

ENCS

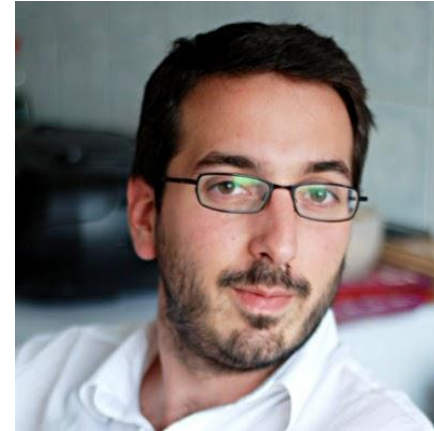
Lessons Learned from Implementing Privacy-Preserving Protocols for Smart Meters

Benessa Defend
Real World Crypto, London
January 9, 2015

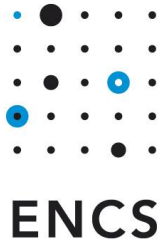
In Collaboration with



- Klaus Kursawe
- George Danezis
- Markulf Kohlweiss
- Elster
- Alliander



Publication to Testing to Standardization



Privacy-friendly Aggregation for the Smart-grid

Klaus Kursawe¹, George Danezis², and Markulf Kohlweiss²

¹Radboud Universiteit Nijmegen,
kursawe@cs.ru.nl

²Microsoft Research, Cambridge, U.K.
{gdane, markulf}@microsoft.com

Abstract. The widespread deployment of smart meters for the modernisation of the electricity distribution network, but also for gas and water consumption, has been associated with privacy concerns due to the potentially large number of measurements that reflect the consumers behaviour. In this paper, we present protocols that can be used to privately compute aggregate meter measurements over defined sets of meters, allowing for fraud and leakage detection as well as network management and further statistical processing of meter measurements, without revealing any additional information about the individual meter readings. Thus, most of the benefits of the Smart Grid can be achieved without revealing individual data. The feasibility of the protocols has been demonstrated with an implementation on current smart meters.



Conference paper at *Privacy Enhancing Technologies Symposium*

Feasibility test for meter implementation

Proof of concept for robustness, integration and configuration

Input for standardization

Implementation of Privacy-Friendly Aggregation for the Smart Grid

Benessa Defend
ENCS
Prinses Beatrixlaan 80D
The Hague, Netherlands
benessa.defend@encs.eu

Klaus Kursawe
ENCS
Prinses Beatrixlaan 80D
The Hague, Netherlands
klaus.kursawe@encs.eu

ABSTRACT

In recent years a number of protocols have been suggested towards privacy-preserving aggregation of smart meter data, allowing electricity network operators to perform a large part of grid maintenance and administrative operations without having to touch any privacy-sensitive data. In light of upcoming European legislation, this approach has gained quite some attention. However, to allow such protocols to have a chance to make it into a real system, it is vital to add credibility by demonstrating that the approach scales, is reasonably robust, and can be integrated into the existing and planned smart metering chains. This paper presents results from integration and scalability tests performed on 100 DLMSCOSEM smart meters in collaboration with a meter manufacturer a lessons learned, the protocols to challenges that

Using modern privacy preserving protocols, many of the privacy concerns can be mitigated, while providing the network operators with all of the data they need for grid operations, potentially with even higher data quality. The most prominent class of protocols in this respect are aggregation protocols, in which the sum of readings from multiple meters is computed without revealing the individual meter readings themselves. This is done by homomorphic encryption, i.e., encrypting the readings in a way that the encrypted ciphertexts can be added up, and the sum of ciphertexts – and only the sum – can then be decrypted to show the sum of the plaintexts. This approach, where applicable, is superior to collecting data and then restricting access to it (which creates a separate problem in itself and has failed some-



DLMSCOSEM smart meters in collaboration with a meter manufacturer a lessons learned, the protocols to challenges that

DLMSCOSEM Contributions 3:

