A Privacy-Enhancing Protocol that Provides In-Network Data Aggregation and Verifiable Smart Meter Billing

IEEE ISCC 2014

Fábio Borges, Denise Demirel, Leon Böck, Johannes Buchmann, and Max Mühlhäuser

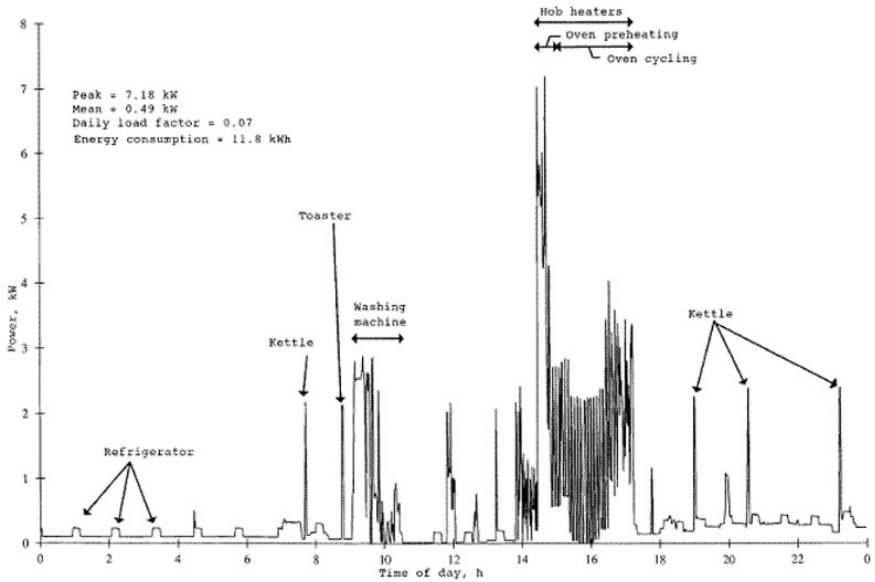
Technische Universität Darmstadt – Telecooperation Lab
Center for Advanced Security Research Darmstadt (CASED)

Table of Contents

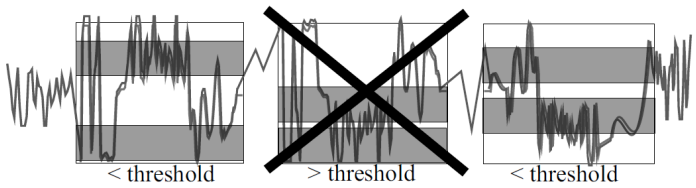
Outline

TECHNISCHE UNIVERSITÄT DARMSTADT

Privacy Problem



[NIST]



output matches to logfile

movie tng1
chunk 1 at 2103h

movie tng1
chunk 3 at 2113h

[Greveler et al., 2012]

Deployment

TECHNISCHE UNIVERSITÄT DARMSTADT

80% of households equipped with smart meters by 2020 in EU [EUD, 2012]

Spatiotemporal consumption

Consolidated Measurements and Verifiable Billing

TECHNISCHE UNIVERSITÄT DARMSTADT

Time Slot	$t = 1$	$t = 2$	$\cdots$	$t = T$	Bill
Customer 1 	m_{1_1}	m_{1_2}	$\cdots$	m_{1_T}	$\sum_{t=1}^{T} m_{1_j}$
Customer 2 	m_{2_1}	m_{2_2}	$\cdots$	m_{2_T}	$\sum_{t=1}^{T} m_{2_j}$
$\vdots$ 	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Customer N 	m_{N_1}	m_{N_2}	$\cdots$	m_{N_T}	$\sum_{t=1}^{T} m_{N_j}$
Consumption	$\sum_{i=1}^{N} m_{i_1}$	$\sum_{i=1}^{N} m_{i_2}$	$\cdots$	$\sum_{i=1}^{N} m_{i_T}$	✓

