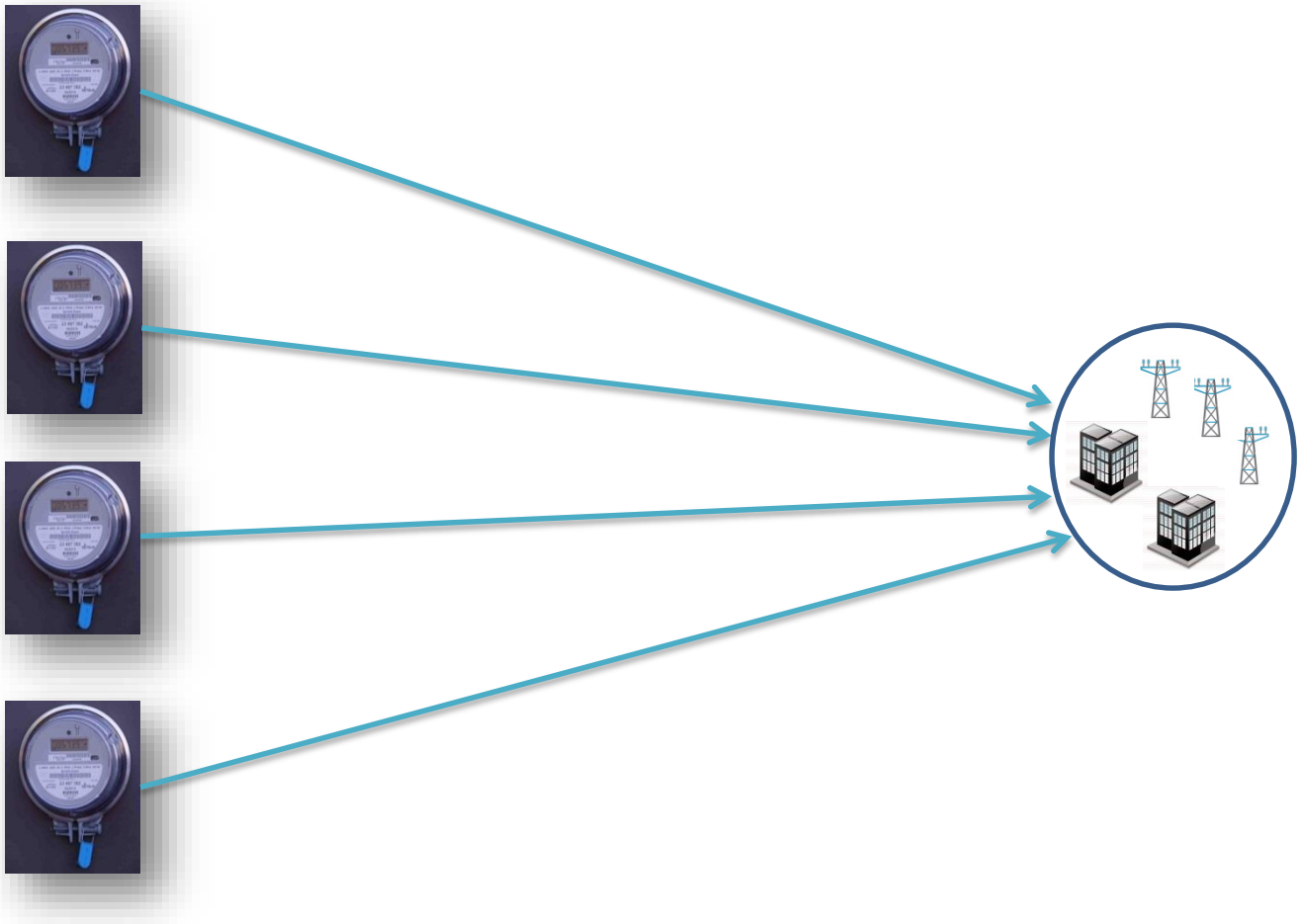
Privacy Preserving Statistics in the Smart Grid