DLMSCOSEM Interface Class

Project: DLMSCOSEM standards maintenance

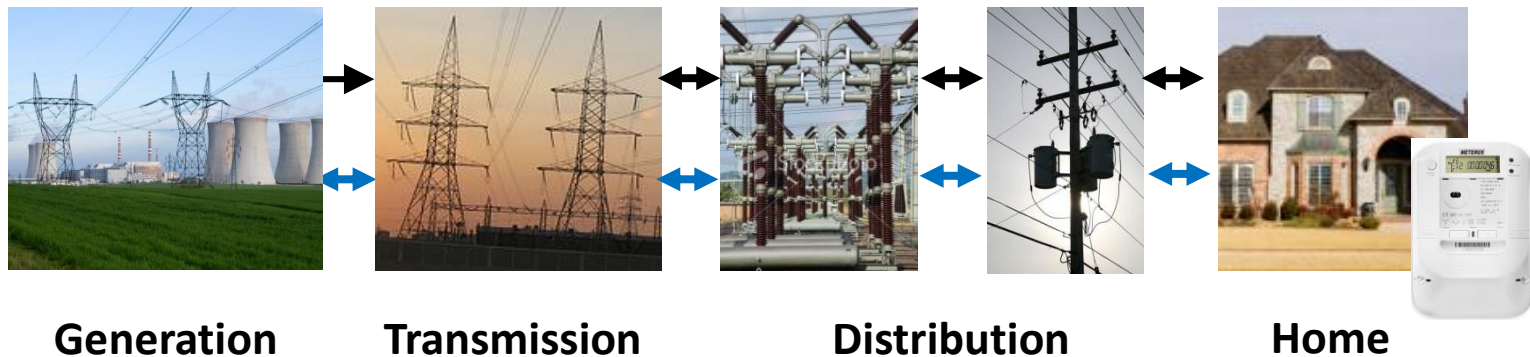
Category: Enter the subject using one of the following categories. Check one or several of them.

- General
- Direct connection (IEC 62056-21 Mode B)
- Physical layer (Green Book, IEC 62056-42)
- HDLC data link layer (Green Book, IEC 62056-46)
- COSEM Transport layer (Green Book, IEC 62056-47)
- COSEM Application layer (Blue Book, IEC 62056-43)
- COSEM Interface classes (Blue Book, IEC 62056-52)
- OBIS codes (Blue Book, IEC 62056-61)
- Conformance testing (Yellow book)
- DLMSCOSEM client

Smart Grid 101

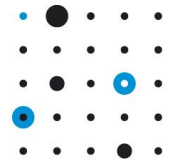


Energy **and information** flows in many directions, from generation to grid or building, from utility to customers, etc.

