Privacy in Smart Grids

Andreas Unterweger

Josef Ressel Center for
User-Centric Smart Grid Privacy, Security and Control
Salzburg University of Applied Sciences

Slides by D. Engel, G. Eibl and F. Knirsch are gratefully acknowledged.

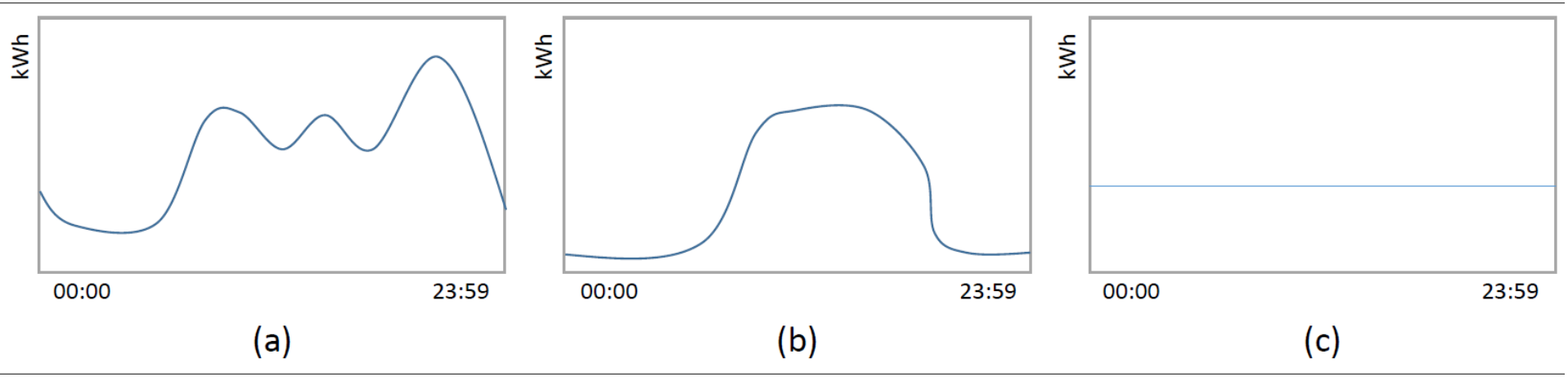
Overview

- What are Smart Grids?
- What could go wrong?
- What can be done about it?
- What is there to do still?

What are Smart Grids?

