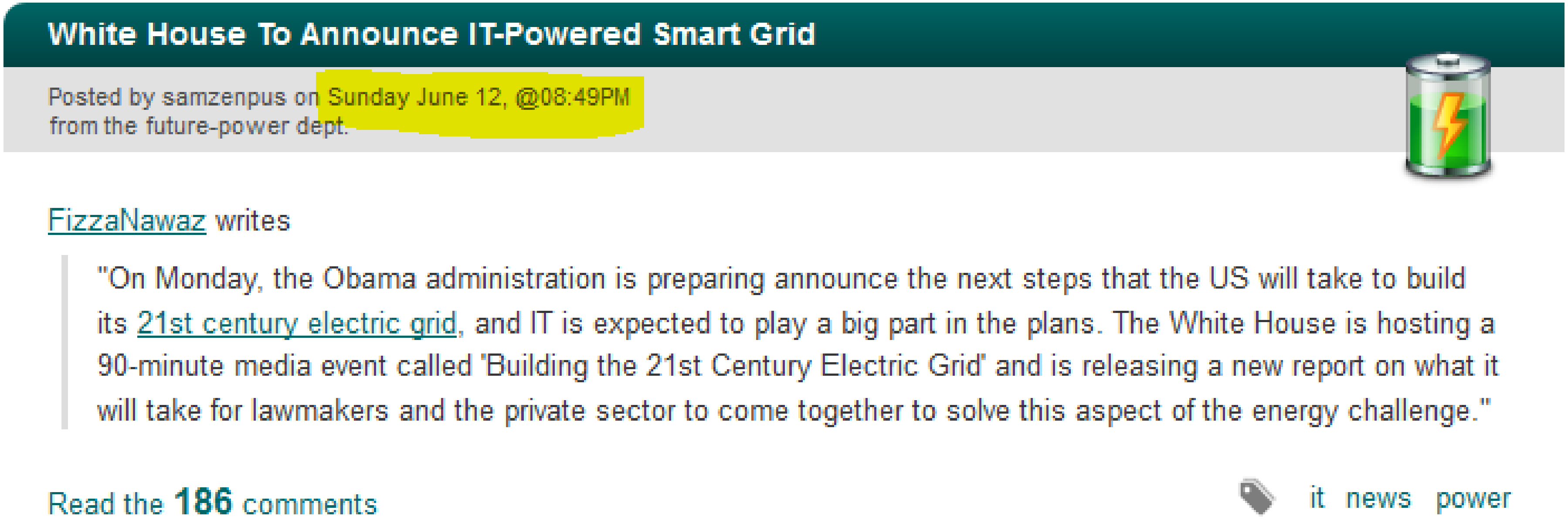
Privacy-Preserving Smart Metering

George Danezis (MSR)
Alfredo Rial (KU Leuven)
Markulf Kohlweiss (MSR),
Klaus Kursawe (Nijmegen),
Cedric Fournet (MSR),
Andy Gordon (MSR),
Misha Aizatulin (OU),
Francois Dupressoir (OU)
and MS XCG



White House To Announce IT-Powered Smart Grid

Posted by samzenpus on Sunday June 12, @08:49PM
from the future-power dept.

FizzaNawaz writes

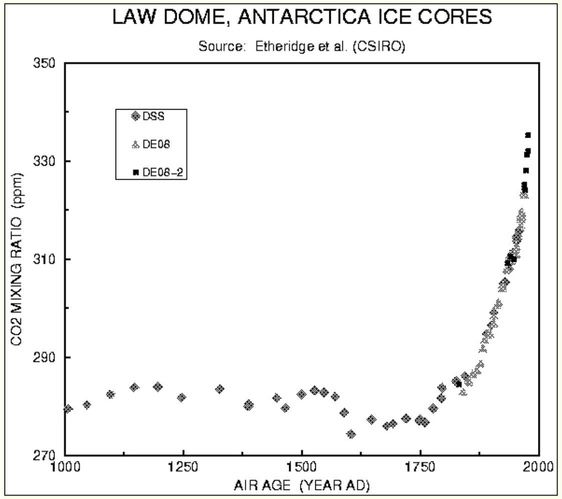
> "On Monday, the Obama administration is preparing announce the next steps that the US will take to build its 21st century electric grid, and IT is expected to play a big part in the plans. The White House is hosting a 90-minute media event called 'Building the 21st Century Electric Grid' and is releasing a new report on what it will take for lawmakers and the private sector to come together to solve this aspect of the energy challenge."

Read the 186 comments

it news power

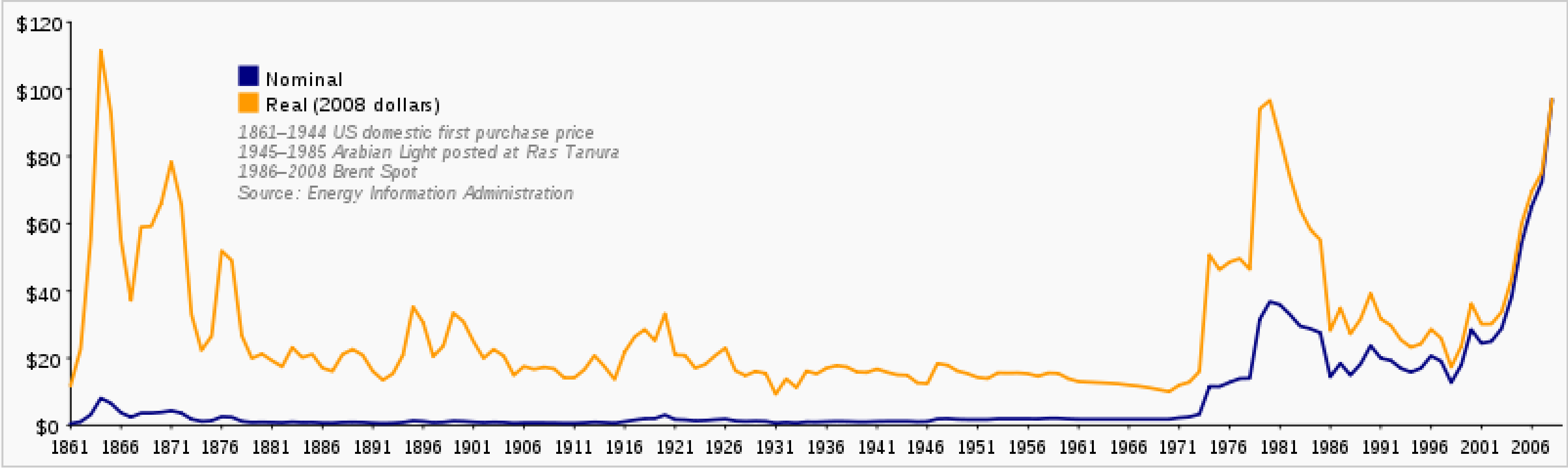
The new energy landscape (I)

- Energy pressures:
  - Energy cost, carbon & climate change
  - Reduce peak consumption (+ efficient transport)