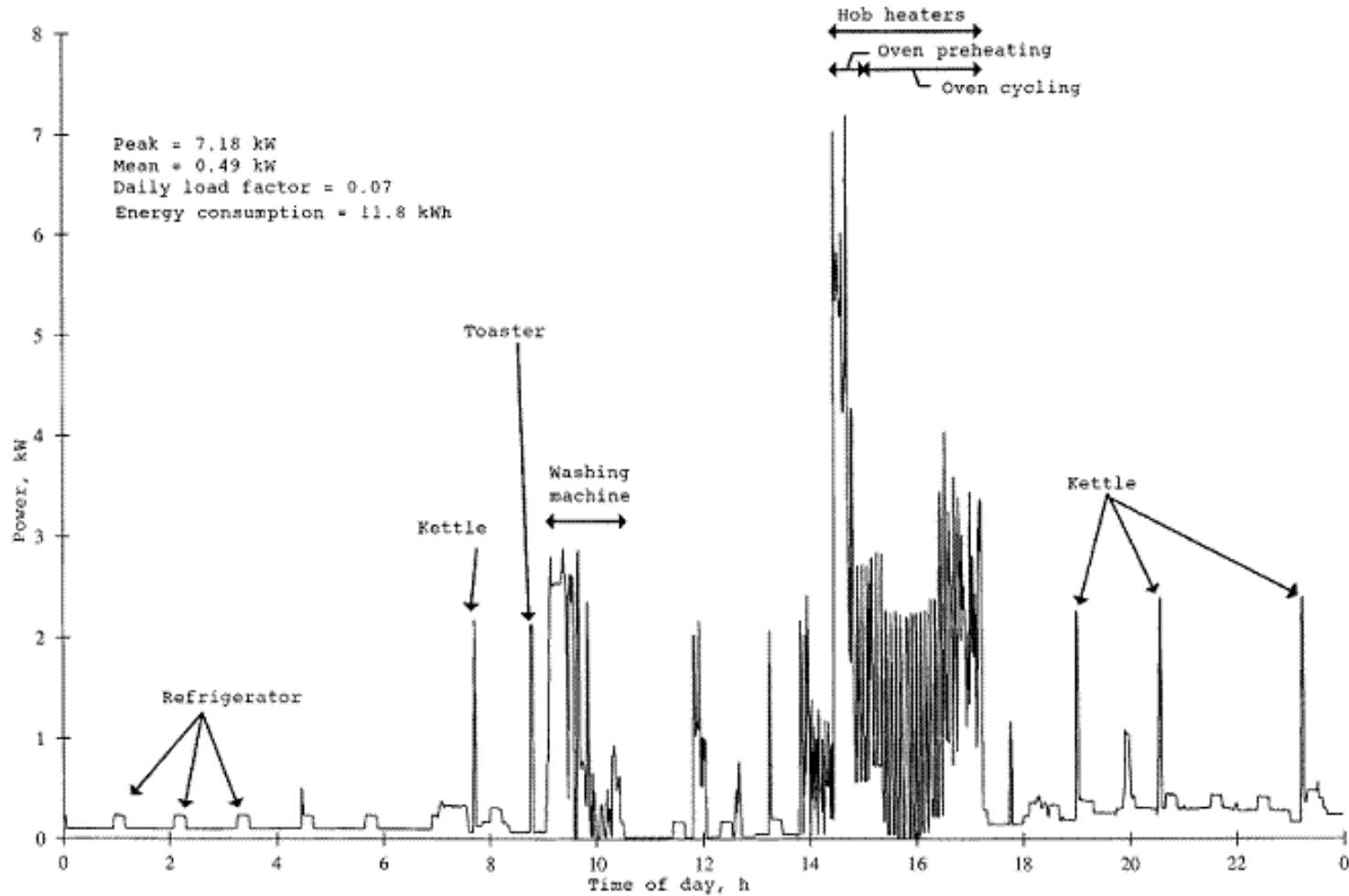


Smart meter data is useful for managing the grid, handling power outages, etc.

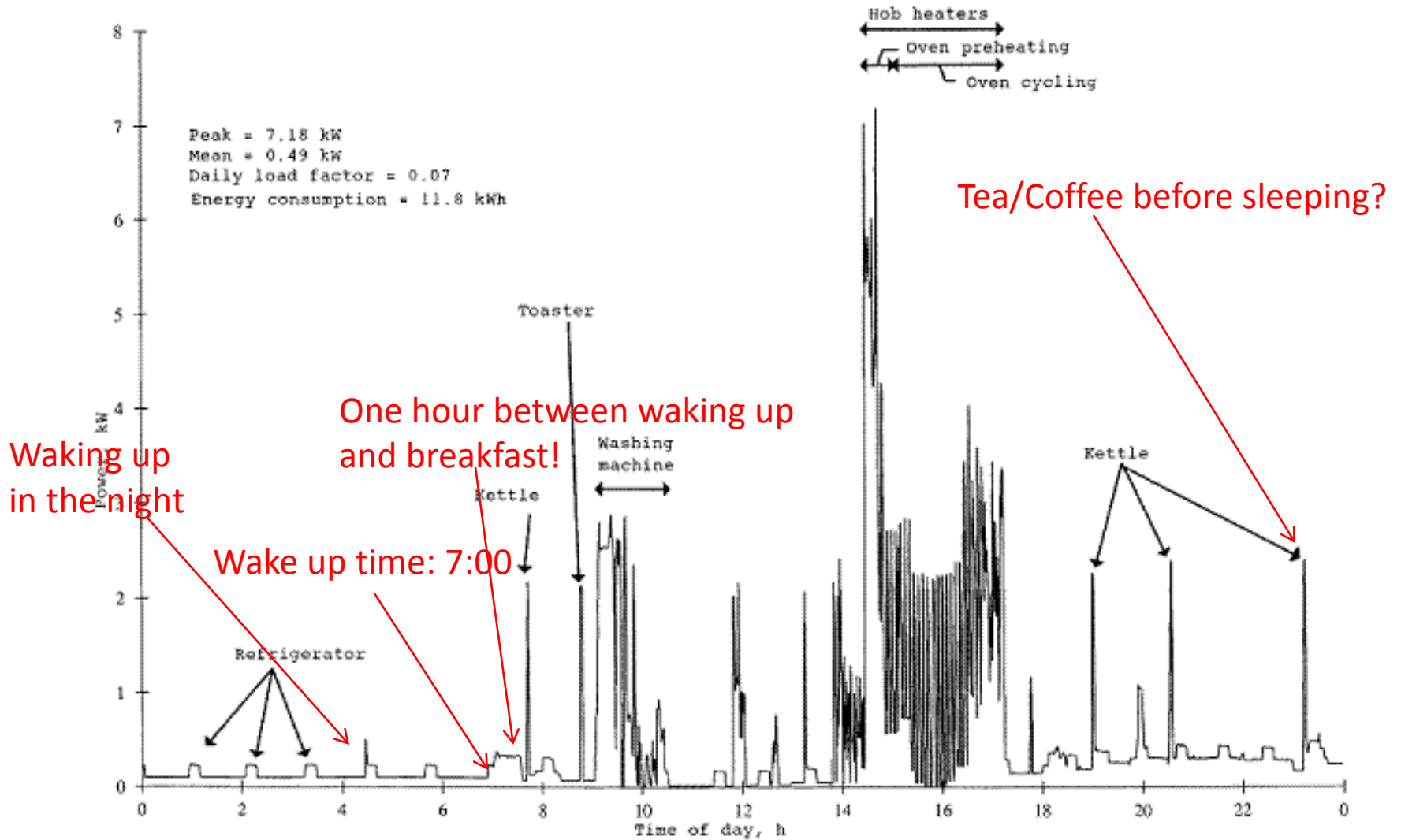
However, smart meter data...