Renewable energy sources and electro-mobility

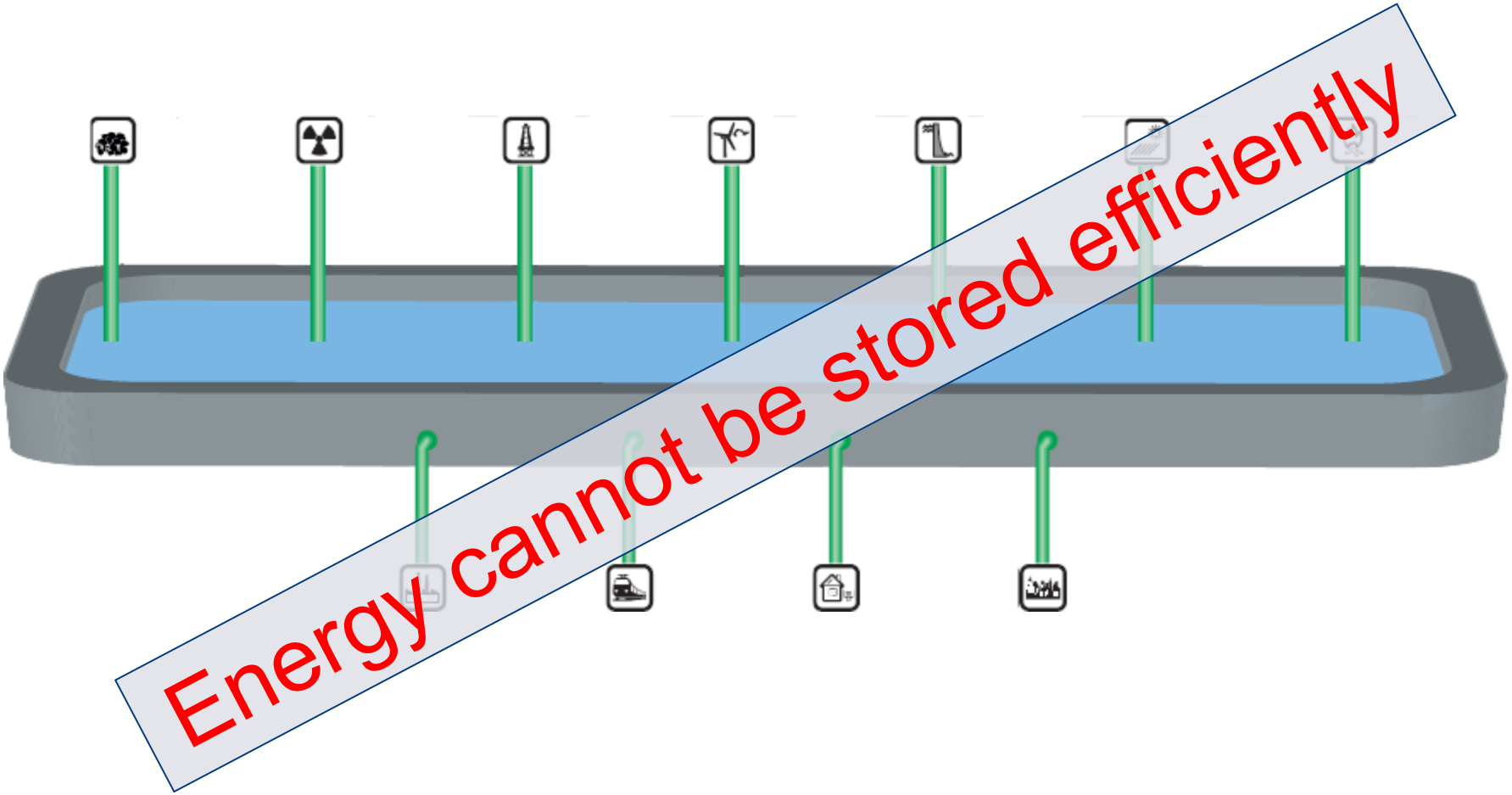
Supply vs. demand



- (a) Typical customer demand
- (b) Supply from solar power on a sunny day
- (c) Supply from a coal-fired power plant

- Supply forecasting depends on type(s) of energy source(s)

So, where is the problem?



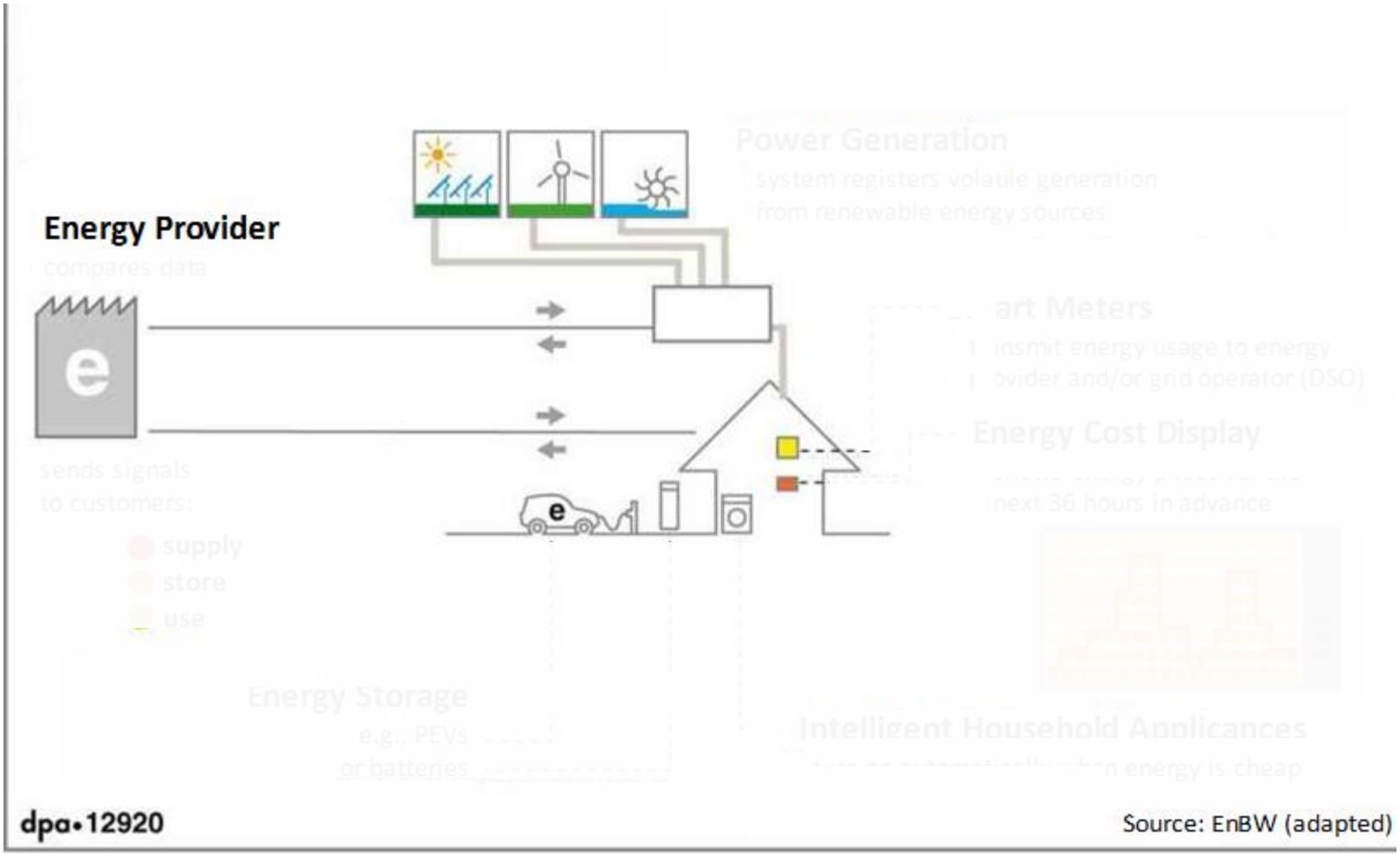
Adopted from M. Dalheimer: „Power to the People – Das Stromnetz der Zukunft“, Fraunhofer ITWM, 2010.

