Microsoft Research

Security and Privacy for 21st Century Metrology

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

NIST PEC Workshop
December 8-9, 2011

Modern metrology

- What is metrology?
- Legal metrology & security (& NIST)
- Liberalization impact
- Digital networked meters
- Digital security & privacy

Microsoft Research

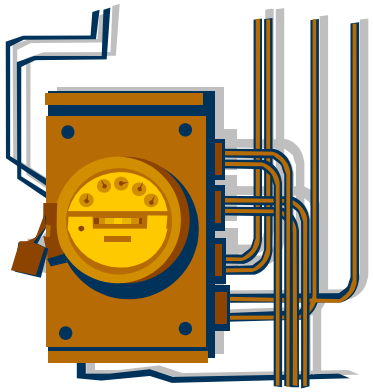
Example: smart electricity meter

Measures power consumption
Over every 15-30 minutes (KW/h)

Utility

- Real time aggregates
- Billing
- Forecasting
- Fraud detection

Registers for input / output (micro generation) and multiple channels



Remote disconnection

Stores readings for up to 13 months.

Tamper resistance

Pre-payment

Wide area network
Communications for control and readings

Microsoft Research

Metering Security or privacy today

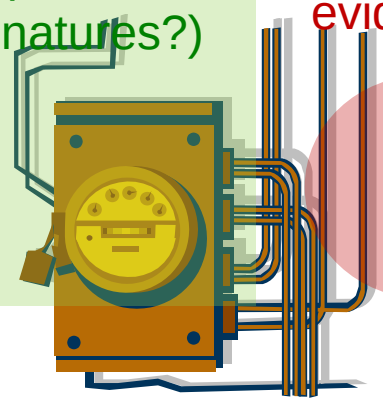
Certification & Tamper evidence (Signatures?)

Chain of evidence gap

Transport security

Exposed readings

Electricity readings per ½ hour



Meter
(Electricity, time)
(Gas, time)

Display

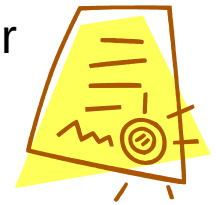
Bill Verification?

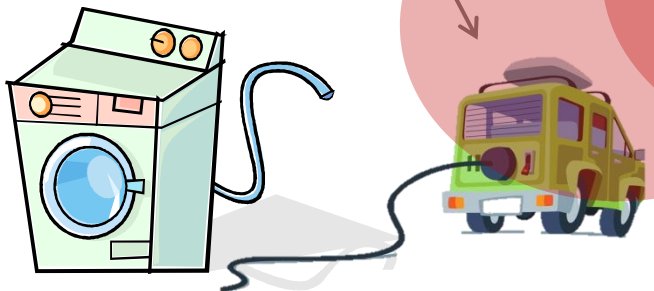
Utility Provider

User control?

Access to data?

Payment





User

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

Desirable security properties

- End-to-end integrity and authenticity
- End-user privacy / information self-determination

- Versatility & public policy objectives
- Robust security engineering

Integrity & Authenticity

- **End-to-end** property:
  - Establish the authenticity & integrity of a reading throughout the life time of the reading.
  - “Valid reading from specific certified metrology unit”
- **Universal** / public verifiability:
  - No need for secrets to verify readings => all parties can verify them.
- Stronger: **integrity of computations**.
  - Interaction with privacy = not trivial.
  - **Software independence** = no chain of custody / can use untrusted hardware.

Privacy & self-determination

- Some readings are **personal data** (DP!)

- Confidentiality / Privacy
  - Gold standard: only data subject has access to raw readings.
  - **Data minimization**: e.g. private aggregation.
  - But: others should still be able to **compute** on them.

- Informational self-determination:
  - Subject can **use readings further** with 3rd parties.
  - **Audit computations** performed on personal data.
  - Use **any device / OS**.

Public policy

- Meters as part of **platform**
  - Need for versatility, extensibility, choice.
  - Lifetime: open to future technologies.
- Support **competition**:
  - No lock-in for any party.
  - High-quality readings for all.
  - Ability to use any user device.
- Support **secondary uses**.
  - Aggregation: with privacy.
- **Need for standardization!**

Microsoft Research

Robust security engineering

- Minimal Trusted Computing Base
  - Minimal trusted hardware
  - Ideally: just the **certified metrology unit**.
  - Amenable to **formal verification**.