LAW DOME, ANTARCTICA ICE CORES

Source: Etheridge et al. (CSIRO)

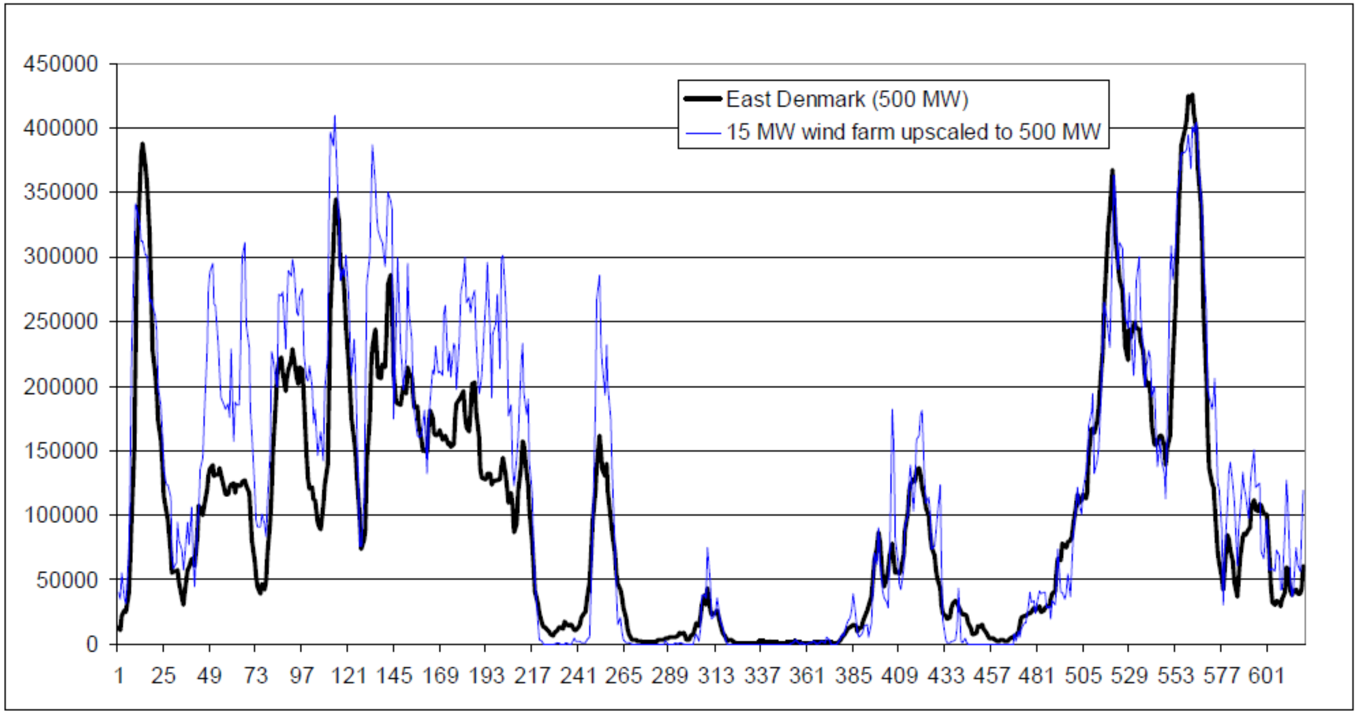


1861–1944 US domestic first purchase price
1945–1985 Arabian Light posted at Ras Tanura
1986–2008 Brent Spot
Source: Energy Information Administration

The new energy landscape (II)

Renewables:

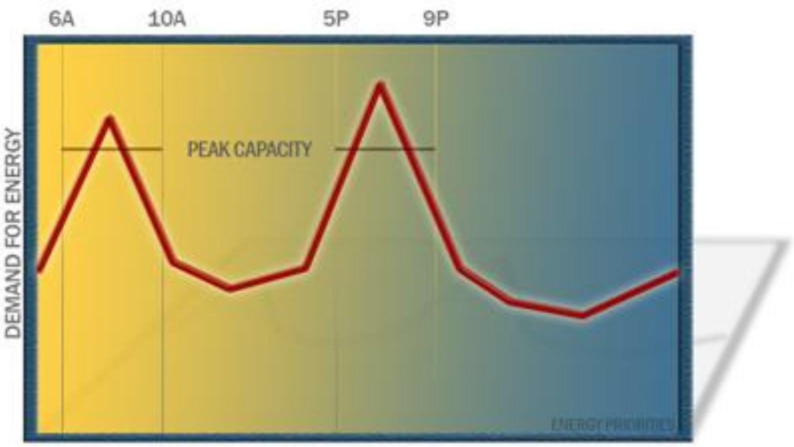
- Unpredictable yield over time
- Electric cars = heavy load to shift

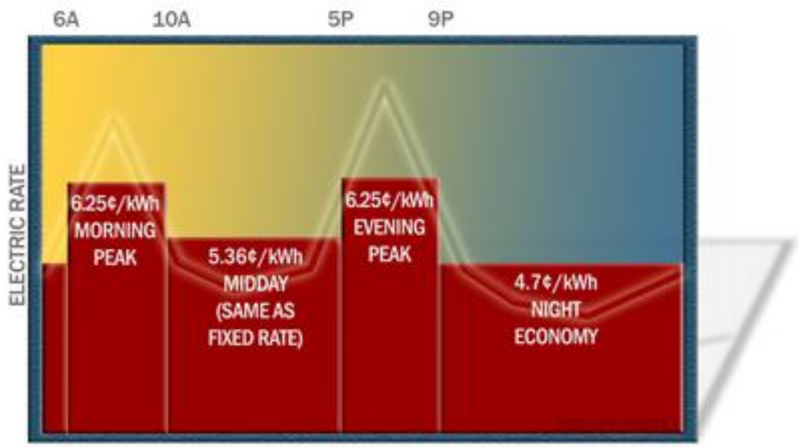


The new energy landscape (III)