Goals

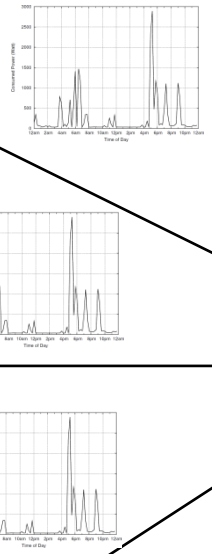
- Integration of renewable energy sources
- Real-time pricing → motivation for customers to shift demand
- Network stability

- By 2020: Smart meters in at least 80% of all households in the EU

The customer‘s (future) view



Smart Metering

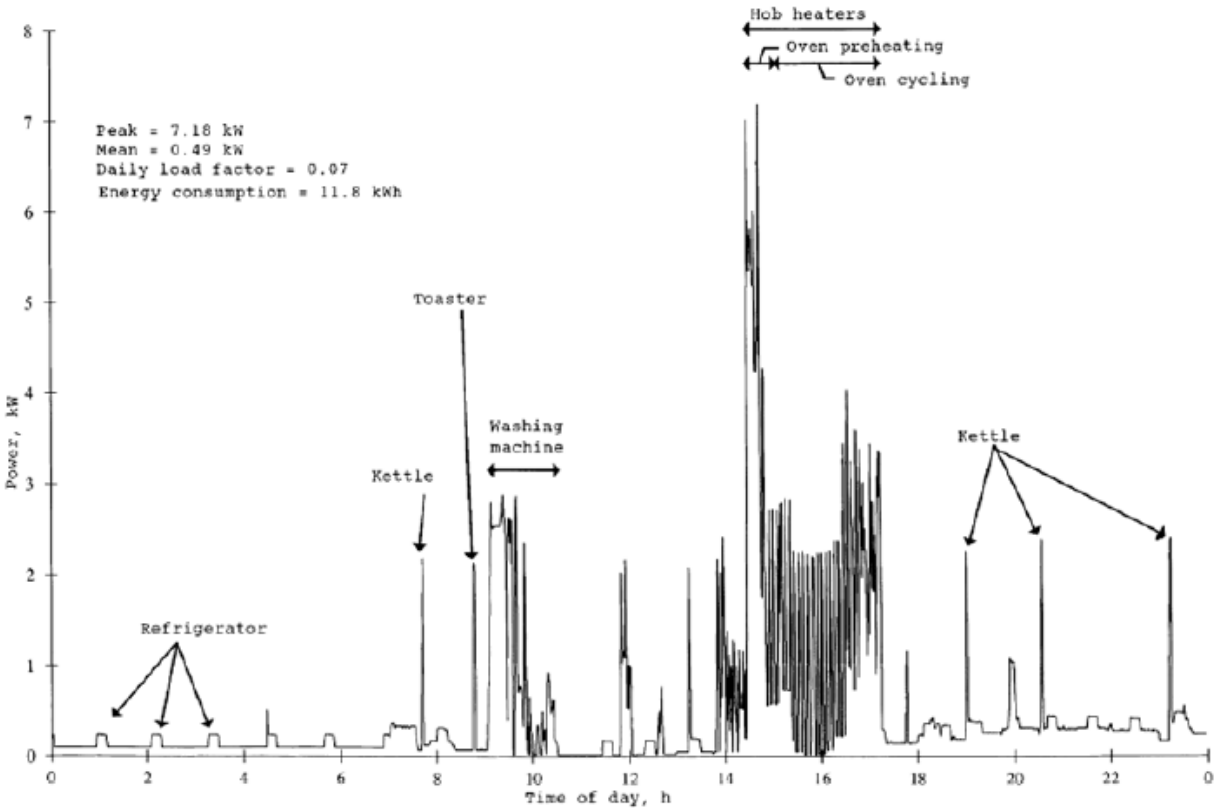


Data concentrator

Grid operator

What could go wrong?

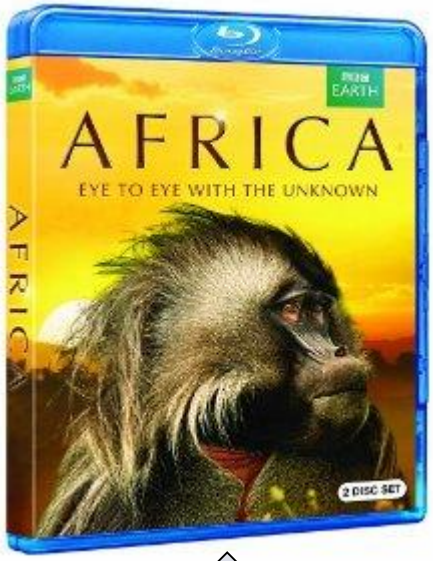
I know what your appliances are doing

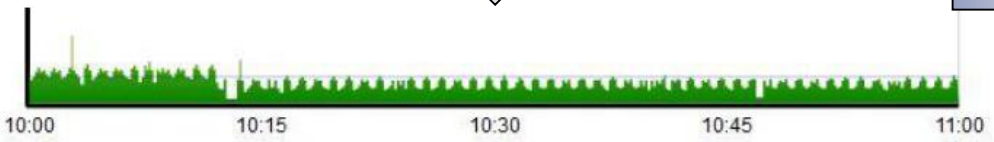


Source: Hart, G.: Nonintrusive appliance load monitoring. Proceedings of the IEEE, vol. 80, no. 12, pp. 1870-1891, 1992.