ENCS



... is revealing.



Legal Ramifications: EU Member States

- General Data Protection Regulation: up to 2% of worldwide revenue fine for data protection violations
- In negotiation: may increase to 5% or 100 million euros



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

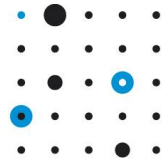
(Text with EEA relevance)

{SEC(2012) 72 final}

{SEC(2012) 73 final}

European Commission, General Data Protection Regulation, COM(2012) 11 final

Legal Ramifications: NL



ENCS

- Dutch Senate blocked 2 smart meter bills in 2009 due to violations of the Dutch Data Protection Act
- Grid operators had to halt smart meter rollout and lost millions in investments

Smart metering and privacy in Europe: lessons from the Dutch case

Colette Cuijpers and Bert-Jaap Koops

Tilburg Institute for Law, Technology, and Society (TILTS), Tilburg University, The Netherlands

{cuijpers, e.j.koops}@tilburguniversity.edu

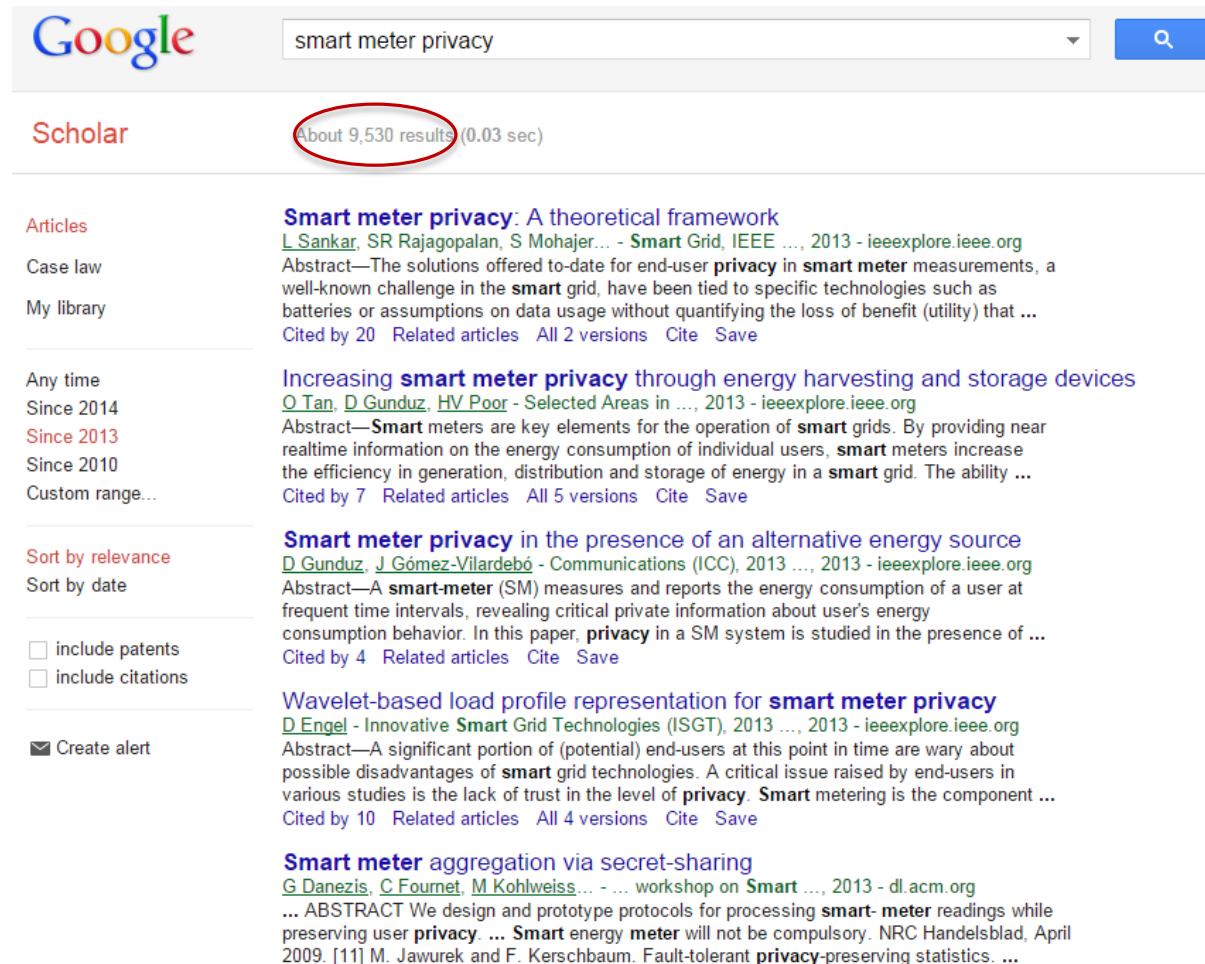
Abstract. The future of energy supply lies in smart grids, which enable energy supply to and from consumers. These two-way energy networks require smart energy metering systems. The vision of smart grids will require one or more decades yet to be fully realised, but since a roll-out of smart meters is a lengthy process, countries are already starting to implement smart metering legislation, following the European legal framework on energy efficiency. Rolling out smart meters, however, requires smart legislation. The Dutch example, where the Senate blocked two smart metering bills in 2009, demonstrates that introducing smart meters can be significantly delayed if the underlying legislation is flawed. In particular, the Dutch case shows that privacy is a crucial element in smart metering legislation. Energy consumption reveals details of personal life, in the most privacy-sensitive place – the home, and therefore smart metering has to strike a careful balance between detailed energy metering and privacy protection.