Smart metering: increase efficiency

- Better feedback to users through **fine grained 15-30 min readings**
- Time of use billing (you pay for when you consume)
- Remote readings, monitoring, change of tariff, disconnection (competition)
- Integrate renewable micro-generation





http://energypriorities.com/entries/2006/02/pse_tou_amr_case.php

Key changes for electricity

Current metering

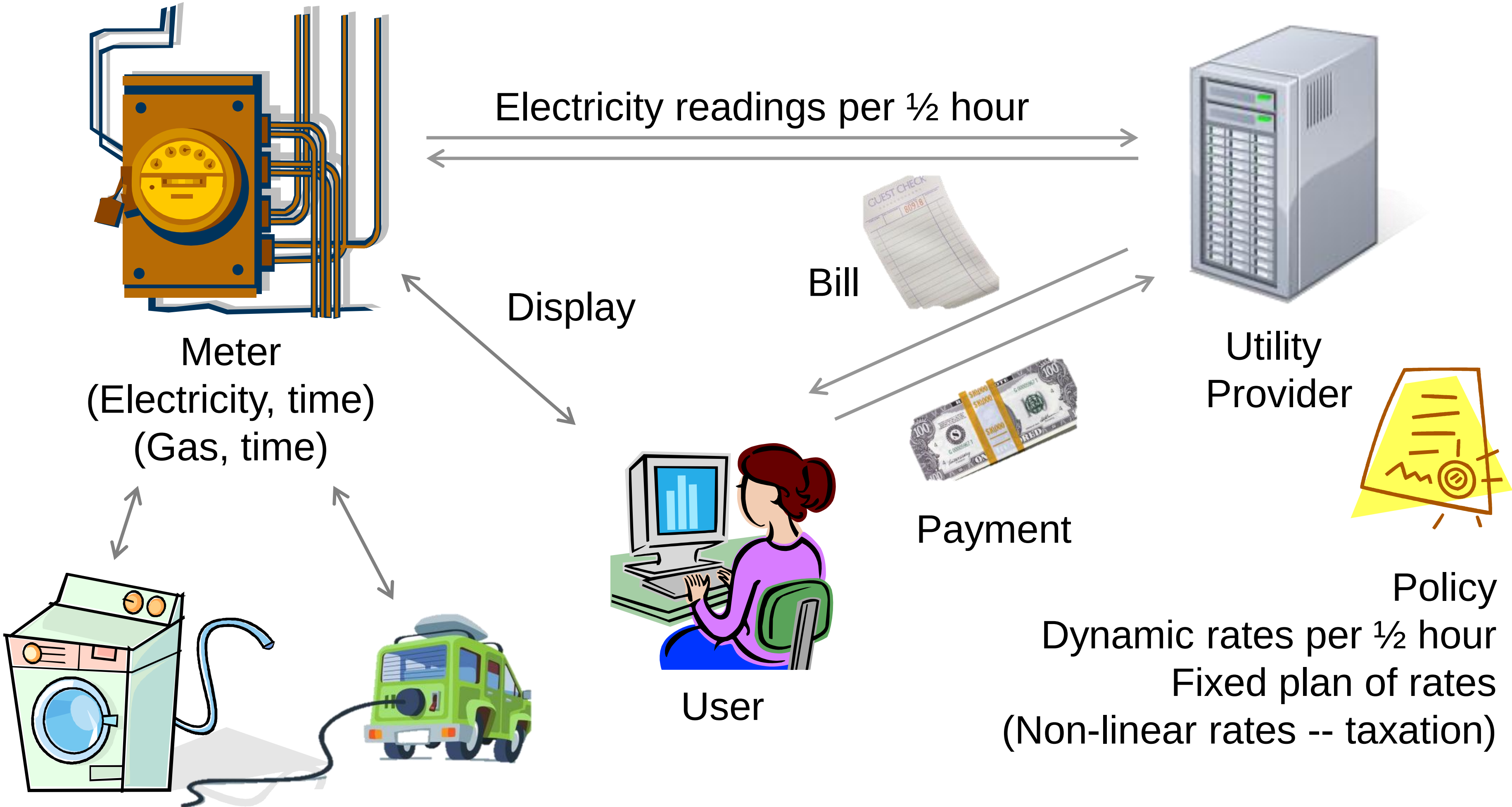
- Manual reads
- One read every ¼ year to 1 month

Smart metering

- Remote reads
- Reads every 15-30 minutes

(+ easy to switch supplier, different tariffs, pre-paid, in-house display, remote disconnection)

What is smart metering?



Electricity readings per ½ hour

Display

Bill

Meter
(Electricity, time)
(Gas, time)

Utility
Provider

Payment

User

Policy
Dynamic rates per ½ hour
Fixed plan of rates
(Non-linear rates -- taxation)

Smart-grid for electricity

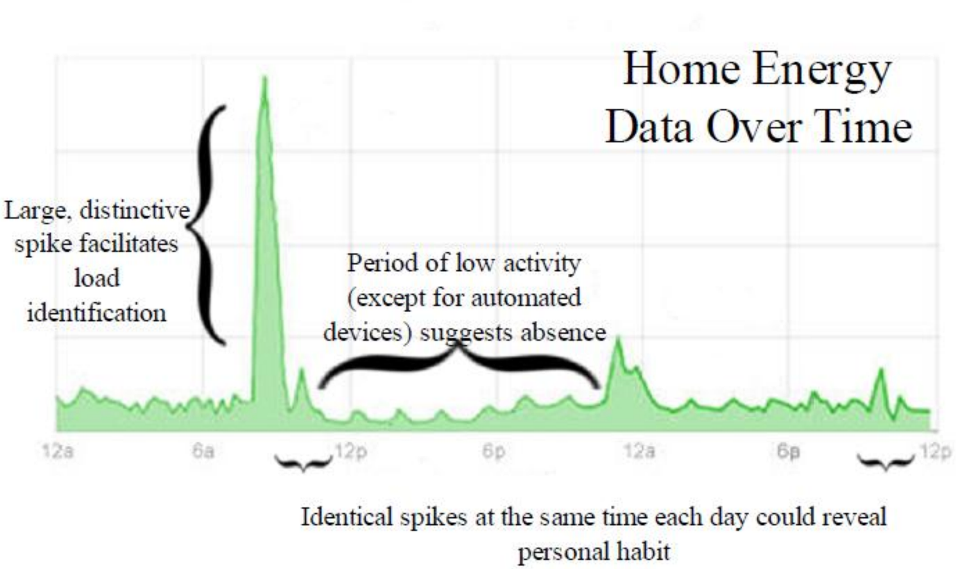
- USA: Energy Independence and Security Act of 2007
  - American Recovery and Reinvestment Act (2009, $4.5bn)
- EU: Directive 2009/72/EC
- UK: deployment of 47 million smart meters by 2020

BUT:

“The Dutch First Chamber considers the mandatory nature of smart metering as an unacceptable infringement of citizens’ privacy and security”