Source: EVB Energie AG,
http://en.wikipedia.org/wiki/File:Intelligenter_zaehler-_Smart_meter.jpg

I know what you are watching on TV





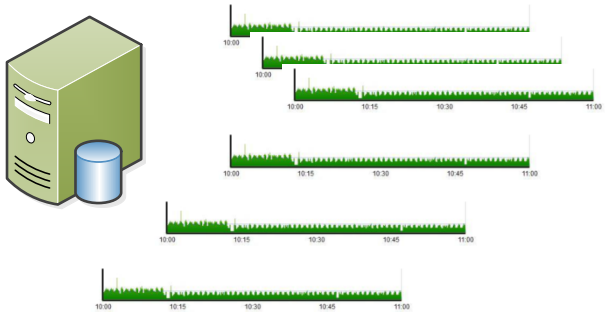
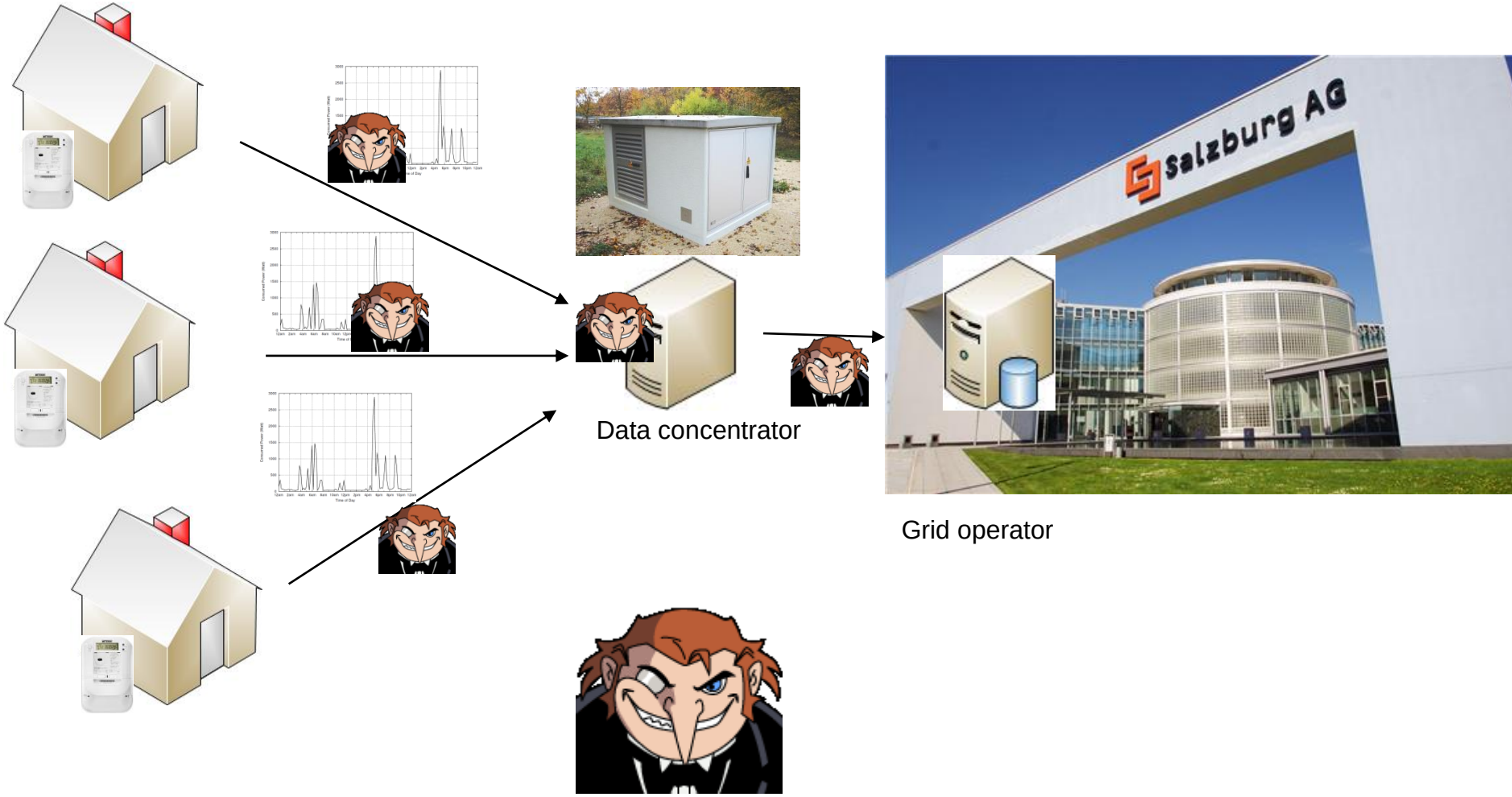


Image sources: Samsung (samsungmobile.us), Amazon (amazon.com)
Greveler, U.; Justus, B. & Löhr, D.: Multimedia Content Identification Through Smart Meter Power Usage Profiles *Proceedings of the 2012 International Conference on Information and Knowledge Engineering (IKE'12),* 2012.

What can be done about it?

