attack (why step 2)



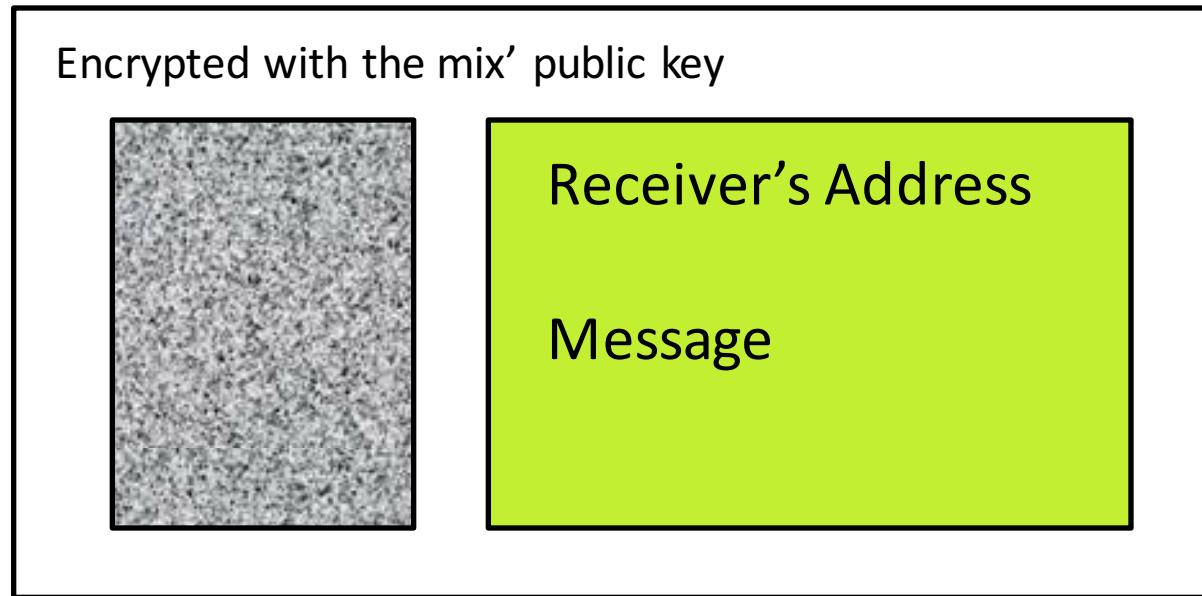
Repetitions need to be
dropped



How to construct the messages?

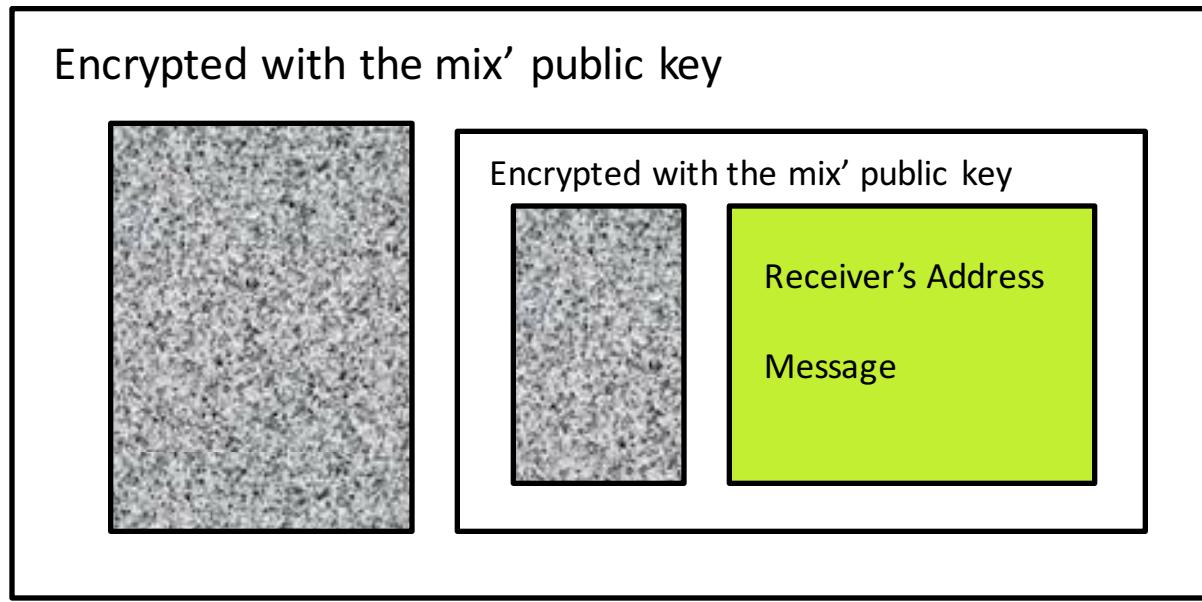


- Symmetric Encryption -> key distribution problem
- Hence Mix provides a public key
- Problem: The attacker knows the public key, can encrypt the forwarded messages