In this paper, we present the recent developments in smart metering and describe the Dutch case in detail. From this, we draw key lessons for countries that want to introduce smart metering. In terms of substance, the level of detail of smart meter readings and the mandatory or voluntary character of smart meters are crucial issues to take into account. Legislators must make a trade-off between the 'smartness' of the meter versus a comprehensive, mandatory roll-out. In terms of procedure, a privacy impact assessment is vital, and pitfalls of function creep should be avoided by resisting the temptation of making a meter 'too smart' all at once. From the outset, privacy and data protection law must be taken into account as an important requirement for the design of smart metering systems.

Keywords: Smart metering, energy, privacy, data protection, Europe, the Netherlands

Privacy Approaches

- Aggregation
- Homomorphic Encryption
- Differential Privacy
- Rechargeable Batteries
- Anonymization
- Pseudonymization
- Trusted Platform Module



Google search for "smart meter privacy" on Scholar. The search bar shows "smart meter privacy" and the results count is "About 9,530 results (0.03 sec)".

Articles

Case law
My library

Any time
Since 2014
Since 2013
Since 2010
Custom range...

Sort by relevance
Sort by date

include patents
 include citations

Create alert

Smart meter privacy: A theoretical framework
[L Sankar](#), SR Rajagopalan, S Mohajer... - *Smart Grid, IEEE* ..., 2013 - [ieeexplore.ieee.org](#)
Abstract—The solutions offered to-date for end-user **privacy** in **smart meter** measurements, a well-known challenge in the **smart grid**, have been tied to specific technologies such as batteries or assumptions on data usage without quantifying the loss of benefit (utility) that ...
Cited by 20 [Related articles](#) [All 2 versions](#) [Cite](#) [Save](#)

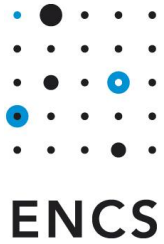
Increasing smart meter privacy through energy harvesting and storage devices
[O Tan](#), [D Gunduz](#), [HV Poor](#) - *Selected Areas in* ..., 2013 - [ieeexplore.ieee.org](#)
Abstract—**Smart meters** are key elements for the operation of **smart grids**. By providing near realtime information on the energy consumption of individual users, **smart meters** increase the efficiency in generation, distribution and storage of energy in a **smart grid**. The ability ...
Cited by 7 [Related articles](#) [All 5 versions](#) [Cite](#) [Save](#)