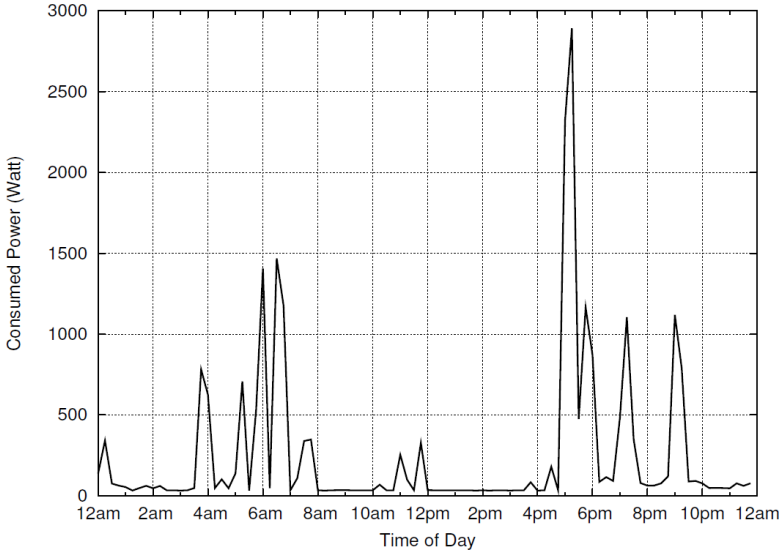
Smart Metering: Potential adversaries

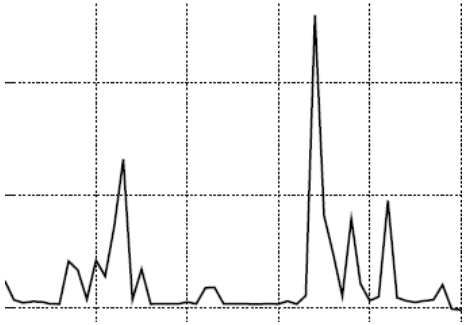


Approaches for privacy preservation

- Multiple resolutions
  - Without encryption
  - With selective encryption
- Aggregation
  - Without encryption
  - With masking
  - With homomorphic encryption

Multiple resolutions





The impact of resolution

- F measures for applicance recognition with edge detection

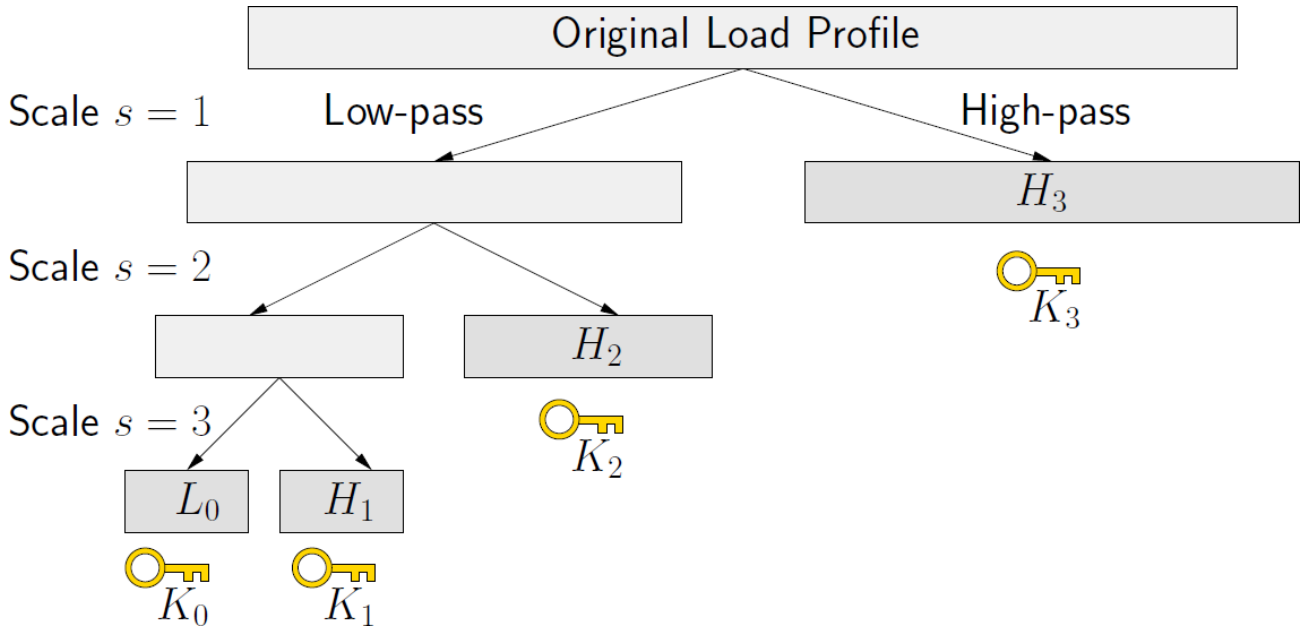
	3s	10s	30s	1m	5m	15m	1h
bathroom_gfi	0.64	0.62	0.76	0.39	0.00	0.00	0.00
dishwaser	0.83	0.51	0.32	0.28	0.04	0.00	0.00
kitchen_outlets2	0.43	0.49	0.47	0.57	0.47	0.33	0.00
kitchen_outlets3	0.81	0.68	0.65	0.52	0.00	0.00	0.00
kitchen_outlets4	0.42	0.37	0.38	0.00	0.00	0.00	0.00
lighting1	0.81	0.81	0.83	0.76	0.47	0.37	0.30
lighting2	0.86	0.90	0.92	0.92	0.91	0.83	0.43
lighting3	0.81	0.89	0.90	0.92	0.92	0.79	0.38
microwave	0.83	0.65	0.08	0.02	0.00	0.00	0.00
oven1	0.79	0.77	0.35	0.25	0.00	0.00	0.00
oven2	0.94	0.84	0.31	0.21	0.00	0.00	0.00
refrigerator	0.94	0.91	0.81	0.80	0.29	0.00	0.01
stove	0.77	0.00	0.00	0.00	0.00	0.00	0.00
washer_dryer1	0.72	0.73	0.47	0.35	0.00	0.00	0.00
washer_dryer3	0.99	0.78	0.21	0.12	0.00	0.00	0.00

Green: high privacy

Red: low privacy

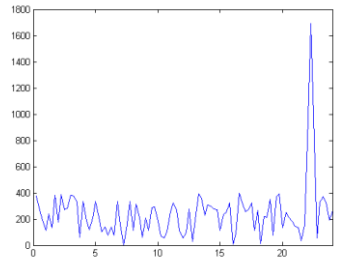
Encryption at multiple resolutions

- Load profiles are stored at multiple resolutions (scales)
- Every resolution is assigned its own key
- User decides who has access to which data (resolution)