Time Series

One Round of Measurements

TECHNISCHE UNIVERSITÄT DARMSTADT

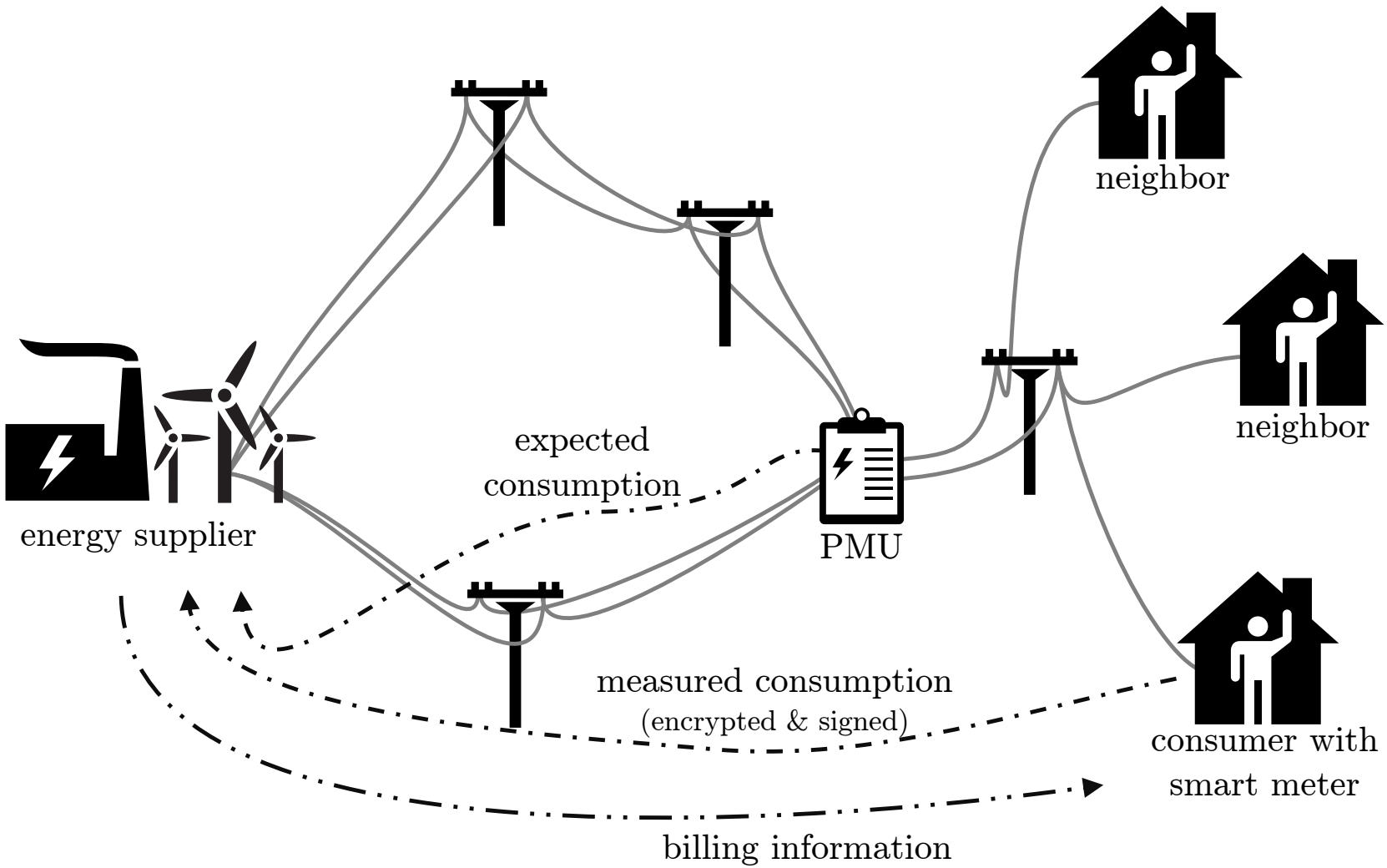
- e-voting
- mobile sensing
- sensor networks
- e-cash