Smart meter privacy in the presence of an alternative energy source
[D Gunduz](#), [J Gómez-Vilardebó](#) - *Communications (ICC), 2013* ..., 2013 - [ieeexplore.ieee.org](#)
Abstract—A **smart-meter** (SM) measures and reports the energy consumption of a user at frequent time intervals, revealing critical private information about user's energy consumption behavior. In this paper, **privacy** in a SM system is studied in the presence of ...
Cited by 4 [Related articles](#) [Cite](#) [Save](#)

Wavelet-based load profile representation for smart meter privacy
[D Engel](#) - *Innovative Smart Grid Technologies (ISGT), 2013* ..., 2013 - [ieeexplore.ieee.org](#)
Abstract—A significant portion of (potential) end-users at this point in time are wary about possible disadvantages of **smart grid** technologies. A critical issue raised by end-users in various studies is the lack of trust in the level of **privacy**. **Smart metering** is the component ...
Cited by 10 [Related articles](#) [All 4 versions](#) [Cite](#) [Save](#)

Smart meter aggregation via secret-sharing
[G Danezis](#), [C Fournet](#), [M Kohlweiss](#)... - ... *workshop on Smart* ..., 2013 - [dl.acm.org](#)
... ABSTRACT We design and prototype protocols for processing **smart-meter** readings while preserving user **privacy**. ... **Smart energy meter** will not be compulsory. NRC Handelsblad, April 2009. [11] M. Jawurek and F. Kerschbaum. Fault-tolerant **privacy**-preserving statistics. ...

Picking a Protocol to Implement & More



Privacy-friendly Aggregation for the Smart-grid

Klaus Kursawe¹, George Danezis², and Markulf Kohlweiss²

¹Radboud Universiteit Nijmegen,
kursawe@cs.ru.nl

²Microsoft Research, Cambridge, U.K.
{gdane, markulf}@microsoft.com

Abstract. The widespread deployment of smart meters for the modernisation of the electricity distribution network, but also for gas and water consumption, has been associated with privacy concerns. A potentially large number of measurements that reflect the user's behaviour. In this paper, we present protocols that can be used to compute aggregate meter measurements over defined sections of the network allowing for fraud and leakage detection as well as network management and further statistical processing of meter measurements, without revealing any additional information about the individual meter readings. Thus, most of the benefits of the Smart Grid can be achieved without revealing individual data. The feasibility of the protocols has been demonstrated with an implementation on current smart meters.



Conference paper at *Privacy Enhancing Technologies Symposium*

Feasibility test for meter implementation

Proof of concept for robustness, integration and configuration

Input for standardization

Implementation of Privacy-Friendly Aggregation for the Smart Grid

Benessa Defend
ENCS
Prinses Beatrixlaan 80D
The Hague, Netherlands
benessa.defend@encs.eu

Klaus Kursawe
ENCS
Prinses Beatrixlaan 80D
The Hague, Netherlands
klaus.kursawe@encs.eu

ABSTRACT

In recent years a number of protocols have been suggested towards privacy-preserving aggregation of smart meter data, allowing electricity network operators to perform a large part of grid maintenance and administrative operations without having to touch any privacy-sensitive data. In light of upcoming European legislation, this approach has gained quite some attention. However, to allow such protocols to have a chance to make it into a real system, it is vital to add credibility by demonstrating that the approach scales, is reasonably robust, and can be integrated into the existing and planned smart metering chains. This paper presents results from integration and scalability tests performed on 100 DLMSCOSEM smart meters in collaboration with a meter manufacturer a lessons learned, the protocols to challenges that

Using modern privacy preserving protocols, many of the privacy concerns can be mitigated, while providing the network operators with all of the data they need for grid operations, potentially with even higher data quality. The most prominent class of protocols in this respect are aggregation protocols, in which the sum of readings from multiple meters is computed without revealing the individual meter readings themselves. This is done by homomorphic encryption, i.e., encrypting the readings in a way that the encrypted ciphertexts can be added up, and the sum of ciphertexts – and only the sum – can then be decrypted to show the sum of the plaintexts. This approach, where applicable, is superior to collecting data and then restricting access to it (which creates a separate problem in itself) and has faced some