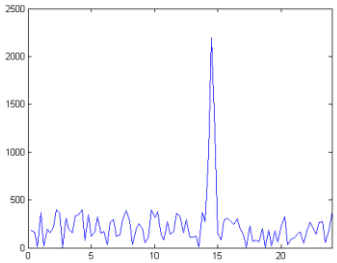


Load profile aggregation

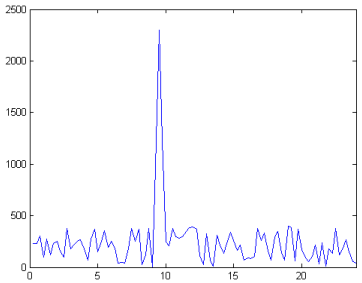
SM_1



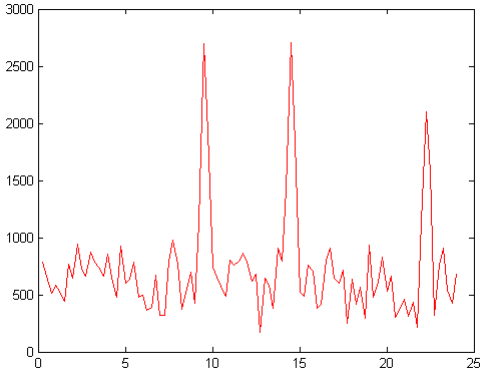
SM_2



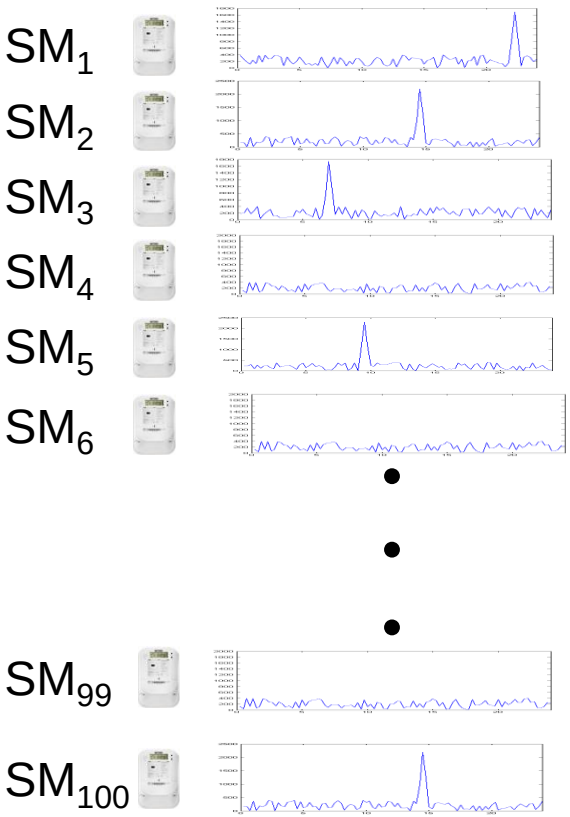
SM_3



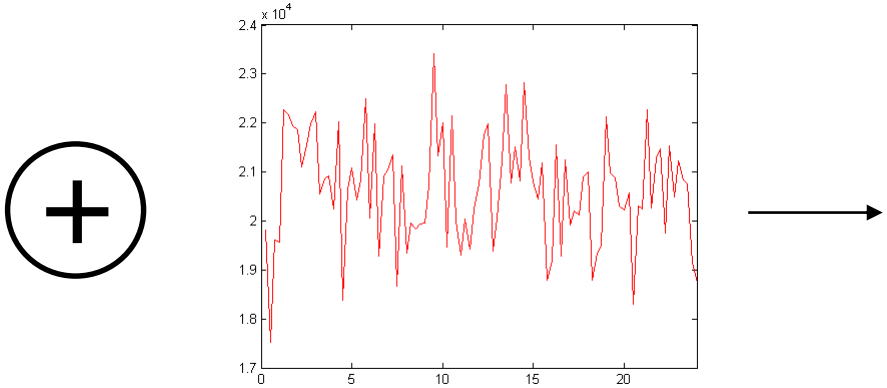
Data concentrator



Load profile aggregation (ctd.)