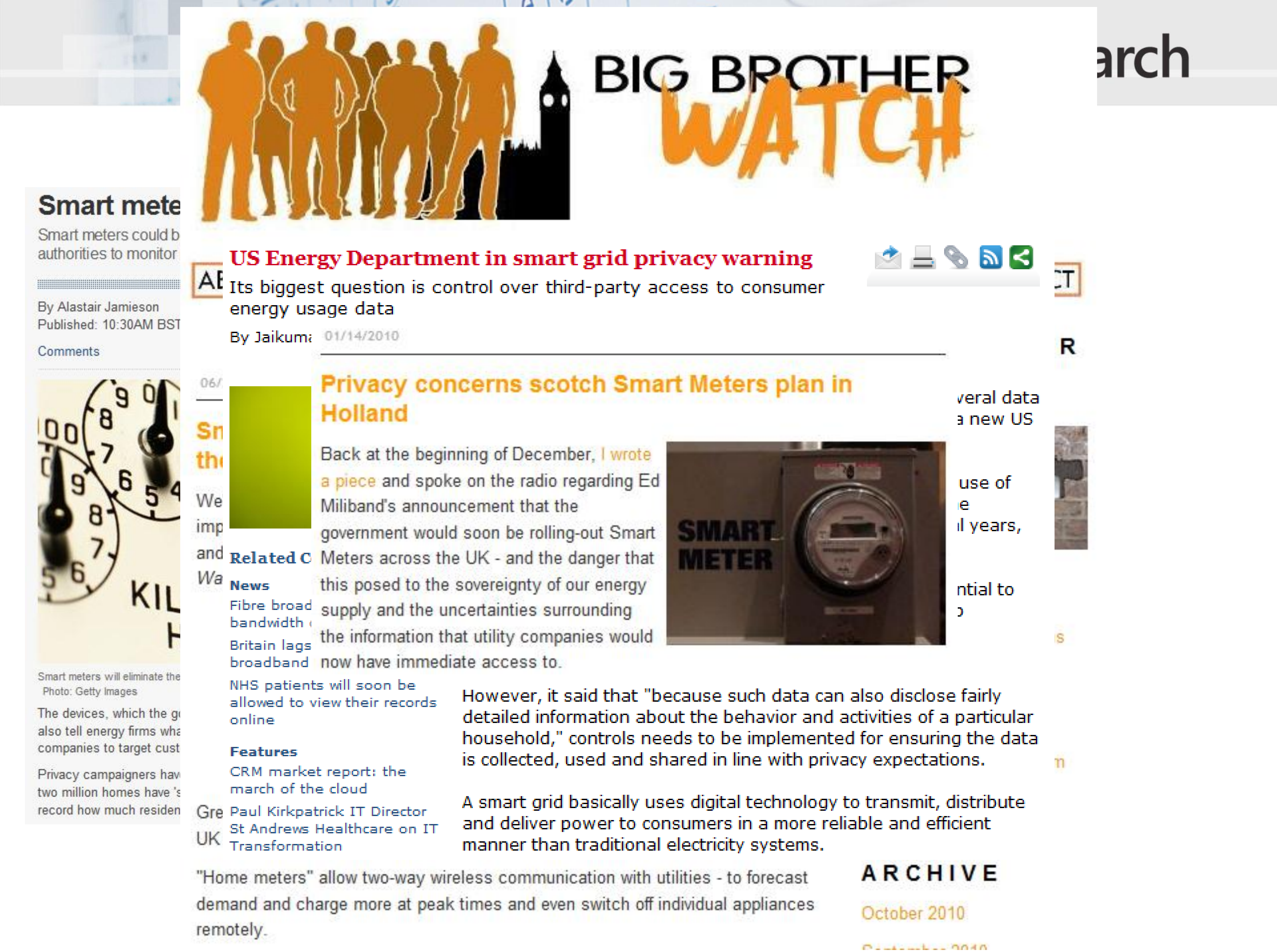
Privacy issues

- Meter readings are sensitive:
  - Were you in last night? You do like watching TV don't you? Another ready meal in the microwave? Has your boyfriend moved in?



- More issues …
  - Proposed centralised routing / database (?) of readings (UK)
  - Mandatory to receive service
  - Ability to switch off / switch to prepaid meters

Toward Technological Defenses Against Load Monitoring Techniques
Thomas Nicol, Student Member, IEEE,
Thomas J. Overbye, Fellow, IEEE



arch

Smart mete

Smart meters could b
authorities to monitor

By Alastair Jamieson
Published: 10:30AM BST

Comments

Smart meters will eliminate the
Photo: Getty Images

The devices, which the g
also tell energy firms wha
companies to target cust

Privacy campaigners hav
two million homes have 's
record how much residen

BIG BROTHER WATCH

US Energy Department in smart grid privacy warning

Its biggest question is control over third-party access to consumer energy usage data

By Jaikuma

01/14/2010

Privacy concerns scotch Smart Meters plan in Holland

Back at the beginning of December, I wrote a piece and spoke on the radio regarding Ed Miliband's announcement that the government would soon be rolling-out Smart Meters across the UK - and the danger that this posed to the sovereignty of our energy supply and the uncertainties surrounding the information that utility companies would now have immediate access to.

AE

06/

Sn
th

We
imp
and
Wa

Related C

News

Fibre broad
bandwidth

Britain lags
broadband

NHS patients will soon be allowed to view their records online

Features

CRM market report: the march of the cloud

Paul Kirkpatrick IT Director St Andrews Healthcare on IT Transformation

Gre
UK

CT

R

veral data
a new US

use of
e
l years,

ntial to
ɔ

s

n

However, it said that "because such data can also disclose fairly detailed information about the behavior and activities of a particular household," controls needs to be implemented for ensuring the data is collected, used and shared in line with privacy expectations.

A smart grid basically uses digital technology to transmit, distribute and deliver power to consumers in a more reliable and efficient manner than traditional electricity systems.

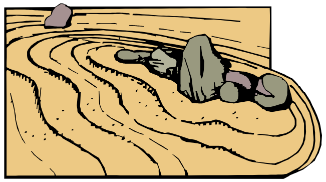
"Home meters" allow two-way wireless communication with utilities - to forecast demand and charge more at peak times and even switch off individual appliances remotely.

ARCHIVE

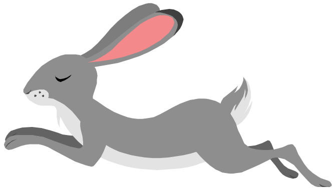
October 2010

Privacy preserving metering: design principles

- Obviously: **integrity & privacy (unconditional)**



- Keep meters very simple = cheap
  - No mobile code
  - No knowledge of tariff policy or structure
  - No need for smartness
  - Low-communication overhead
  - Ease of certification