Standardization!

- Trusted third parties
  - Ideally: **no TTP**
  - 4C: Cost, Collusion, Corruption, Compromise.

Security & Privacy technologies for metrology

- Special signature scheme
  - Allows for end-to-end integrity & authenticity + privacy friendly computations.

Hint: Sign Pedersen commitments of readings.

- Special encryption scheme
  - Allow for aggregation from ciphertexts to get statistics.

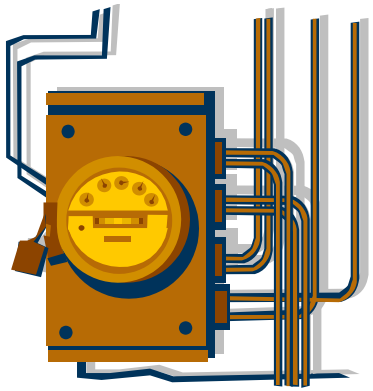
Hint: Blind readings with shares from other meters.

- Standard zero-knowledge techniques
  - Perform computations on user machines while preserving privacy and integrity.

Microsoft Research

Illustration in a smart meter setting

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



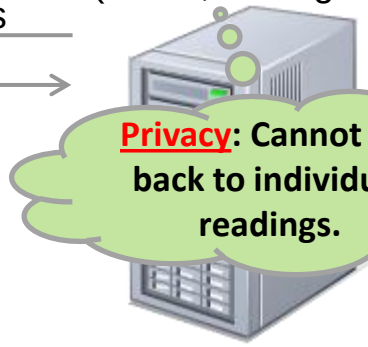
Meter
(Electricity, time)

Shared key K

Define aggregation groups & request readings

Extract aggregates
(Sums, averages, variances)

Signed & encrypted electricity readings per ½ hour



Privacy: Cannot get back to individual readings.

Signed & encrypted readings

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

Utility Provider

Privacy: readings Do not leave the user device

User Device

Can verify correctness of computation without access to secret readings!

Certified Bill
& Zero-knowledge
Proof of correctness

Two flavours of computations

- Fast linear computations (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 computations 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/

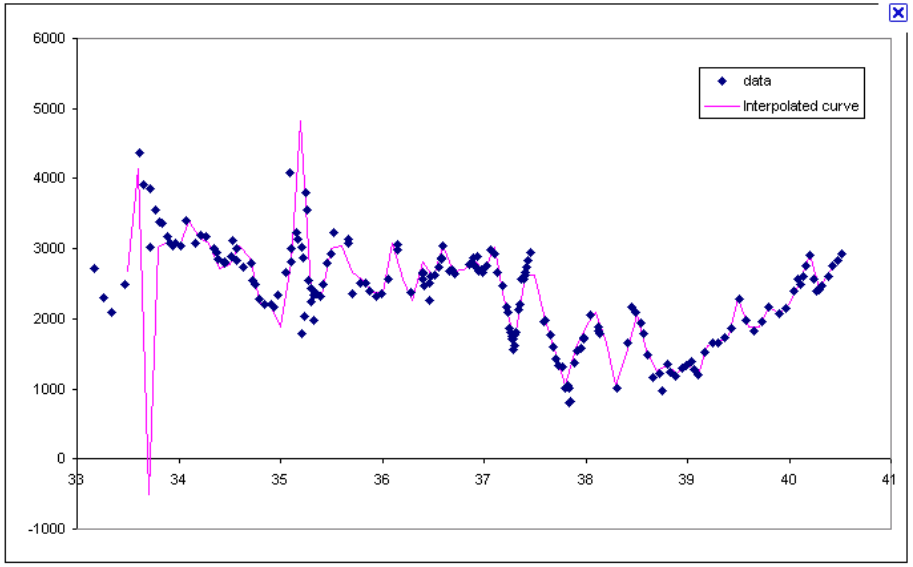
General computations?

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

Microsoft Research

Really any function!