Don't want to trust in 1 single MIX

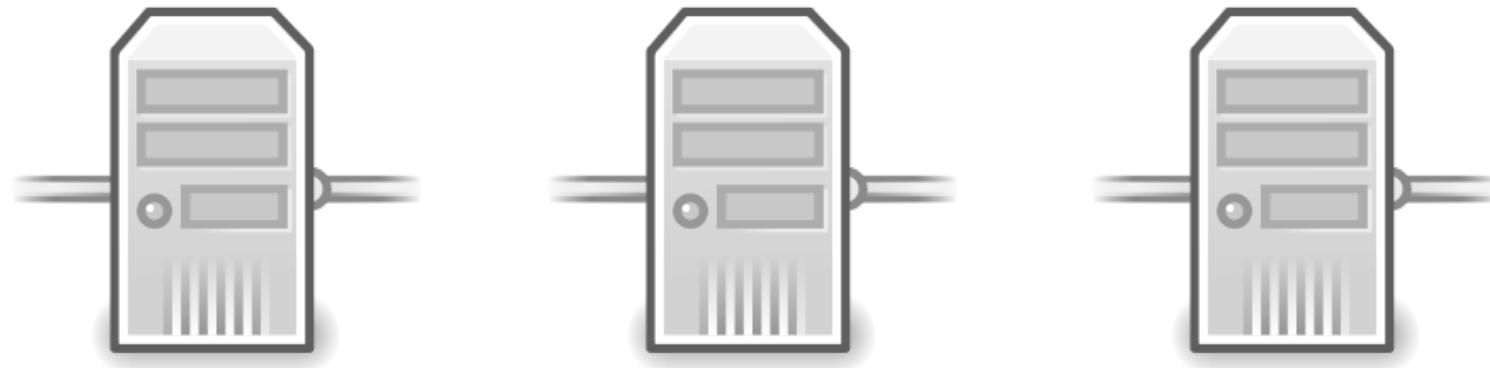




MIX Cascades



TECHNISCHE
UNIVERSITÄT
DARMSTADT

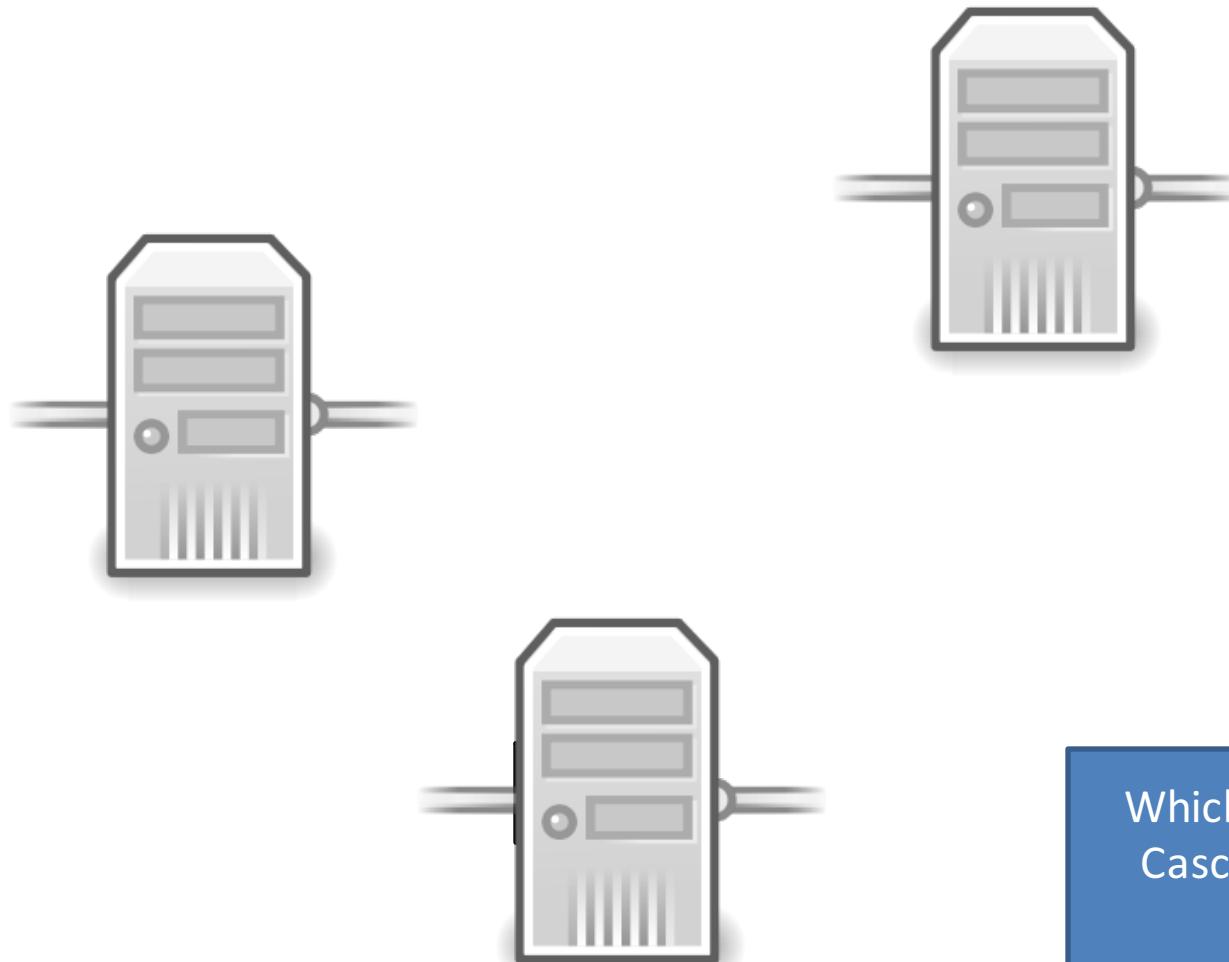




Free Routes



TECHNISCHE
UNIVERSITÄT
DARMSTADT

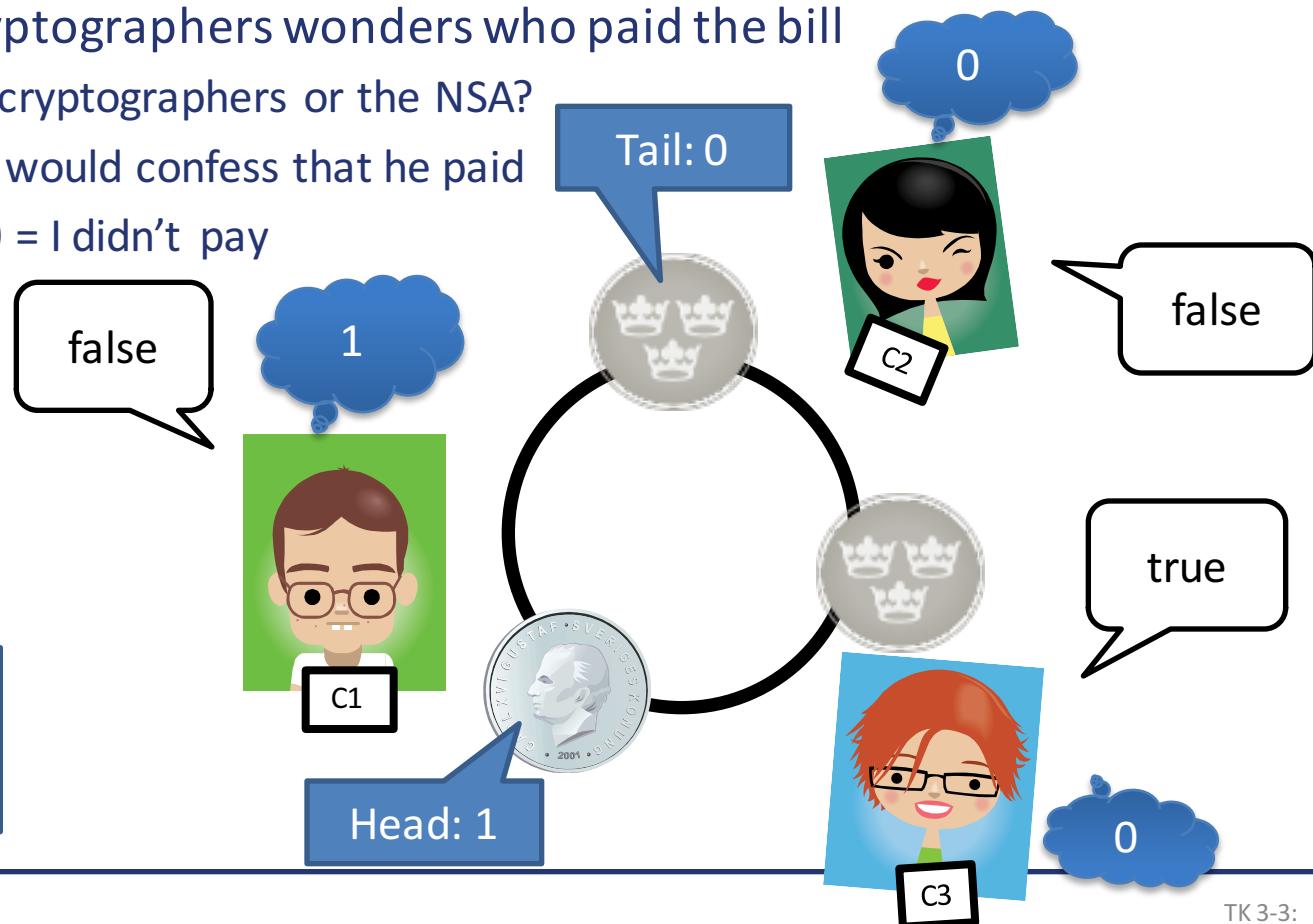




Is information theoretic anonymity possible



- DC-Nets
- A short tale about dining cryptographers
 - A group of cryptographers wonders who paid the bill
 - One of the cryptographers or the NSA?
 - But no one would confess that he paid
 - $1 = \text{I paid}, 0 = \text{I didn't pay}$

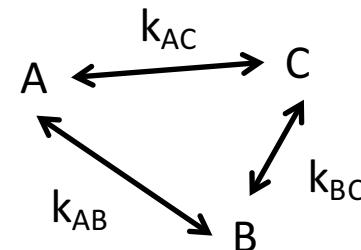




DC Nets – Binary Superposed



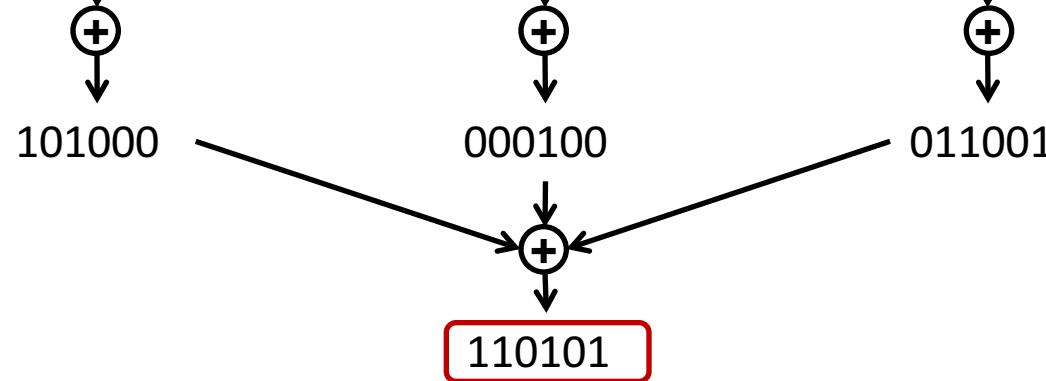
Sender and Receiver Anonymity



A
$m_A = 110101$
$k_{AB} = 101011$
$k_{AC} = 110110$

B
$m_B = 000000$
$k_{AB} = 101011$
$k_{BC} = 101111$

C
$m_C = 000000$
$k_{BC} = 101111$
$k_{AC} = 110110$





Anonymous Communication!

We are Safe!

Really?

A large, solid red arrow points diagonally downwards from the text "We are Safe!" towards a red rectangular box containing the word "Really?".