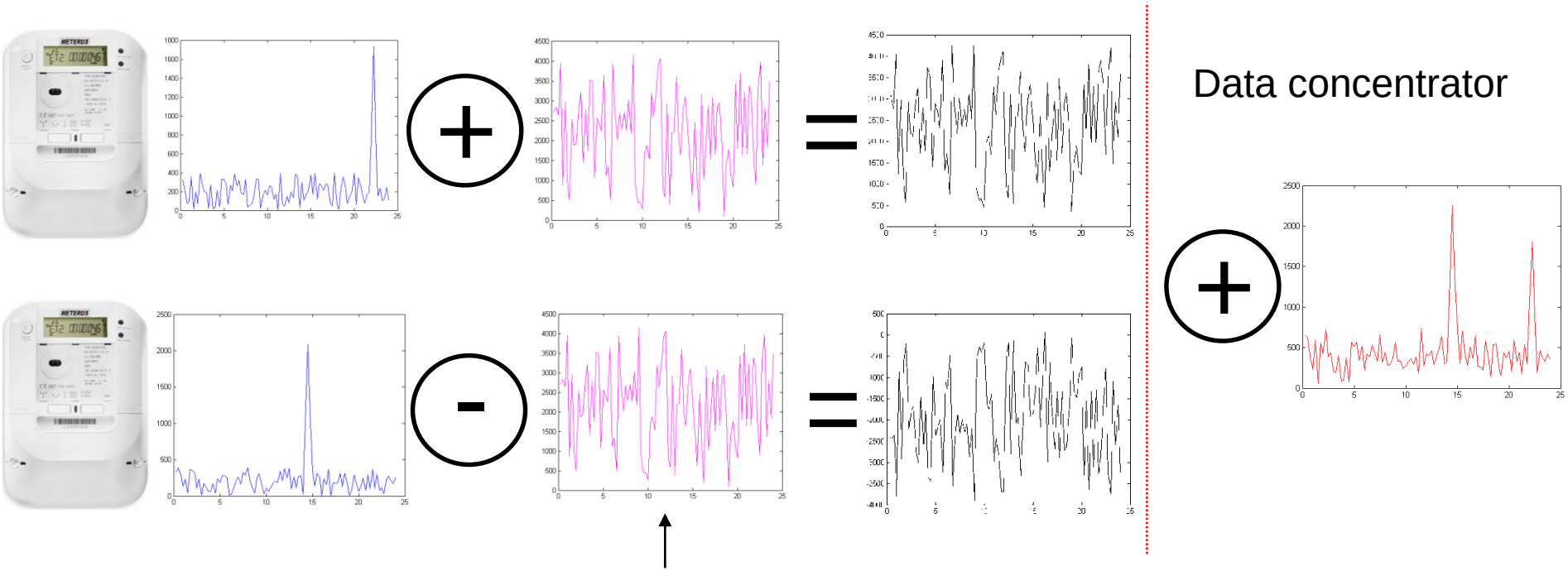
Data concentrator



Aggregated signals hide individual contributions

Data concentrator should only get the aggregated signal

Aggregation with masking



Pairwise identical random share

$(m_1+r_{12}) + (m_2-r_{12}) = m_1+m_2$

„One-way“ functions (with a catch)