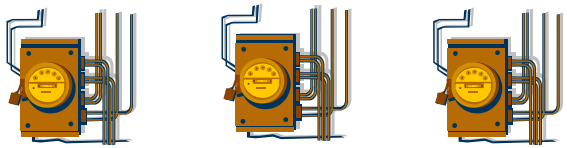
- Ranges + polynomials
  = splines
  = any function



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

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

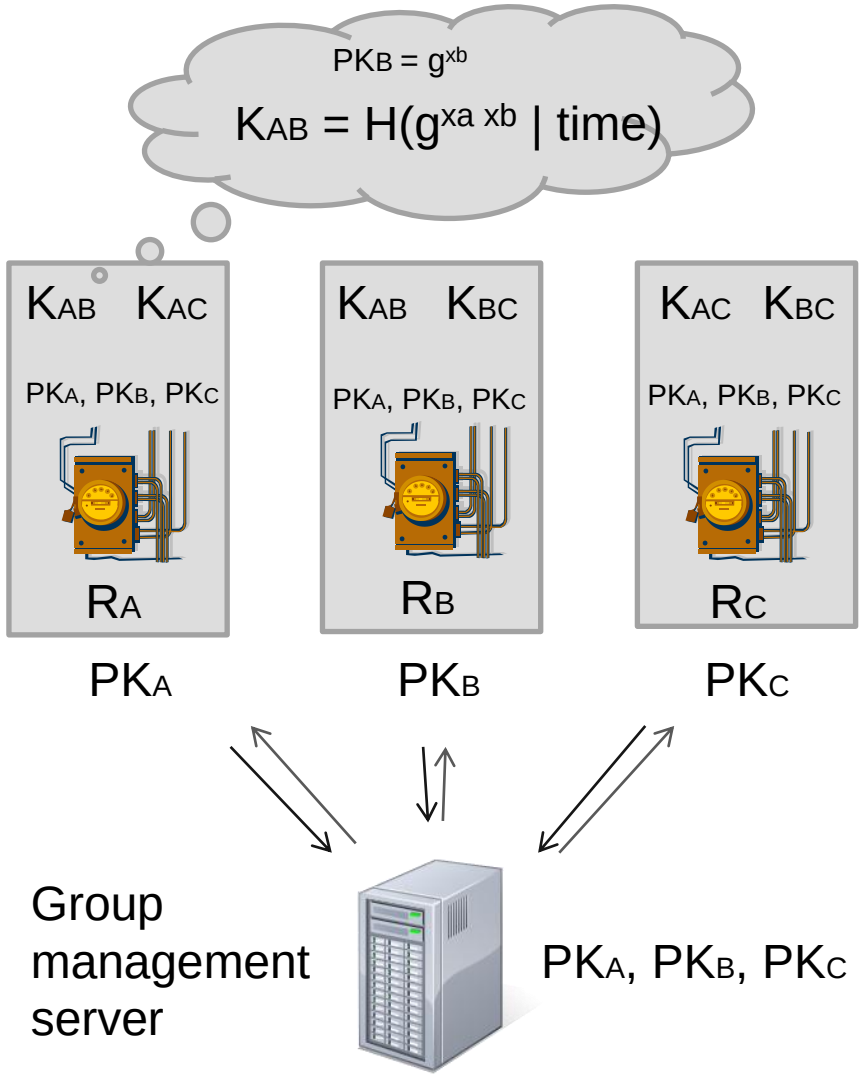
Privacy friendly aggregation



R_A R_B R_C

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

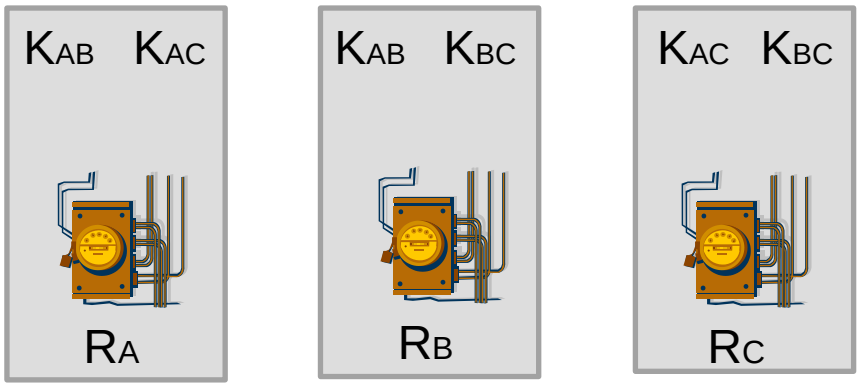
Privacy friendly aggregation



- Aim:
  compute sum without revealing readings.