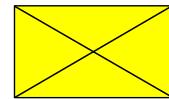
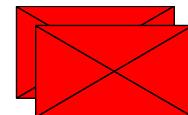
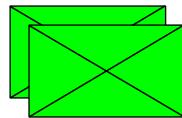
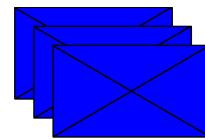
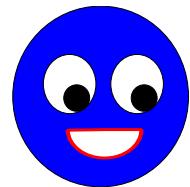
Application Layer Information



System Model



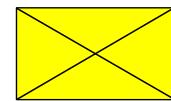
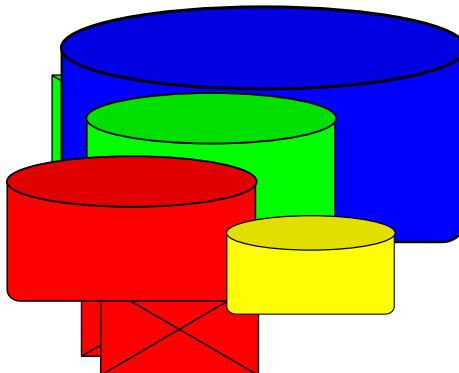
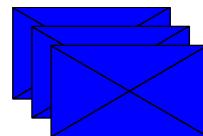
TECHNISCHE
UNIVERSITÄT
DARMSTADT



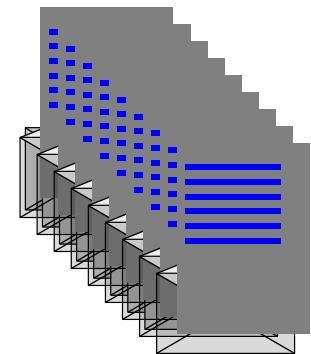
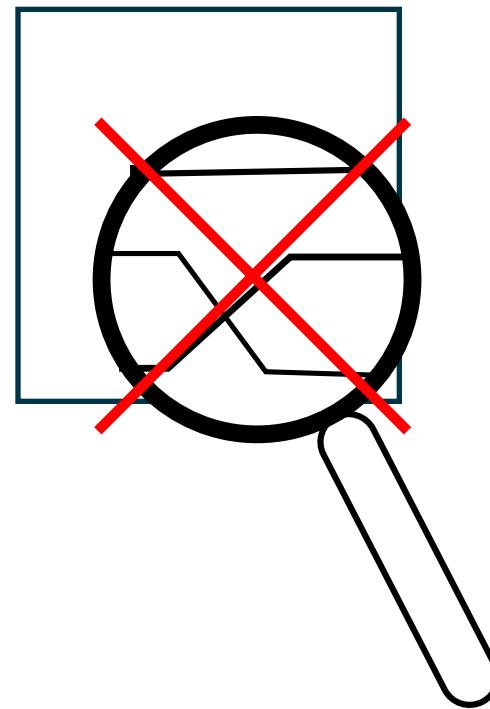
Mix



Attacker Knowledge



Traffic Data



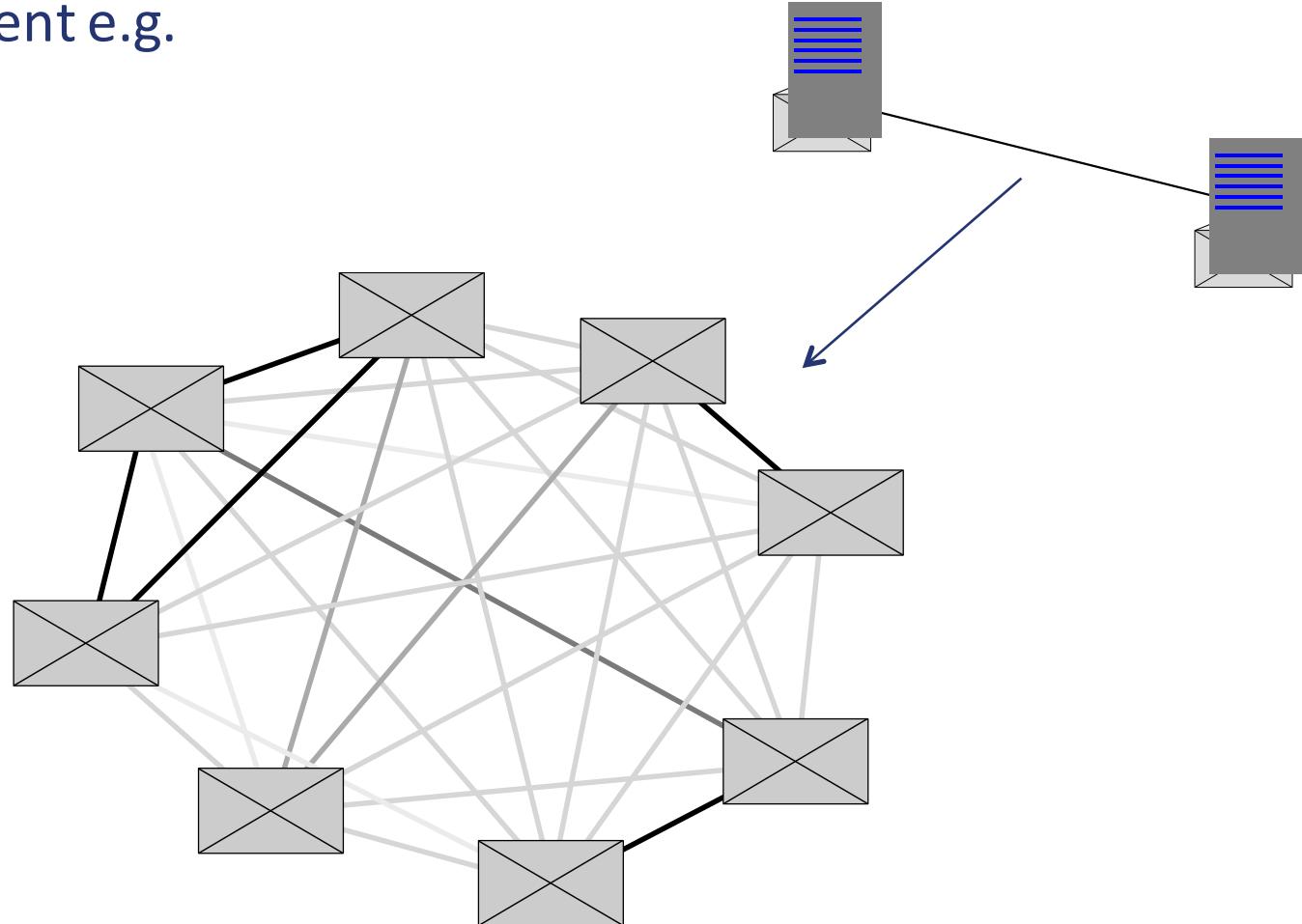
Application Data



Linkability Information

Message Content e.g.