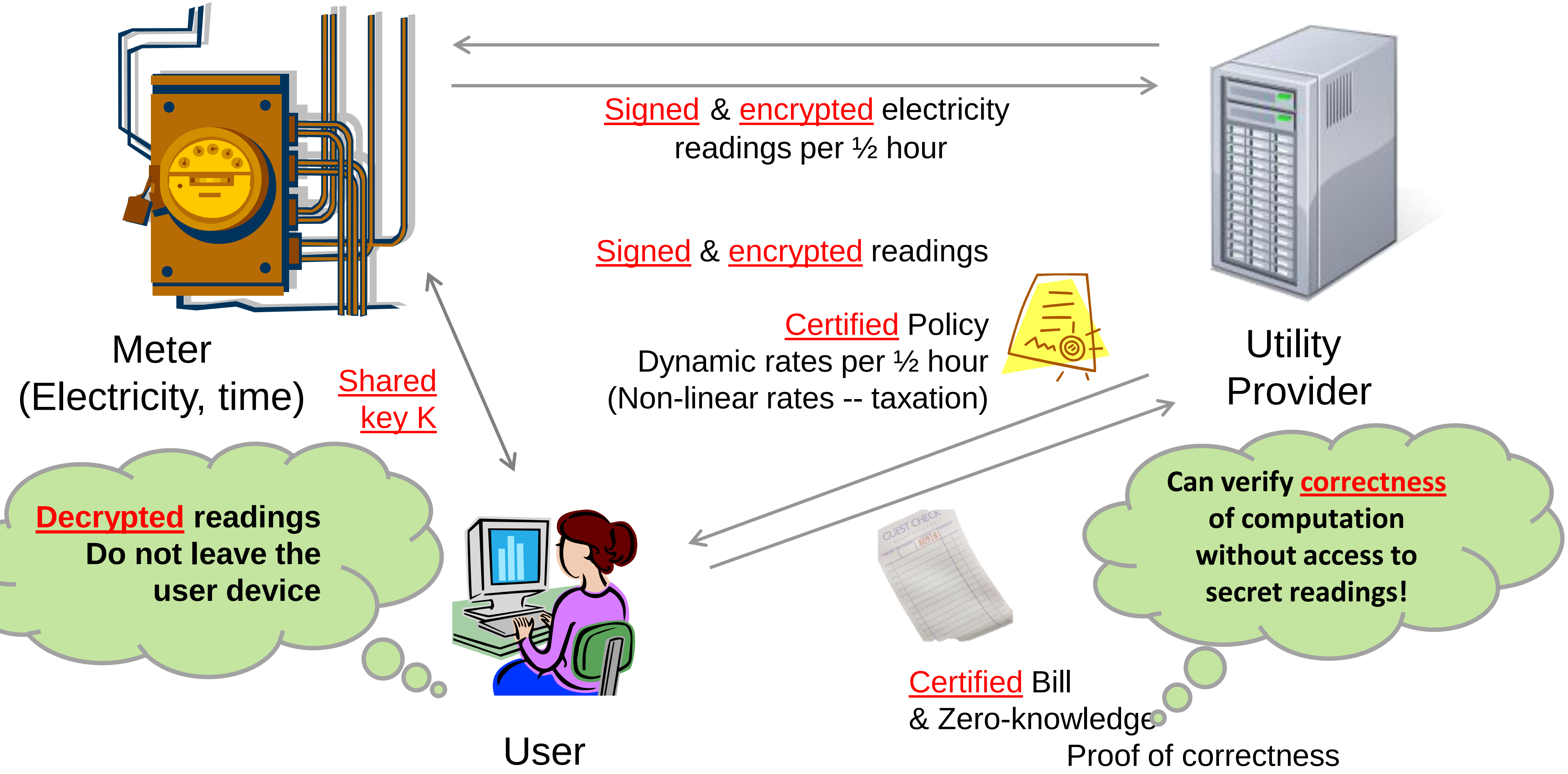


- Agility
  - Use any device to compute bills = user control
  - Compute arbitrary functions of readings aside bills
  - Keep up with changing infrastructure for WAN communications
  - Same meter for different utilities or relying parties

- End-to-end verifiability
  - Bills can be verified, and show to be correct (or incorrect) to third parties.

Our approach

(A) Certified readings & policy (B) Proof of bill & verification



Meter
(Electricity, time)

Shared
key K

Signed & encrypted electricity
readings per ½ hour

Signed & encrypted readings

Certified Policy
Dynamic rates per ½ hour
(Non-linear rates -- taxation)

Utility
Provider

Decrypted readings
Do not leave the
user device

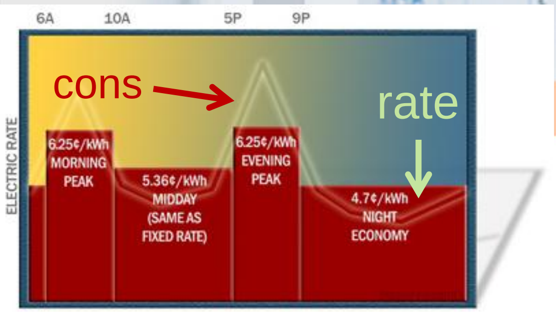
User

Certified Bill
& Zero-knowledge
Proof of correctness

Can verify correctness
of computation
without access to
secret readings!

Two flavours of crypto

- Fast Billing protocol:
  - Special case: policy is public, and selection of rate independent of reading.
  - Very fast: process 3 weeks of all UK data in 12 days on 1 CPU.
- Generic protocol:
  - Supports any tariff policy that can be expressed as table look-ups and polynomial splines.
  - In theory supports any computation (some faster than others)
- Technical report & other resources:
  - http://research.microsoft.com/en-us/projects/privacy_in_metering/



The fast protocol

Reveal! **Hide!**

$$\boxed{Bill} = \Sigma_i\, rate_i \cdot cons_i$$

Meter

Provider

Prove

$Bill = \Sigma_i\, rate_i \cdot cons_i$

$Open' = \Sigma_i\, rate_i \cdot open_i$

Open Readings

$E_k[\{ \ldots, (i, cons_i, open_i) \ldots \}]$

Blind Readings

$\{\ldots\, i, C_i = g^{cons_i} h^{open_i}, \ldots\}_{sign}$

Policy

$\{ \ldots, i \rightarrow rate_i, \ldots\}_{sign}$

User

Blind readings C_i &

$\{Bill, Open'\}_{sign}$

Verify

(Verify all signatures)

$\Pi_i\, C_i^{rate_i} = g^{Bill} h^{Open'}$

ACCEPT or **REJECT**

Commitments ?:

(1) Hiding (2) Binding

Why the verification works?

Verify

1. Verify all signatures
2. Check $\Pi_i\, C_i^{rate_i} = g^{Bill} h^{Open'}$

$$C_i = g^{cons_i} h^{open_i}$$

$$\Pi_i\, C_i^{rate_i} =$$
$$= \Pi_i\, (g^{cons_i} h^{open_i})^{rate_i}$$
$$= \Pi_i\, (g^{cons_i * rate_i}\, h^{open_i * rate_i})$$
$$= g^{\Sigma\, cons_i * rate_i}\, h^{\Sigma\, open_i * rate_i}$$
$$= g^{Bill} h^{Open'}$$