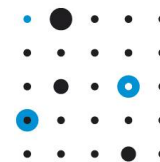


DLMS_OXX_PETS_V02_MJ09130605.doc

DLMSCOSEM Contributions 3:

DLMSCOSEM Interface Class

- Project:** DLMSCOSEM standards maintenance
- Category:** Enter the subject using one of the following categories. Check one or several of them.
- General
 - Direct connection (IEC 62056-21 Mode E)
 - Physical layer (Green Book, IEC 62056-42)
 - HDLC data link layer (Green Book, IEC 62056-46)
 - COSEM Transport layer (Green Book, IEC 62056-47)
 - COSEM Application layer (Blue Book, IEC 62056-53)
 - COSEM Interface classes (Blue Book, IEC 62056-52)
 - OBIS codes (Blue Book, IEC 62056-61)
 - Conformance testing (Yellow book)
 - DLMSCOSEM client

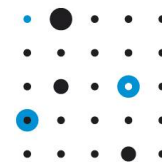


Implementation

- Implementation in Perl*
 1. Diffie-Hellman-based aggregation protocol
 2. Dining Cryptographers-based low-overhead aggregation protocol
 3. Billing protocol
- Implementation on 4 meters (and later 100)
 - Low-overhead aggregation protocol only



*by George Danezis



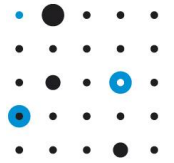
ENCS

Understanding Requirements

1. Meter Restrictions - cost, computing power, memory
2. Bandwidth - limited bandwidth, geography
3. Security Architecture - network topologies
4. Protocol Integration - integration into existing standards
5. Use cases – understand what data is needed

Result: implemented low-overhead aggregation instead of more feature-rich & robust protocols





ENCS

Lessons Learned

1. Define the use cases
2. Selling privacy
3. Provide clear explanations
4. Ease of integration vs. Feature richness
5. Importance of standardization
6. Working prototypes
7. Patience

Define the Use Cases

- Interview potential users
 - What kind of data do you need?
 - If I was the privacy fairy and could eliminate all privacy restrictions, what kind of information would you want?
- Usually only a derivative of private data is needed



Selling Privacy

- Frame as business enabler
- With privacy:
 - Legal access to data you couldn't get otherwise
 - Easier DPIA
 - No private data to protect
 - No bad press from accidental loss or theft of private data

Sony Hack Lawsuit: Former Employees Sue Film Studio For Not Protecting Private Data

By Lora Mofrah @LoraMofrah | l.mofrah@btimes.com on December 16 2014 2:48 PM



Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users

BY ANDY GREENBERG | 11.18.14 | 10:54 AM | PERMALINK



Sony hack reveals health information on employees, children, spouses

BLOOMBERG

NEW YORK – Documents stolen from Sony Corp. by hackers include detailed and identifiable health information on more than three dozen employees, their children or spouses — a sign of how much information employers have on their workers and how easily it can become public.

One memo by a human resources executive, addressed to the company's CEO, discussed details on an employee's child with special needs and the type of treatment the child was receiving. Another memo discussed the employee's appeal of thousands of dollars in costs by the insurance company.

The memo in the hack is a spreadsheet from a human resources department that includes the birth dates, gender, health condition and names of employees, their spouses and children who had

DEC 13, 2014
ARTICLE HISTORY
PRINT SHARE

KEYWORDS
CYBERATTACKS, HACKERS,
INFORMATION LEAK, PRIVACY,
SONY, SONY PICTURES

BUSINESS
• JR Tokai begins building maglev train stations

Apple expands data encryption under iOS 8, making handover to cops moot

"Apple cannot bypass your passcode and therefore cannot access this data."

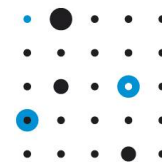
by Cyrus Farivar - Sept 18 2014, 6:57am WEDT



Growing up in Soviet Ukraine in the 1980s, he distrusted the government and detested its surveillance and created his ultra-popular messaging system. WhatsApp would never make eavesdropping easy by following through on that anti-snooping promise.



Tim Cook unveils iOS 8 at WWDC 2014.