- Language
- Context
- Style

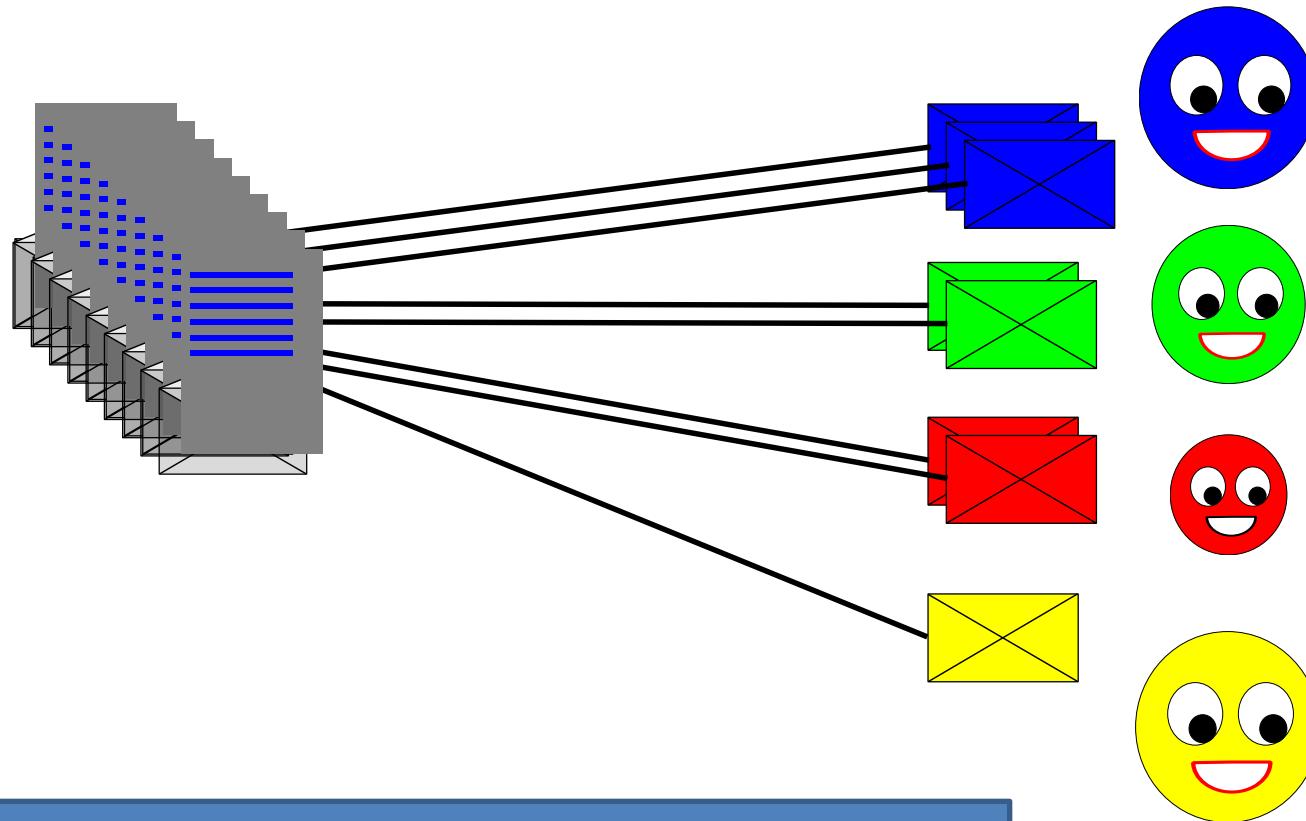




Attacker Aim



- To map anonymized messages to senders

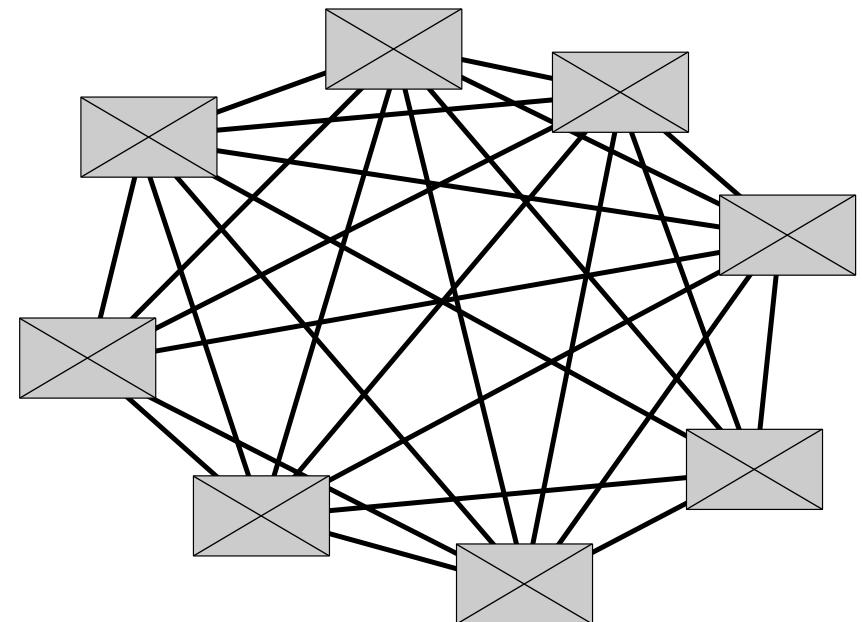
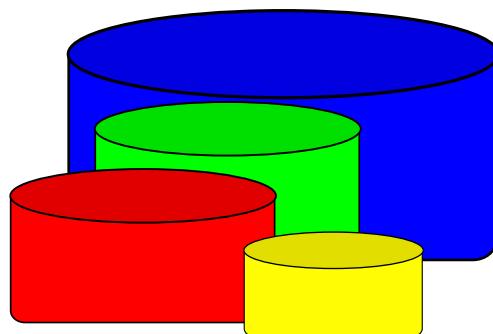


Note: this is not mapping a given ingoing message to a certain outgoing message!



Random Attacker

Number of messages



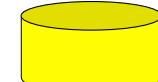
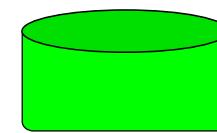
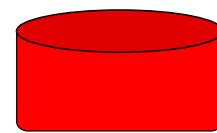
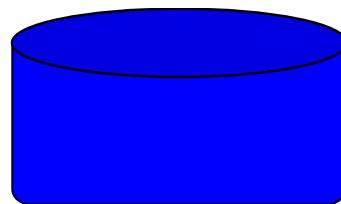
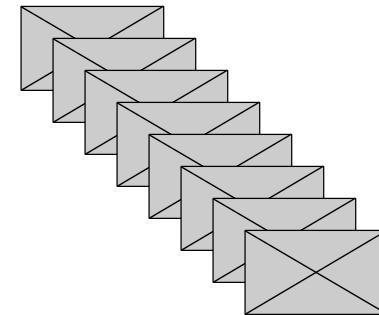
No linkability information



Random Attack



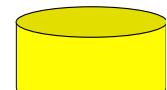
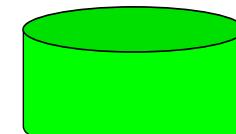
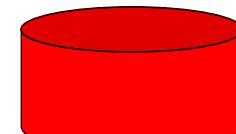
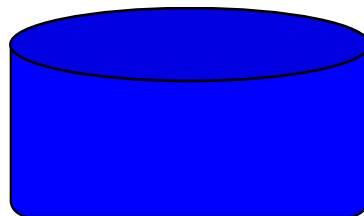
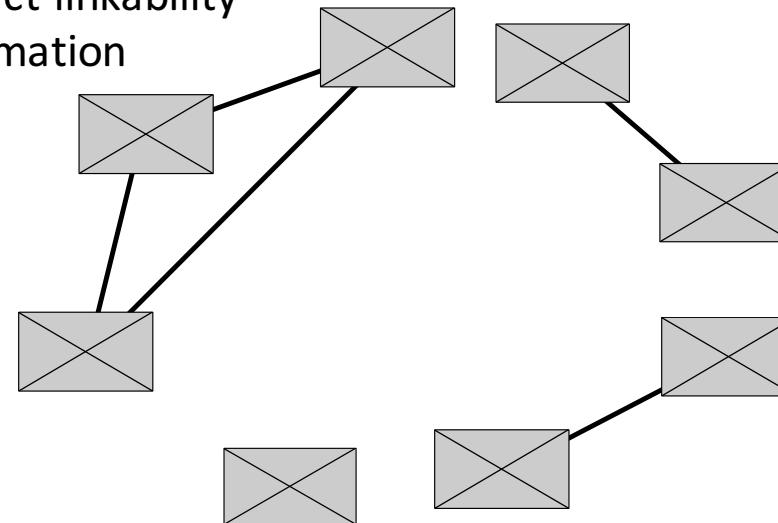
TECHNISCHE
UNIVERSITÄT
DARMSTADT