$$(g^a)^b = g^{ab}$$

$$g^a\ g^b = g^{a+b}$$

Prove

$Bill = \Sigma_i\, rate_i \cdot cons_i$

$Open' = \Sigma_i\, rate_i \cdot open_i$

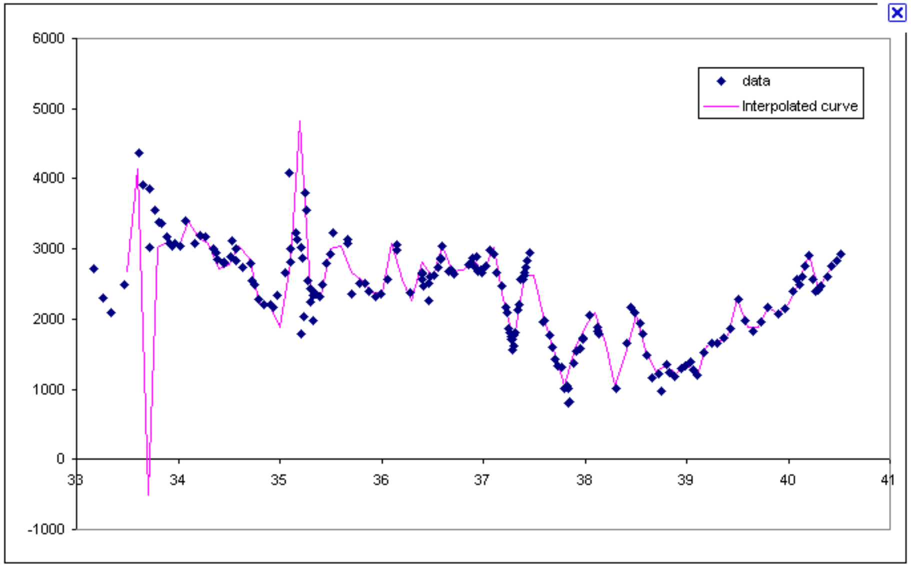
Security: binding property of commitments!
= cannot find a “fake” bill, open’ that opens to the same commitment

General computations?

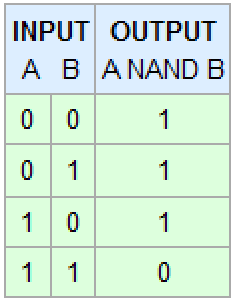
- Fast protocol:
  - Linear algebra: $Result = \Sigma_i\, x_i \cdot cons_i$
- General zero-knowledge proofs:
  - Multiplication $Result = x_i \cdot cons_i$
  - Lookup: $Result = Table[\, cons_i]$
  - Range: $Result = Table[\, min < cons_i < \mathrm{max}]$
  - Polynomial: $Result = a\; cons_i^3 + \mathrm{b}\; cons_i$
  - Any circuit (decompose into gates)

Really any function!

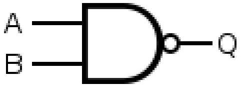
- Ranges + polynomials
  = splines
  = any function



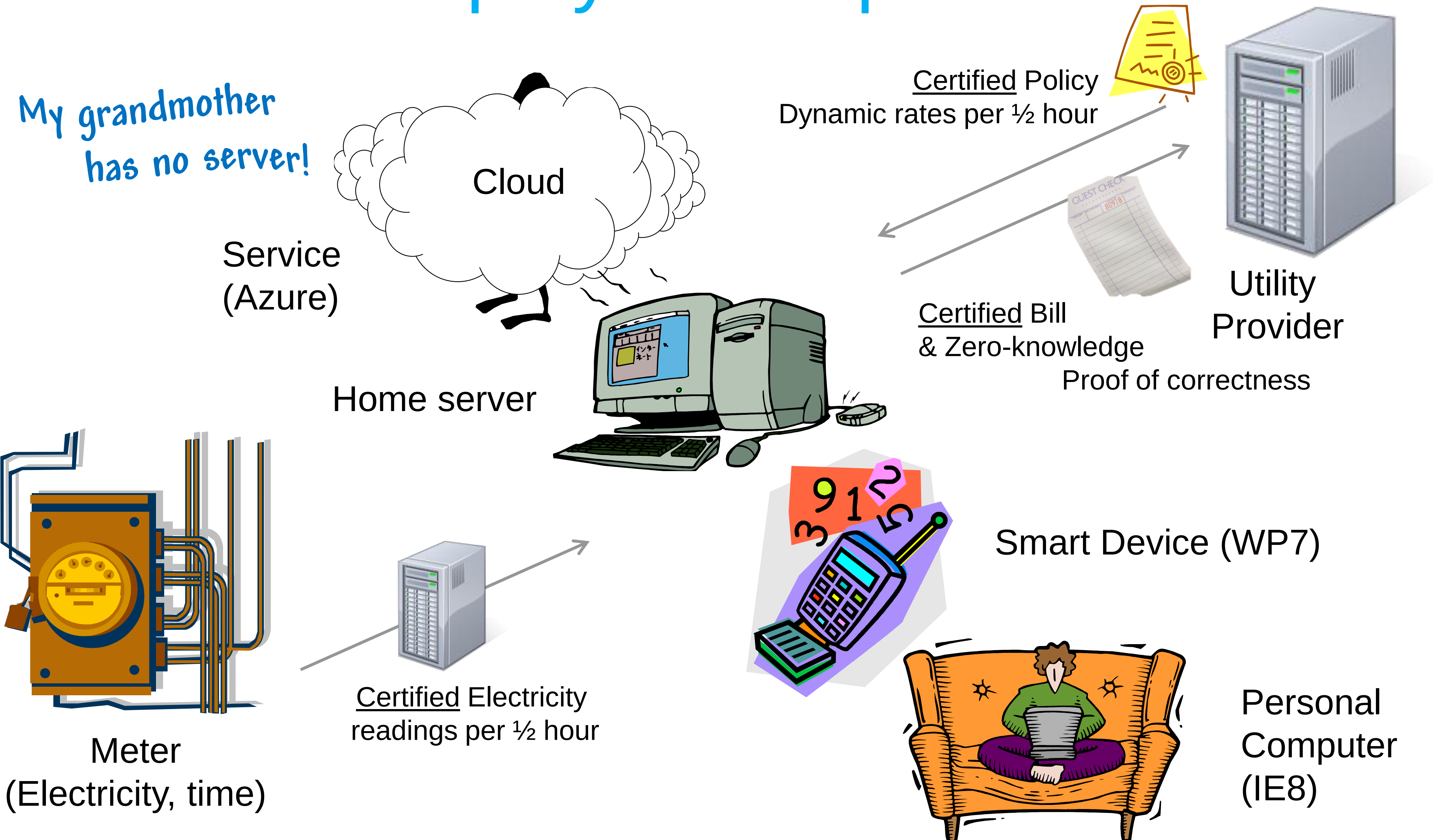
- "*" or Table[]
  = NAND gate
  = any circuit



INPUT		OUTPUT
A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0



Deployment options



My grandmother has no server!

Cloud

Service (Azure)

Home server

Certified Policy
Dynamic rates per ½ hour

Utility Provider

Certified Bill
& Zero-knowledge
Proof of correctness

Meter
(Electricity, time)

Certified Electricity
readings per ½ hour

Smart Device (WP7)

Personal Computer (IE8)

Demo!