Importance of Clear Explanations

- Good metaphors
- Intuitive examples
- Explaining one-way functions using Lego:

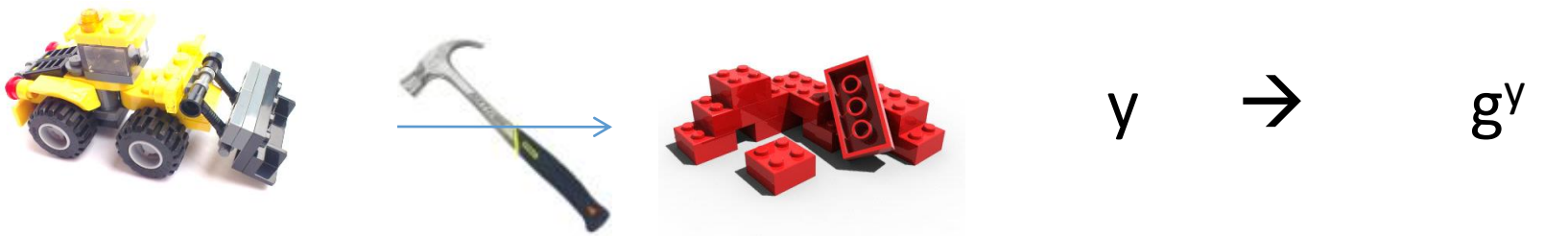


LEGO Example: Homomorphic One-Way Functions



+

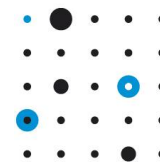
+



=

=





Ease of Integration vs. Feature Richness

- Optimize protocol and parameters for easy integration
 - Deep changes require more effort and money
- Fewer changes means it is more likely to be adopted
 - Add-on to standard
 - No changes to central system
 - Only small changes to meter firmware
- Simple protocol might be better than a fancy protocol
 - Very low overhead vs. more features



Importance of Standardization

- Ensure widespread adoption - individual companies don't have to seek out their own solution
- Create an add-on vs. major change



Working Prototypes

- Need to prove it works
- Small implementation for feasibility
- Large scalability, integration, robustness tests



4 Meters



100 Meters

Patience: 2011 - Now

Privacy-friendly Aggregation for the Smart-grid

Klaus Kursawe¹, Georg Danzels², and Markulf Kobbweis³

¹Bosch University Nijmegen, Eindhoven, Nl, nl

³Microsoft Research, Cambridge, U.K. {klaus, markulf}@microsoft.com

Abstract. The widespread deployment of smart meters for the measurement of the electricity distribution network, but also for gas and water consumption, has been associated with privacy concerns due to the potentially large number of measurements that reflect the consumers' behavior. In this paper, we present protocols that can be used to privately compute aggregate meter measurements over defined sets of meters, allowing for fraud and leakage detection as well as network management and further analytical processing of meter measurements, without revealing any additional information about the individual meter readings. Thus, most of the benefits of the Smart Grid can be achieved without revealing individual data. The feasibility of the protocols has been demonstrated with an implementation on current smart meters.



PETS
Publication

Implementation:
4 Meters

Scalability & Integration
Tests: 100 Meters

2011



2012



2013



Working Groups
Talking to Industry

TASK FORCE SMART GRIDS

EXPERT GROUP 2: REGULATORY
RECOMMENDATIONS FOR DATA SAFETY,
DATA HANDLING AND DATA PROTECTION

REPORT

ISSUED: FEBRUARY 16, 2011

Interviews



Input for
Standardization



DLMS_DOL_PETS_V02_MUCO-0008.doc

DLMS/COSEM Contributions 2:

DLMS PETS Interface Class

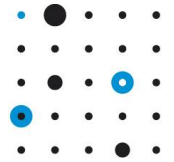
1

Project: DLMS/COSEM standards maintenance

Category: Enter the subject using one of the following categories. Check one or several of them.

- Data
- Data connection (IEC 62052-2: Home B)
- Physical layer (Open Book IEC 62054-2)
- A-CLC data link layer (Open Book IEC 62054-4)
- COSEM Transport layer (Open Book IEC 62054-7)
- COSEM Application layer (Open Book IEC 62054-8)
- COSEM Interface classes (Open Book IEC 62054-9)
- DLMS codes (Open Book IEC 62054-9)
- Conformance testing (Yellow book)
- DLMS/COSEM client

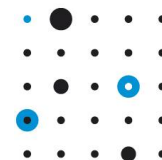
Conclusions



ENCS

- Use good examples
- Privacy as business enabler
- Ease of integration can trump fancy features
 - But don't exclude use cases!
- Make sure all required properties are included – hard to make changes later
- Standardization can lead to widespread adoption





ENCS

Questions

Benessa.Defend@encs.eu