Perfect Attack

perfect linkability
information

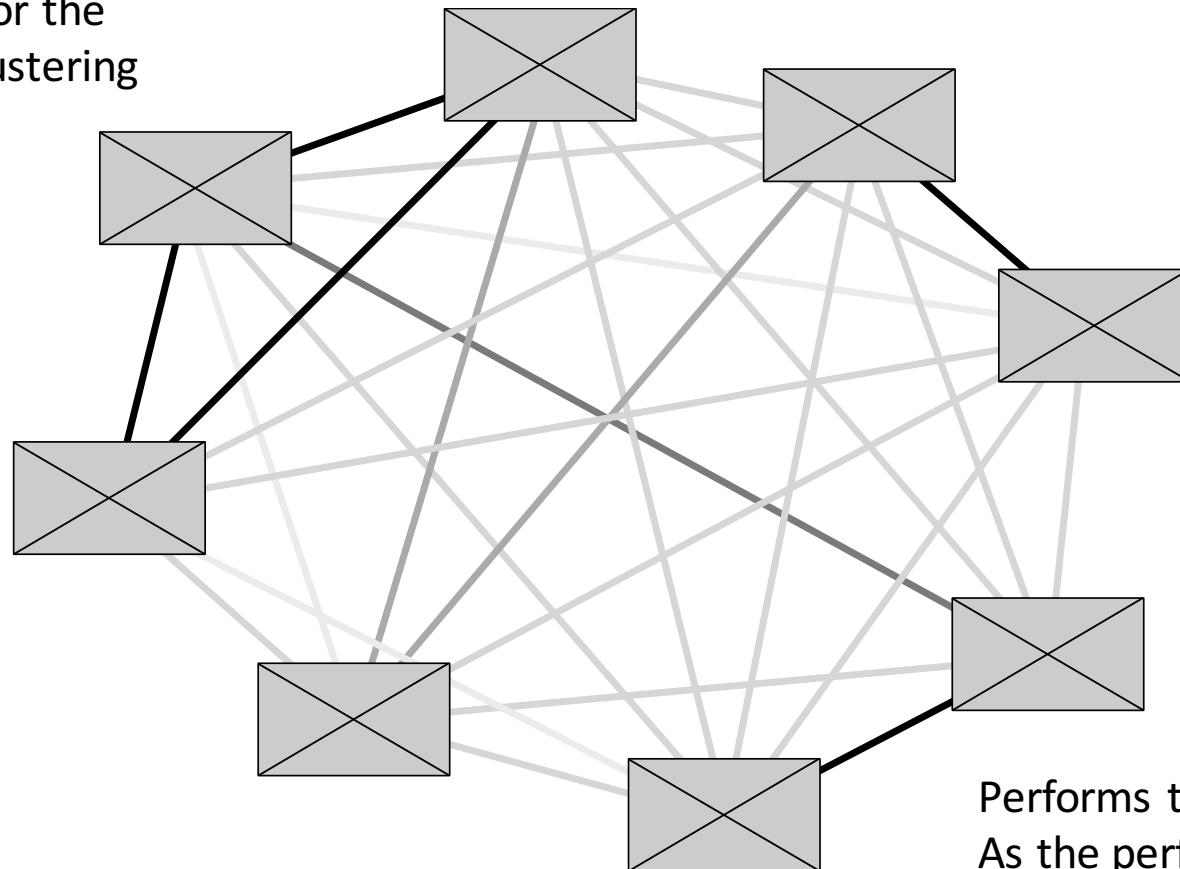


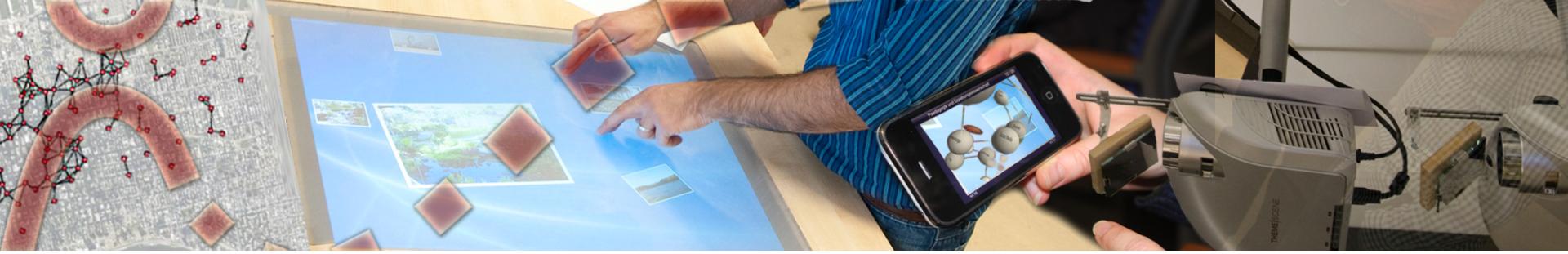
same # of messages



Noisy linkability information

Searches for the optimal clustering





Smart Meter Privacy

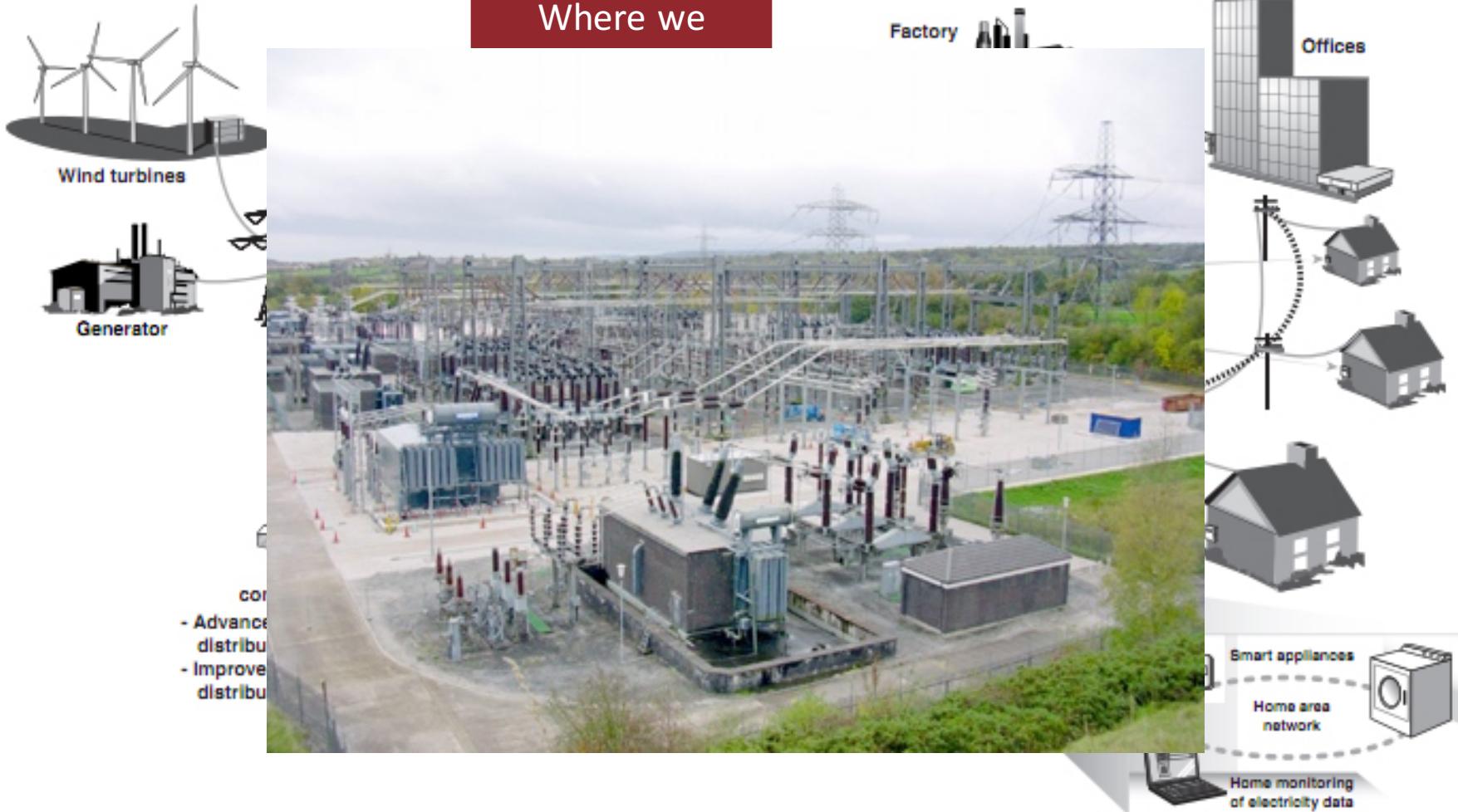


Smart Grid Anatomy



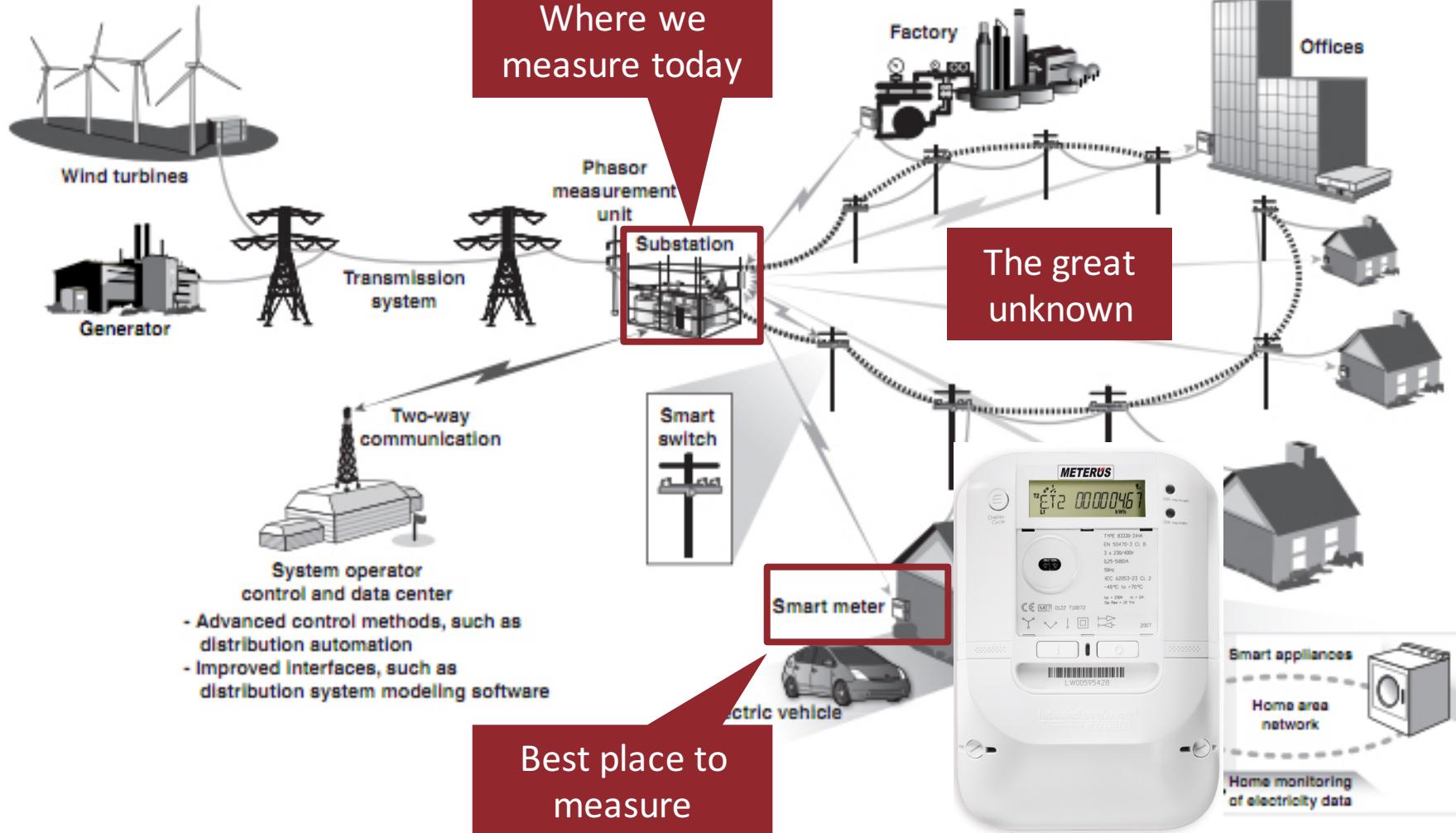
TECHNISCHE
UNIVERSITÄT
DARMSTADT

Where we





Smart Grid Anatomy





Smart Meter Privacy Issue



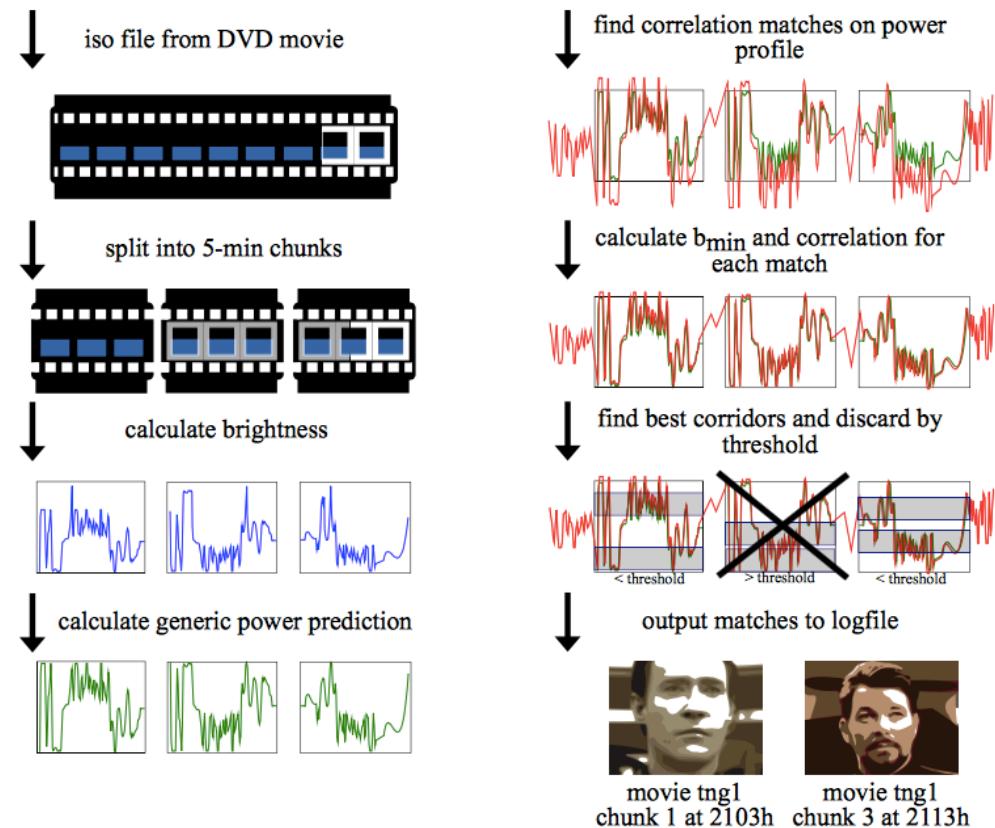
Greveler 2012
Smart Meter pilot project
Real meter
Real energy supplier
Real plain HTTP
2s intervals

Flat screen TV:
more white →
more power

```
POST /api/w.html HTTP/1.1
Content-Type: application/
Host:85.214.93.99
Content-Length:851
```

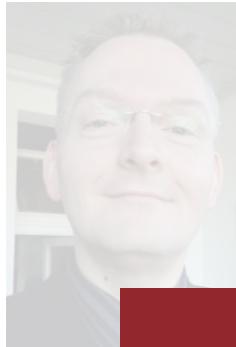
```
version=0.9&identity=
{"meterdata": "00000285.9822239*kWh", "seconds": "399511319.61"}, {"meterdata": "00000285.9824793*kWh", "seconds": "399511321.61"}, {"meterdata": "00000285.9826075*kWh", "seconds": "399511323.61"}, {"meterdata": "00000285.9827358*kWh", "tickdelta": "00000285.982636*kWh", "seconds": "399511325.62"}, {"meterdata": "00000285.9828636*kWh", "tickdelta": "00000285.9827358*kWh", "seconds": "399511327.62"}, {"meterdata": "00000285.9829915*kWh", "tickdelta": "00000285.9828636*kWh", "seconds": "399511329.62"}, {"meterdata": "00000285.9831196*kWh", "tickdelta": "00000285.9829915*kWh", "seconds": "399511331.62"}, {"meterdata": "00000285.9832476*kWh", "tickdelta": "00000285.9831196*kWh", "seconds": "399511333.62"}]