Idea by Klaus Kursawe

Homomorphic encryption

$x \rightarrow g^x$

+

+

$y \rightarrow g^y$

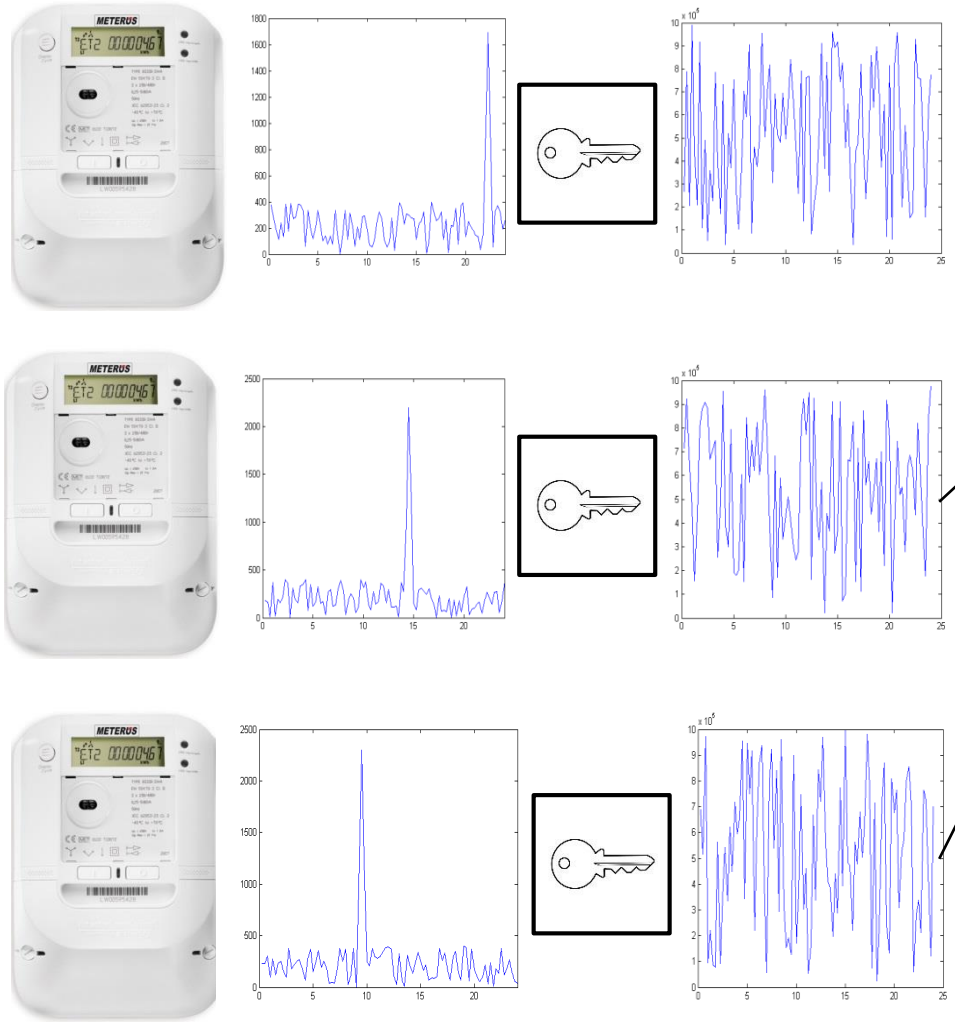
=

=

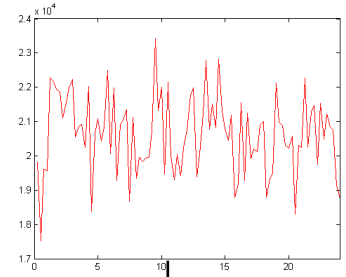
$x \cdot y \rightarrow g^{x+y}$

Idea by Klaus Kursawe

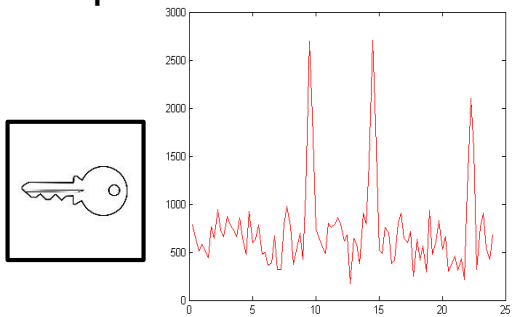
Aggregation with homomorphic encryption



Data concentrator



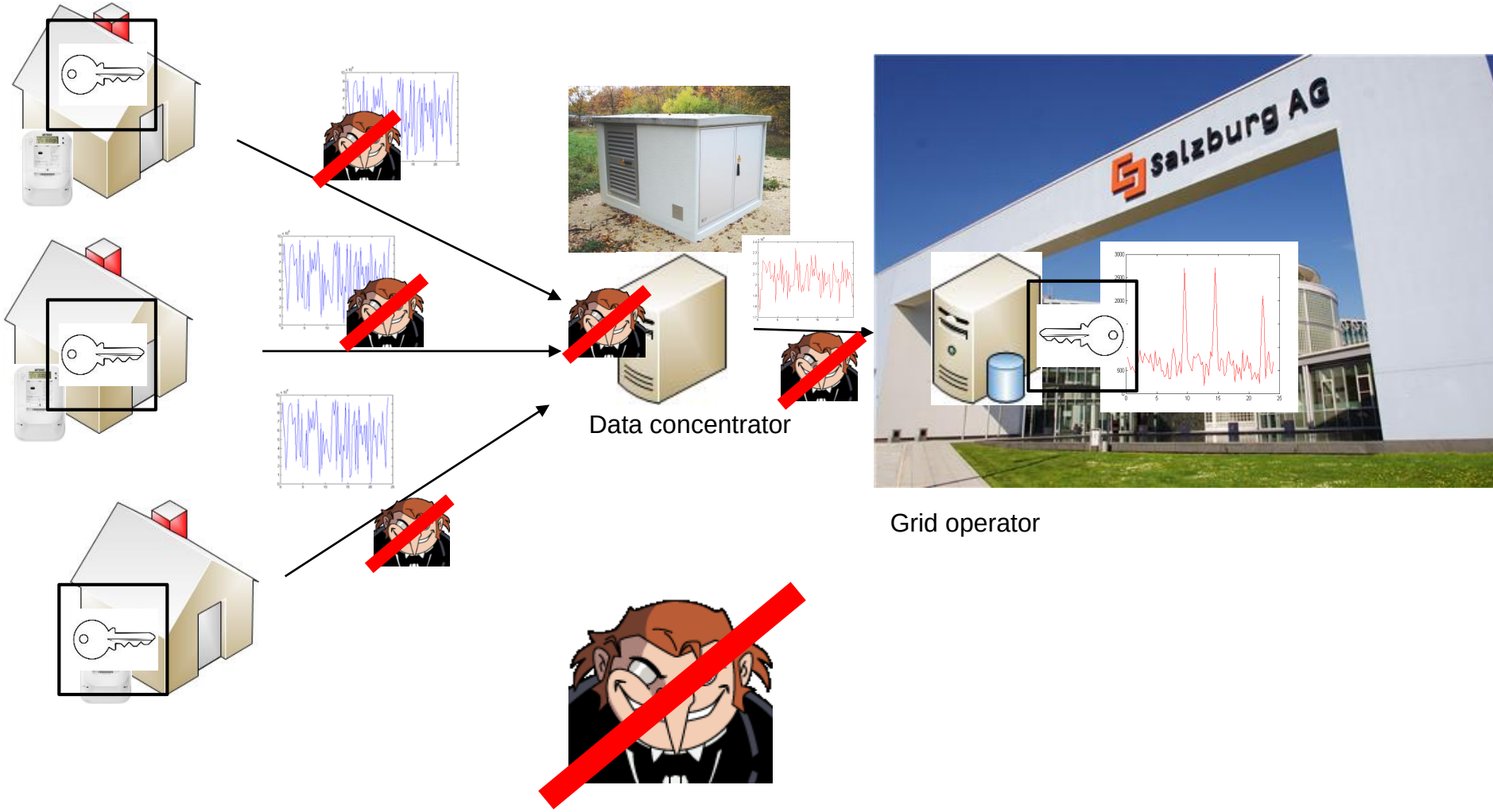
Grid operator



Homomorphic encryption:

$$D\big(E(m_1)\cdot E(m_2)\cdot E(m_3)\big) = m_1+m_2+m_3$$

Aggregation with homomorphic encryption (ctd.)



What is there to do still?

Open questions

- How to measure privacy?
  - Information-theoretic approaches exist
  - How to account for laws and legislation, e.g., GDPR?
  - What impact do aggregation, masking, … have?
- How to make smart meter users aware of privacy?
  - Issue not specific to smart metering
  - Educating to avoid ignorance/fear
  - Increasing acceptance does not solve privacy issues
- How to speed up the adoption of privacy-preserving approaches?
  - Many proposed algorithms in the literature, few used in practice
  - Grid operators can‘t switch equipment/algorithms monthly
  - Customers may not care about what they can‘t see (“invisible changes“)

Thank you for your attention!

Questions?