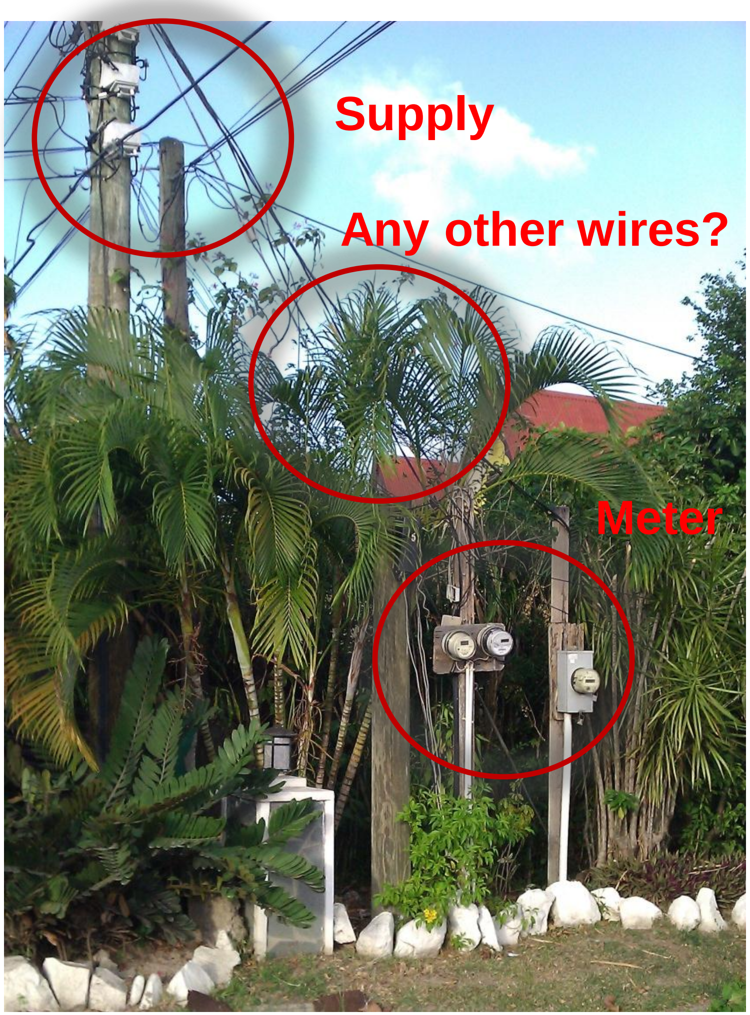
- My grandmother does not understand crypto!

How do we know its secure?

- Proofs & definitions in the UC model
  - Abstract functionality defining metering & billing.
  - Proof that our protocols are indistinguishable from the abstract functionality.
  - Use of lemmas from standard primitives:
    - Commitments, signatures, ZK proofs

- Aspects verified in F# and C (for real meter)

Fraud detection



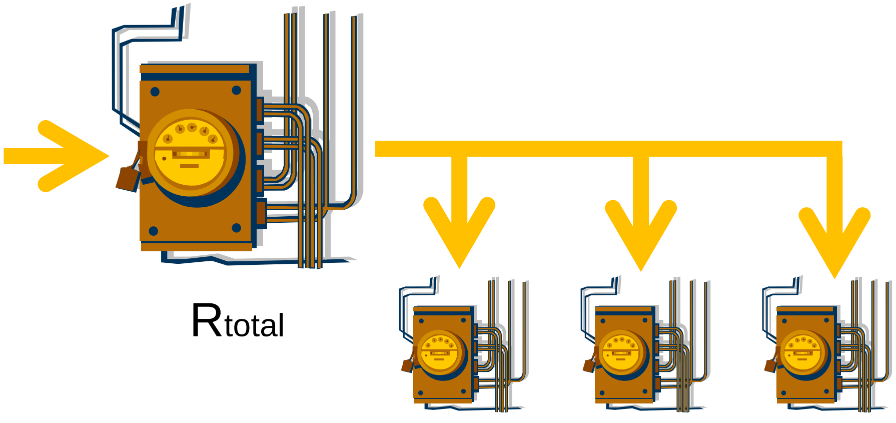
Problem:

- US – about 10%
- Brazil Favelas – 60%

Solution:

- Physical
- Aggregation

Aggregation for fraud detection



R_{total}

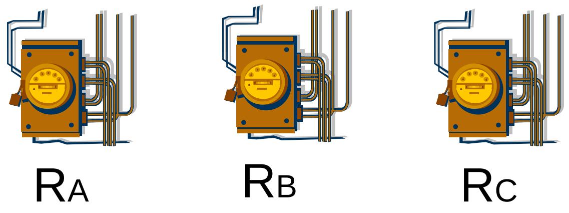
R_A R_B R_C

How to detect fraud?

$R_{total} \gg R_A + R_B + R_C$

- Use a feeder meter for a group of houses
- Sum all house readings
- Compare with feeder meter
- Readings should be about the same

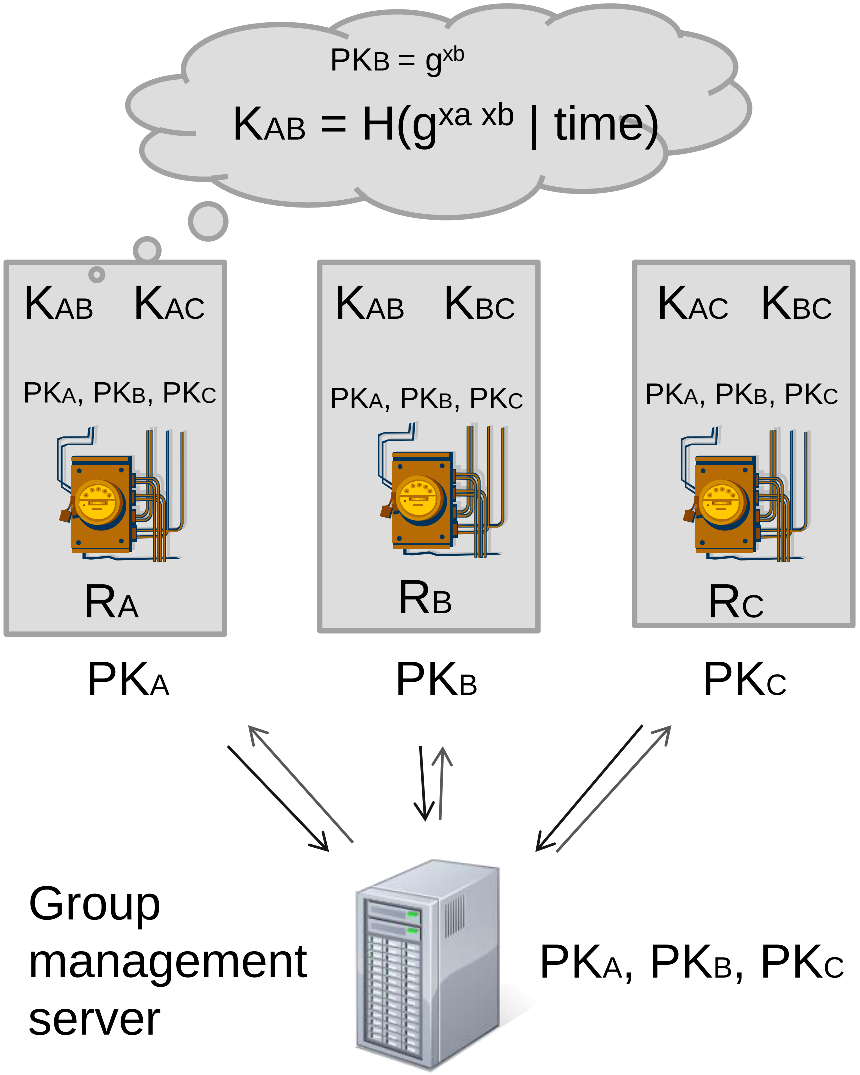
Privacy friendly aggregation



- Aim:
  compute sum without revealing readings.