&now=399511335.65
```

00000285.9822239*kWh", "seconds": "399511319.61"},
00000285.9823514*kWh", "seconds": "399511321.61"},

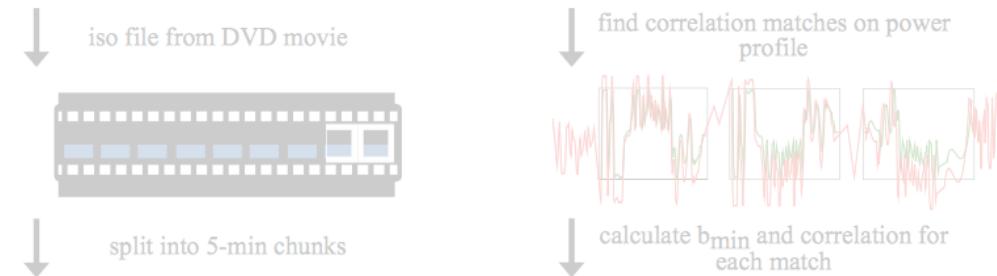




Smart Meter Privacy Issue



Greveler 2012
Smart Meter pilot project
Real meter
Real energy supplier
Real plain HTTP

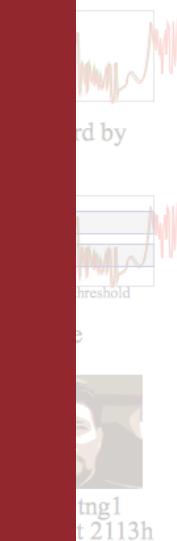


- No privacy!
- Energy supplies learns absolutely everything!
- Noise (fridge, etc) does NOT help!
- 80% of EU households with smart meter until 2020
- Clear need for technical privacy protection

POST /api/wifi
Content-Type: application/json
Host: 85.214.8.1
Content-Length: 103

version=0.98
{"meterdata":
{"meterdata":
{"meterdata":
{"meterdata":
{"meterdata":
{"meterdata":
{"meterdata":
{"meterdata":
&now=39951}

0000
0000



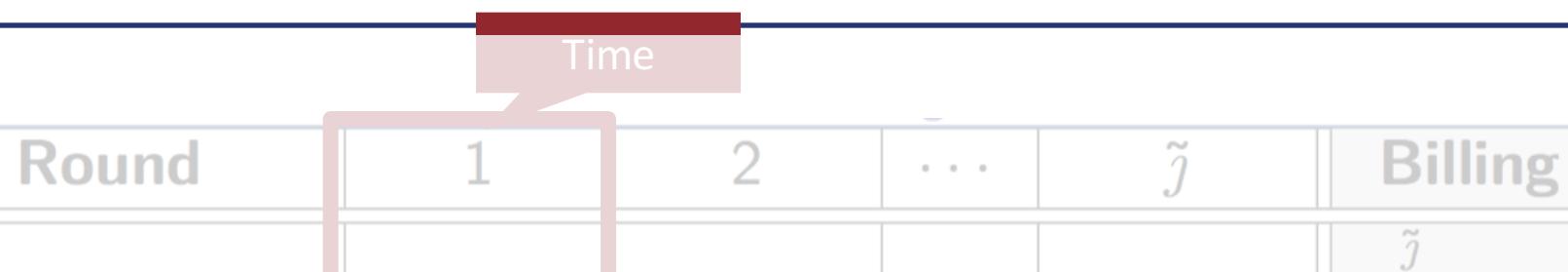


Smart Metering Goals

Round	1	2	...	\tilde{j}	Billing
Meter 1	$m_{1,1}$	$m_{1,2}$...	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$...	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
:	:	:	..	:	:
Meter \tilde{i}	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$...	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidated	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$...	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	=