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

Privacy friendly aggregation



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

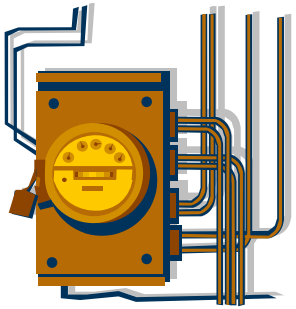
Deployment?

We have augmented
real-world smart meters
to support privacy-friendly
computations and aggregation.

How to deploy?
What is the eco-system?
What is the bigger picture?

Microsoft Research

Deployment: HAG



Metrology unit

Home Access Gateway (HAG)

Description of computation

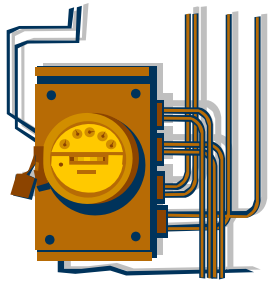
Supplier

- Certified
- Sign + Encrypt readings

- Untrusted HW / SW
- Perform computation
- Audit

- Get aggregates
- Verify computation

Deployment: Cloud + Browser



Metrology unit

- Certified
- Sign + Encrypt readings

Utility Cloud

- Get aggregates

Check + download
Encrypted readings

User Browser

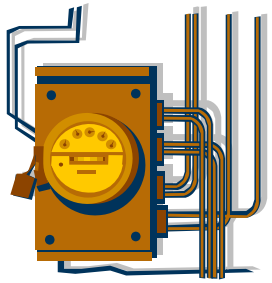
- Untrusted **browser** (js)
- Perform computation

Supplier

- Verify computation

Microsoft Research

Deployment: Cloud + Smart Phone



Metrology unit

- Certified
- Sign + Encrypt readings

Utility Cloud

- Get aggregates

Push readings

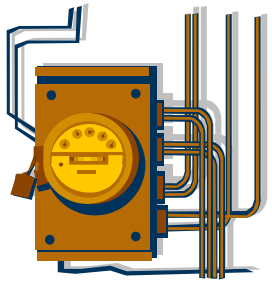
Phone App

- Untrusted **Phone App**
- Perform computation

Supplier

- Verify computation

Deployment: (Cloud | LAN) + PC



Metrology unit

- Certified
- Sign + Encrypt readings

or

Utility Cloud

- Get aggregates

Push / Pull readings

Supplier

- Verify computation

- Untrusted **PC / Laptop**
- Perform computation
- Audit
- Store other uses

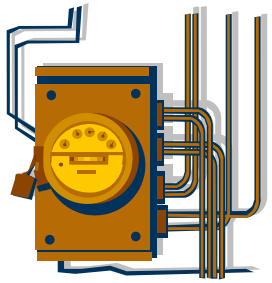
PC

3rd Party service

- Verify computation

Deployment: Cloud + Cloud

My grandmother has no smart phone!



Metrology unit

- Certified
- Sign + Encrypt readings

- Get aggregates

Utility Cloud

Push / Pull readings

Supplier

Verify computation

3rd Party service
(user trusts with readings)

Or *granddaughter*

Authorize!

PC / snail mail

- Delegation
- Perform computation
- Audit
- Store for other uses

Microsoft Research

Key message:

A simple metrology unit enables secure & private uses of readings

What cost?

- Tamper resistant metrology unit
- Key generation (once)
- Pseudo-random functions (negligible)
- Generation of a commitment per reading (2 exp)
- Batch signature of commitments. (2 exp)
- Encryption of readings (aggregation)

- **No communication overhead!**
- **Easy to formally verify!**

Enables …

- End-to-end integrity + authenticity
- Privacy friendly computations
- Privacy-friendly aggregation
- Software independent integrity
- Choice of devices
- Auditability
- Generic & future proof
- …

Leave options open!

Conclusion

- **Metering can be done without violating privacy + with very high integrity**
- **Paradigm shift: Trustworthy computations in the client domain for privacy.**

Microsoft Research

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.