Table of Contents

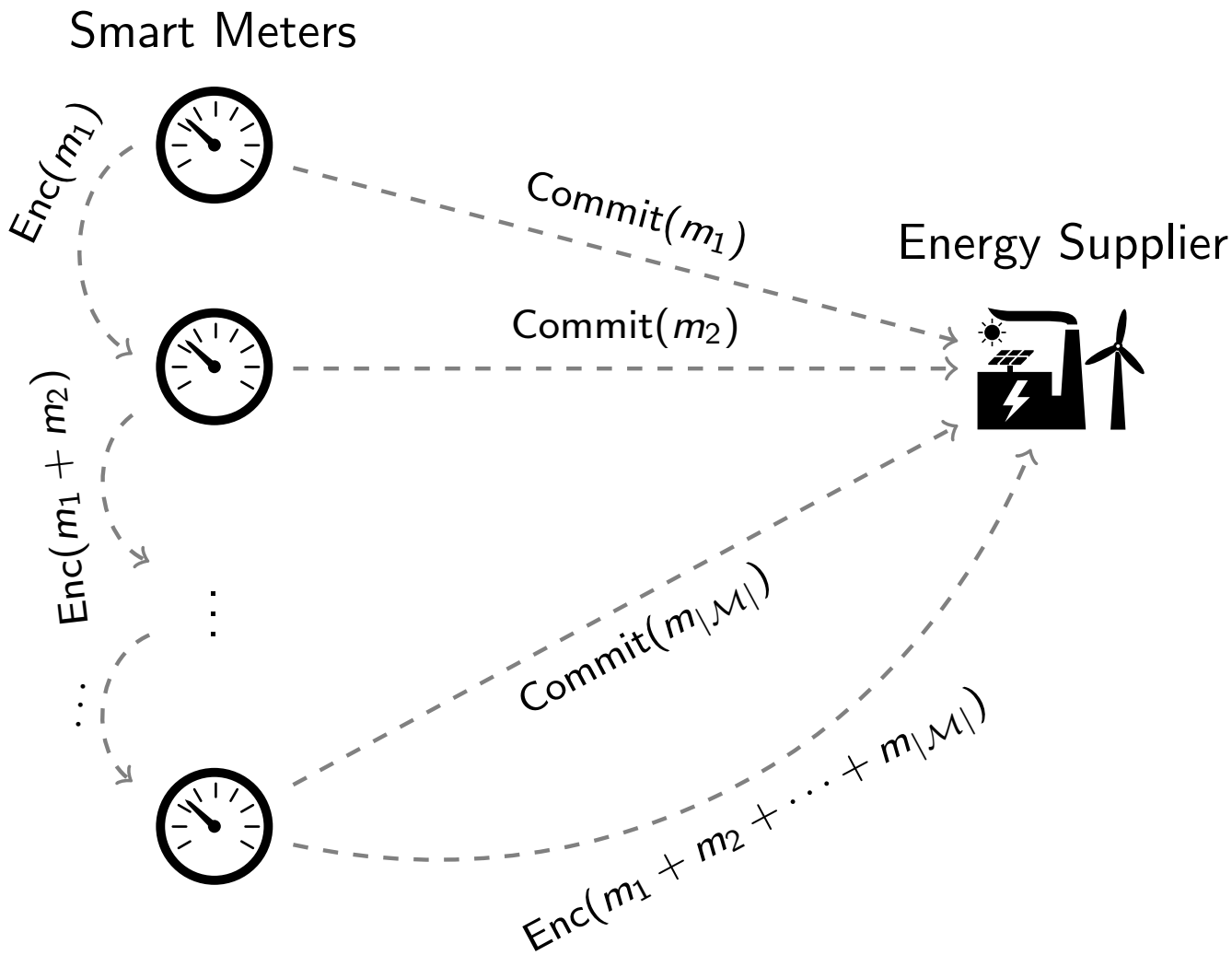
TECHNISCHE UNIVERSITÄT DARMSTADT

Smart Grid Scenario

with a phasor measurement unit (PMU)



Communication Model



Cryptographic Primitive

Commitment with a matching homomorphic encryption

TECHNISCHE UNIVERSITÄT DARMSTADT

Paillier Cryptosystem:

$$\mathrm{Enc}(m) = \mathrm{Enc}(m, s) = \gamma^m \cdot s^N \mod N^2$$

Pedersen Commitments:

$$\mathrm{Commit}(m, r) = g^m \cdot h^r \mod p$$

Matching: commitments take place in the order N subgroup of $\mathbb{Z}^*_{4N+1}$, where $4N + 1$ is a prime number.

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Further Work

TECHNISCHE UNIVERSITÄT DARMSTADT

Further Reading:

- IEEE CNS 2014
- iKUP Keeps Users' Privacy in the Smart Grid
- [Borges and Martucci, 2014]

Further Work:

- efficient cryptographic primitives
- communication complexity
- privacy in e-vehicle to grid

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

- Privacy-preserving protocols should have:
  - Consolidated Consumption
  - Billing
  - Verification
- Commitment with a matching homomorphic encryption

Thank You!

Any comments and suggestions are welcomed.
Contact: fabio.borges@cased.de

Bibliography I

TECHNISCHE UNIVERSITÄT DARMSTADT

(2012).

Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending directives 2009/125/EC and 2010/30/EU and repealing directives 2004/8/EC and 2006/32/EC.

Official Journal L No.315.

Borges, F., Demirel, D., Böck, L., Buchmann, J., and Mühlhäuser, M. (2014).

A Privacy-Enhancing protocol that provides In-Network data aggregation and verifiable smart meter billing.

In *19th IEEE Symposium on Computers and Communications (IEEE ISCC 2014)*, Madeira, Portugal.

Borges, F. and Martucci, L. A. (2014).

iKUP keeps users' privacy in the smart grid.

In *2014 IEEE Conference on Communications and Network Security (CNS) (IEEE CNS 2014)*, San Francisco, USA.

Bibliography II

TECHNISCHE UNIVERSITÄT DARMSTADT

Greveler, U., Justus, B., and Löhr, D. (2012).

Identifikation von videoinhalten über granulare stromverbrauchsdaten.

In Suri, N. and Waidner, M., editors, *Sicherheit*, volume 195 of *LNI*, pages 35–45. GI.