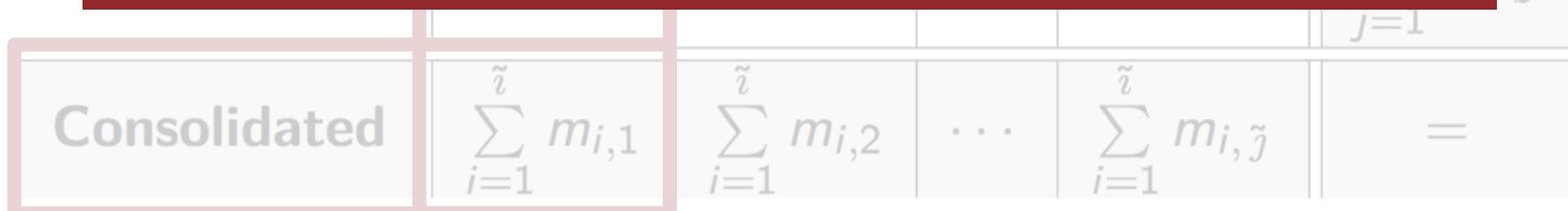


Smart Metering Goals



Goals:

1. Billing—Aggregation over rounds (per meter)
 - E.g., monthly bills
2. Grid monitoring—Aggregation over meters (per round)
 - E.g., consumption per street





Smart Metering Protocol (1)



Meters



$m_{1,j}$



$m_{2,j}$



$m_{3,j}$

⋮



$m_{i,j}$

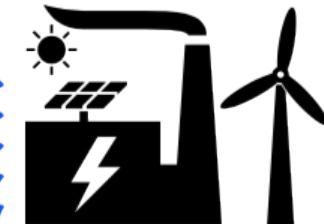
Measurement $m_{i,j}$

Meter i

Round j (second, minute)

Round: j

Supplier





Smart Metering Protocol (2)



Meters



1) Need encryption to protect against external attacker.



$m_{2,j}$



$m_{1,j}$

⋮



$m_{i,j}$

Measurement $m_{\{i,j\}}$
Meter i
Round j (second, minute)

Round: j

Supplier





Smart Metering Protocol (3)



Meters



1) Need encryption to protect against external attacker.



$\text{Enc}(m_{2,j})$



$\text{Enc}(m_{3,j})$

:



$\text{Enc}(m_{i,j})$

2) Need aggregation to protect against internal attacker.

Round: j

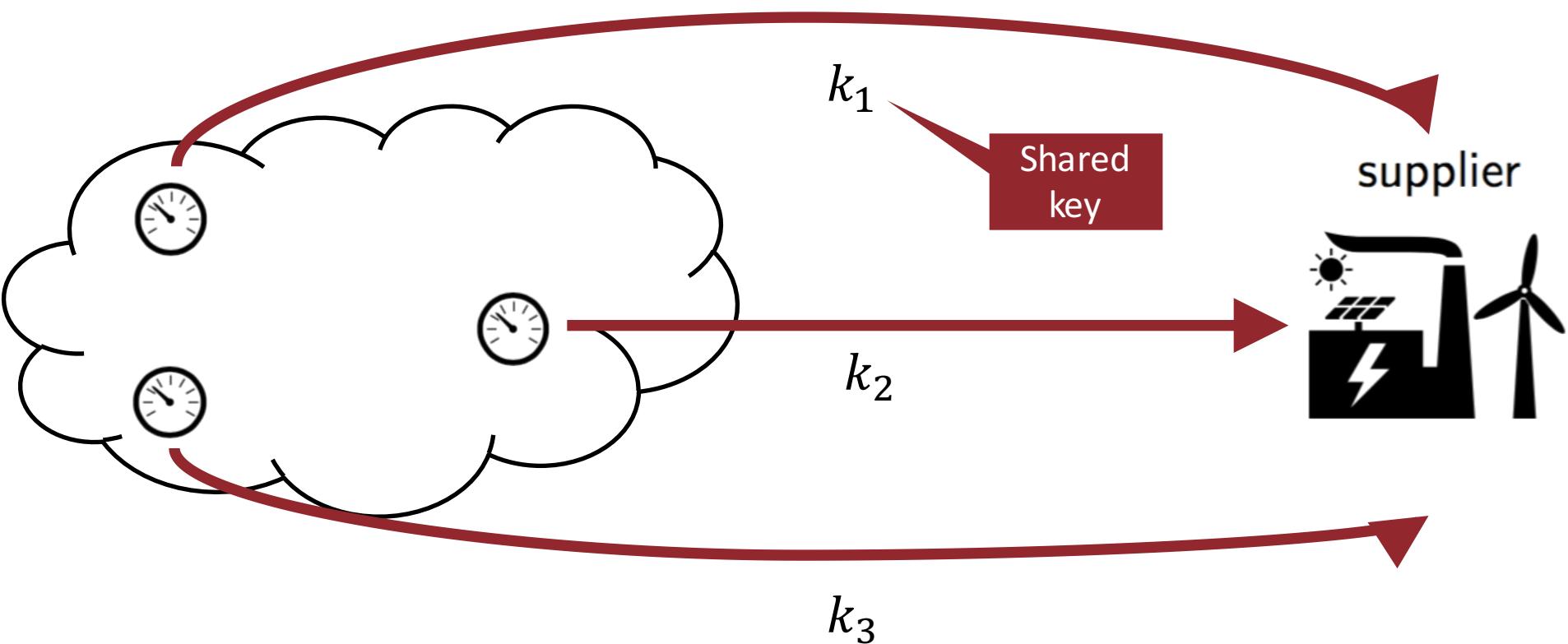
Supplier





In Network Aggregation (PPP1)

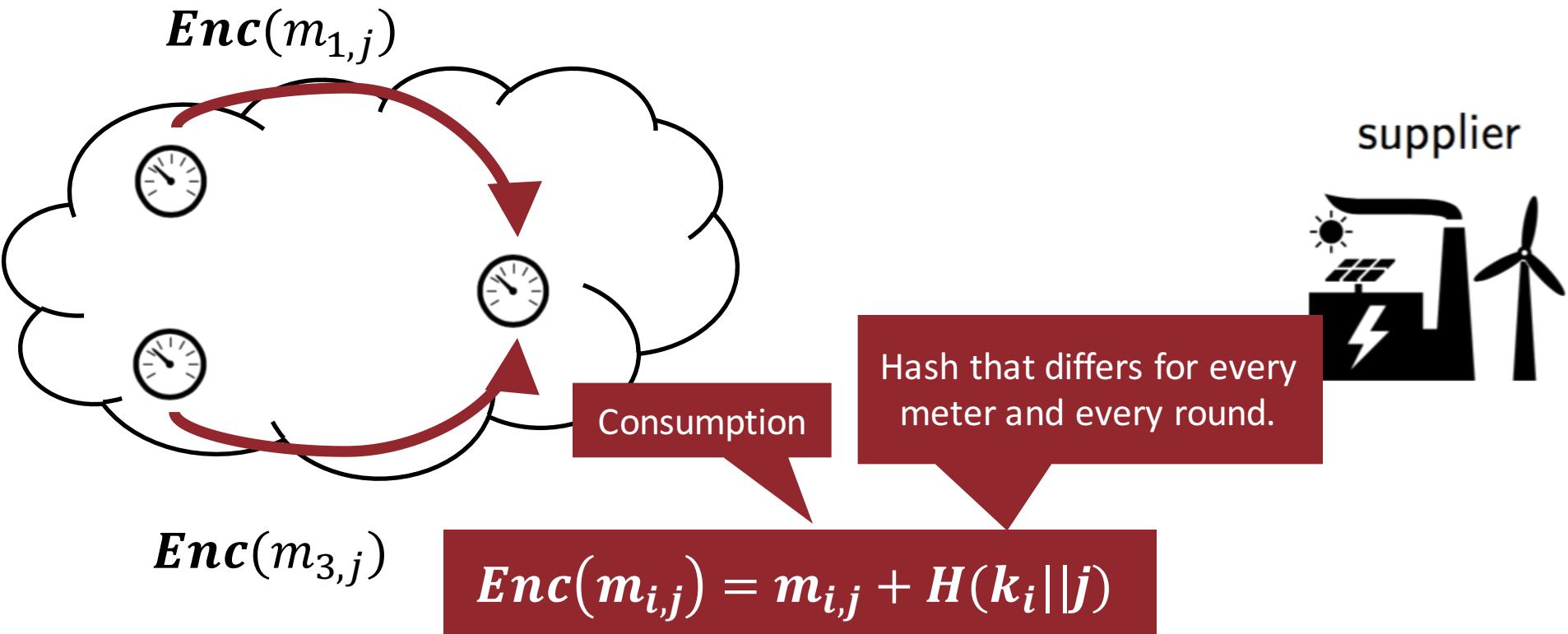
Step 0 (setup)