- 2 Phases:
  - Distribute keys
  - Compute readings

Privacy friendly aggregation



$PK_B = g^{xb}$

$K_{AB} = H(g^{xa\ xb} \mid time)$

K_{AB} K_{AC}

PK_A, PK_B, PK_C

R_A

PK_A

K_{AB} K_{BC}

PK_A, PK_B, PK_C

R_B

PK_B

K_{AC} K_{BC}

PK_A, PK_B, PK_C

R_C

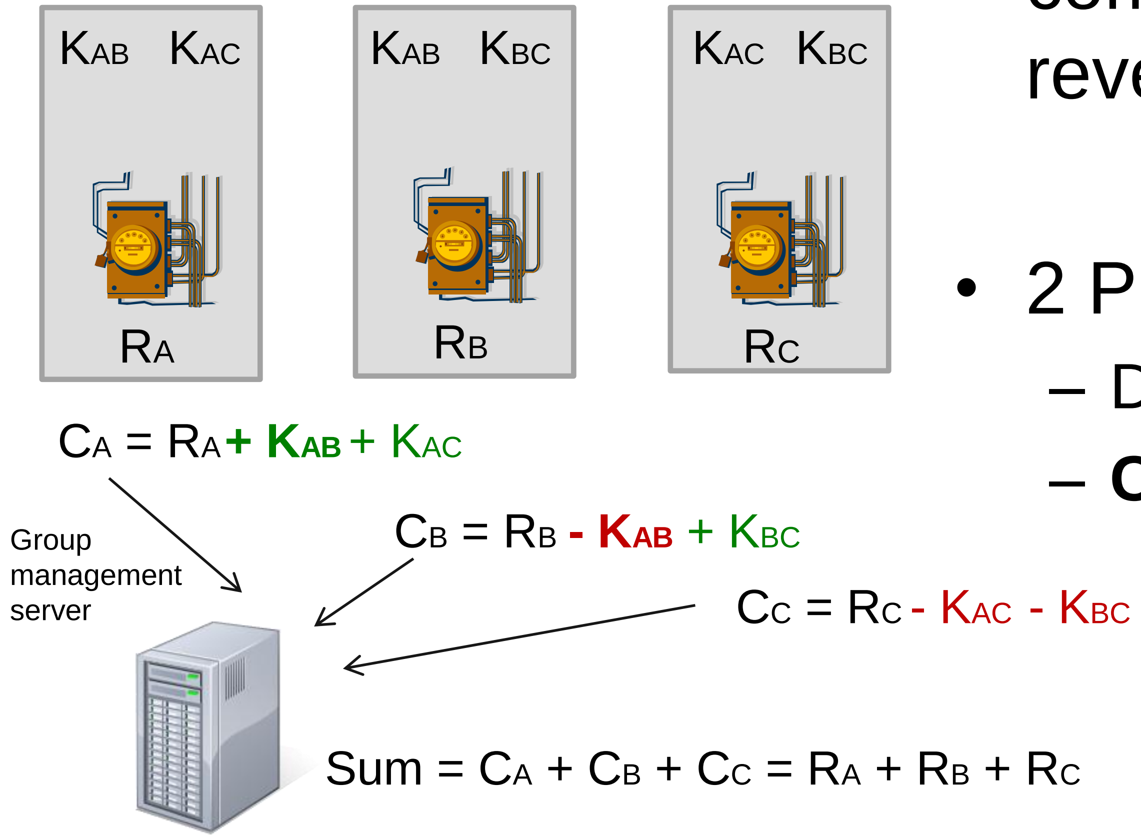
PK_C

Group management server

PK_A, PK_B, PK_C

- Aim:
  compute sum without revealing readings.
- 2 Phases:
  – **Distribute keys**
  – Compute readings

Privacy friendly aggregation



K_{AB} K_{AC}

R_A

K_{AB} K_{BC}

R_B

K_{AC} K_{BC}

R_C

$C_A = R_A + K_{AB} + K_{AC}$

$C_B = R_B - K_{AB} + K_{BC}$

$C_C = R_C - K_{AC} - K_{BC}$

Group management server

$\text{Sum} = C_A + C_B + C_C = R_A + R_B + R_C$

- Aim:
  compute sum without revealing readings.

- 2 Phases:
  - Distribute keys
  - **Compute readings**

Really?

$$\text{Sum} = C_A + C_B + C_C =$$

$$R_A + \cancel{K_{AB}} + \cancel{K_{AC}} + R_B - \cancel{K_{AB}} + \cancel{K_{BC}} \quad R_C - \cancel{K_{AC}} - \cancel{K_{BC}}$$

$$= R_A + R_B + R_C$$

Security & performance

- Privacy friendly aggregation is possible without revealing any readings!
  - (Proofs of security reduce scheme to DH + Hash)

- Very efficient
  - Public keys are 32 bytes
  - No public key operations to generate readings
  - No communication overhead

Where next?

- Language & compiler for complex verifiable computations.
- Automotive applications & metering
  - PAYD, LBS, CC, Tax

Conclusion

- **Smart metering can be done without violating privacy**
- Private billing, and other uses of data are possible.
  - Side information can be revealed (and is certified) for other uses
  - Tariff structure can change as fast as software can be updated on untrusted machines.
  - Fast protocols as fast as uncertified calculations.
  - General protocols well within realm of real-time.
- Aggregation does not require anyone to know detailed readings
  - Can do real time monitoring and fraud detection with privacy
- Paradigm shift: Trustworthy computations in the client domain for privacy.

Resources

Technical report & other resources:

http://research.microsoft.com/en-us/projects/**privacy_in_metering/**

- Alfredo Rial & George Danezis. Privacy-friendly smart metering. Microsoft Research Technical Report MSR-TR-2010-150. November 19, 2010.

- George Danezis, Markulf Kohlweiss, and Alfredo Rial. Differentially Private Billing with Rebates. Microsoft Research Technical Report MSR-TR-2011-10. February 2011.

- Klaus Kursawe, Markulf Kohlweiss, George Danezis. Privacy-friendly Aggregation for the Smart-grid. Microsoft Research Tech Report, March 2011.

- Nikhil Swamy, Juan Chen, Cedric Fournet, Karthikeyan Bharagavan, and Jean Yang. Security Programming with Refinement Types and Mobile Proofs. Microsoft Research Technical Report MSR-TR-2010-149. November 2010.