In Network Aggregation (PPP1)

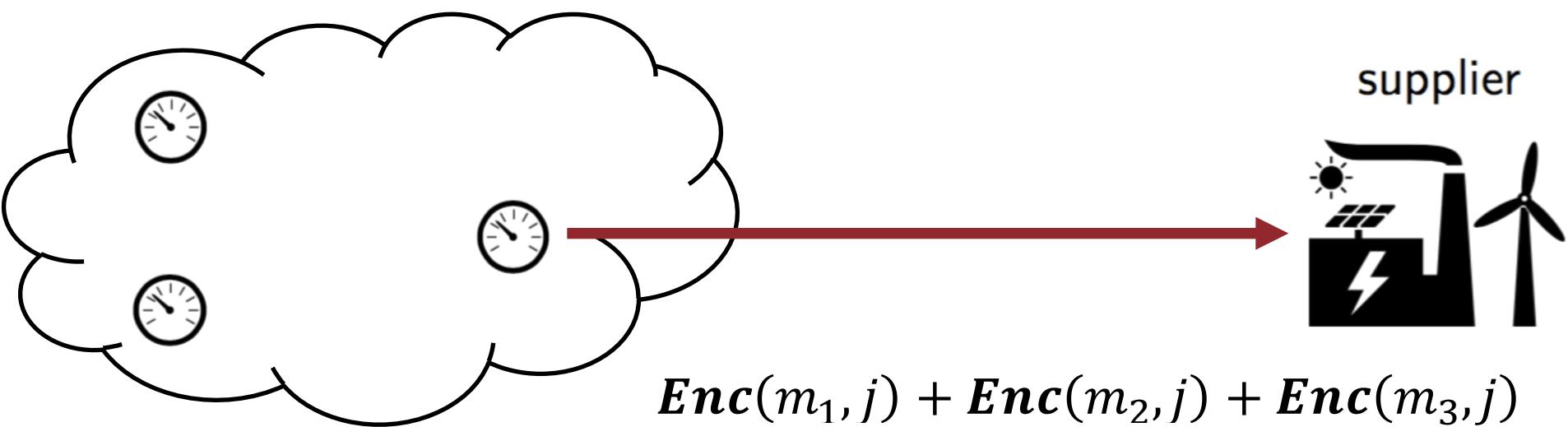
Step 1





In Network Aggregation (PPP1)

Step 2

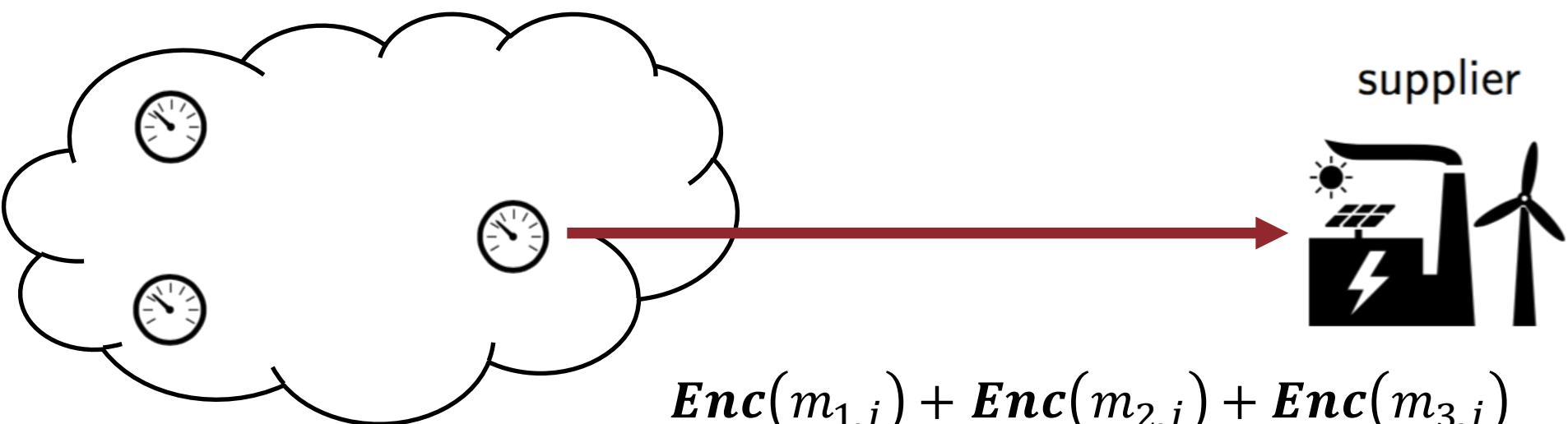




In Network Aggregation (PPP1)



Step 2



$$\begin{aligned} & \mathbf{Enc}(m_{1,j}) + \mathbf{Enc}(m_{2,j}) + \mathbf{Enc}(m_{3,j}) \\ &= \mathbf{Enc}(m_{1,j} + m_{2,j} + m_{3,j}) = C \end{aligned}$$



In Network Aggregation (PPP1)



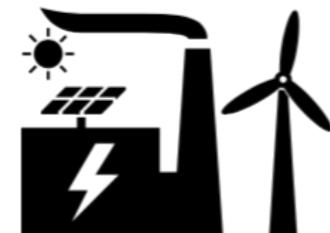
Step 3

$$C = \text{Enc}(m_{1,j} + m_{2,j} + m_{3,j})$$



$$\text{Dec}(C) = C - \sum_{i=1}^N H(k_i || j) = \sum_{i=1}^N m_{i,j}$$

supplier



Aggregate over
meters



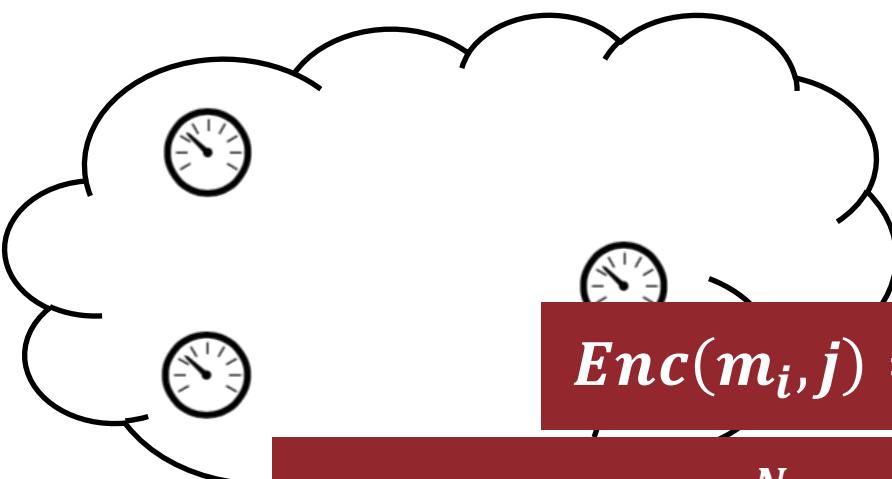
In Network Aggregation (PPP1)



Borges 2014
DC-Net

Step 3

$$C = \text{Enc}(m_{1,j} + m_{2,j} + m_{3,j})$$



$$\text{Enc}(m_{i,j}) = m_{i,j} + H(k_i || j)$$

$$\text{Dec}(C) = C - \sum_{i=1}^N H(k_1 || j) = \sum_{i=1}^N m_{i,j}$$



Aggregate over
meters



Take home message



- Privacy protection is a legal requirement
- Data minimization is the technical mean to protect privacy
- Anonymous communication is the basis
 - MIX (practical)
 - DC-Net (theoretical bounds)
- Application layer info can be used for attacks
- Smart Metering as application of DC-Nets
- **Do not try this at home**



Further Reads



- Terminology
 - Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology
http://dx.doi.org/10.1007/3-540-44702-4_1
 - For General understanding of anonymous communication
 - Untraceable electronic mail, return addresses, and digital pseudonyms
<http://dl.acm.org/citation.cfm?id=358563>
 - The dining cryptographers problem: *Unconditional sender and recipient untraceability*
<http://link.springer.com/article/10.1007/BF00206326>
 - For Application Layer Privacy
 - Using Linkability Information to Attack Mix-Based Anonymity Services
<https://www.cosic.esat.kuleuven.be/publications/article-1215.pdf>
 - For Smart Metering Privacy
 - iKUP keeps users' privacy in the Smart Grid
<http://dx.doi.org/10.1109/CNS.2014.6997499>