Iraklis Leontiadis, Refik Molva, Melek Önen

Eurecom - France

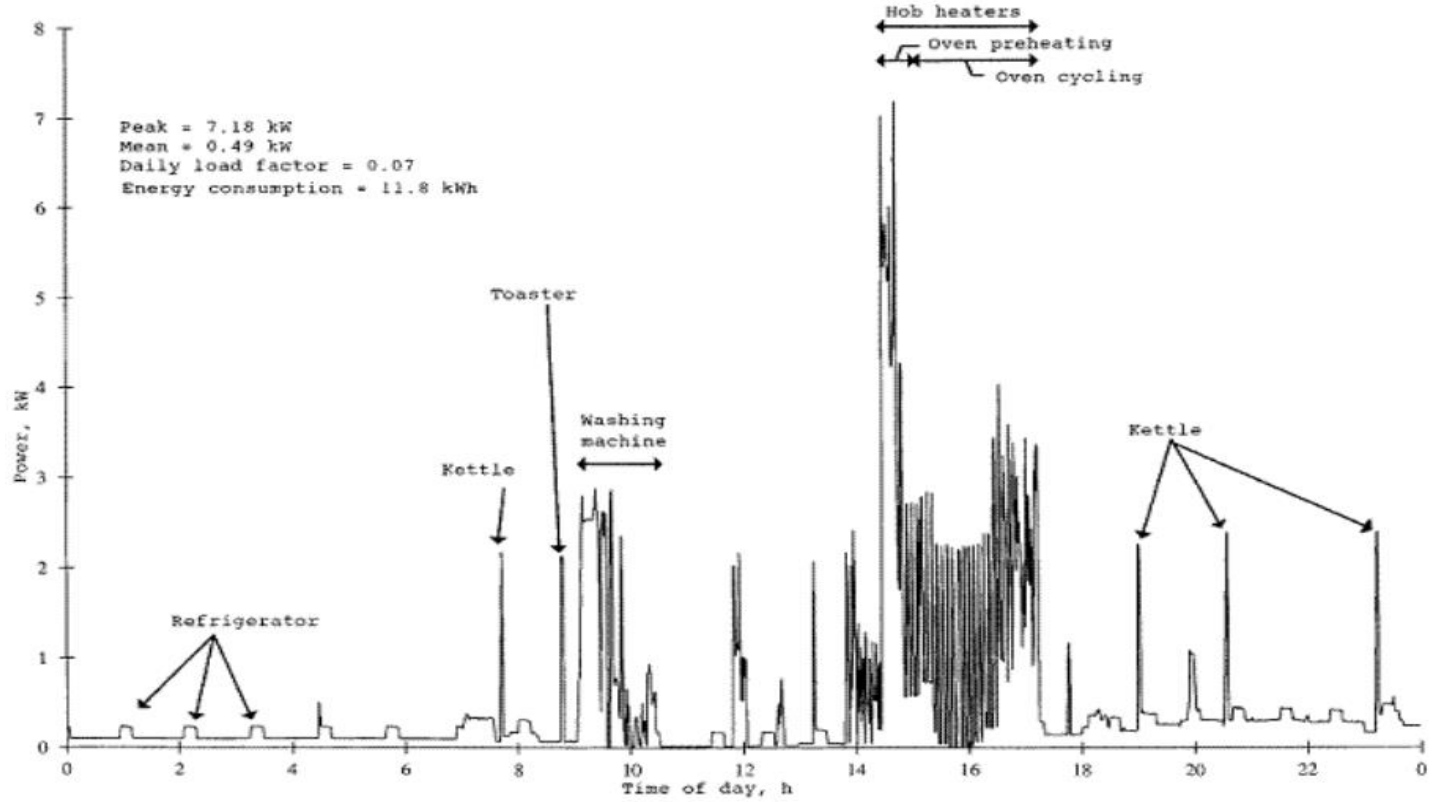
Smart metering



- Promote awareness
- Energy allocation - forecasting
- Fraud detection
- Billing

Privacy concerns

"Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid"



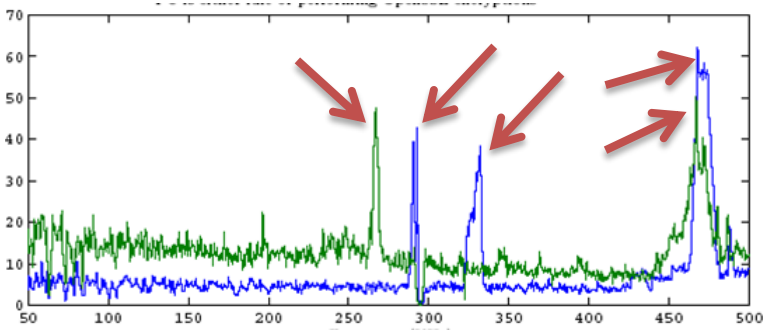
Existing work

- Private aggregation of data
  - Secret sharing [ET2012]
  - Differential privacy [JK2012, CSS2012, RN2010]
  - Trusted Key Dealer [SCRCS2011, JL2013]

Motivation

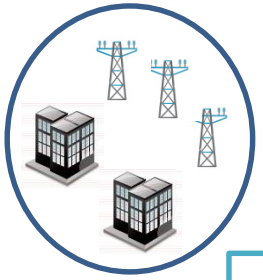
- Provide accurate individual Statistics

Obfuscate real values but reveal the order



Augment functionality by detecting spontaneous peaks

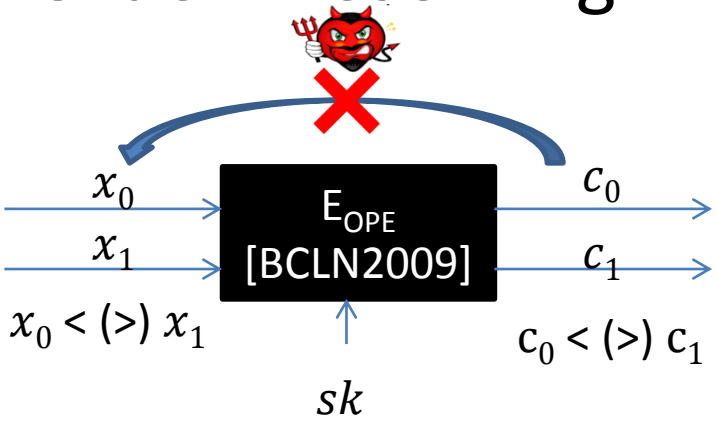
When did dwelling consume the maximum energy?



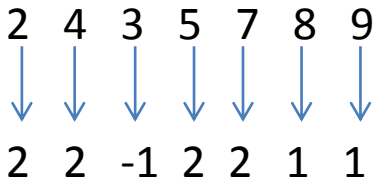
Promote awareness

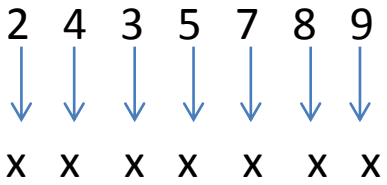
Building blocks

- Symmetric Order Preserving Encryption



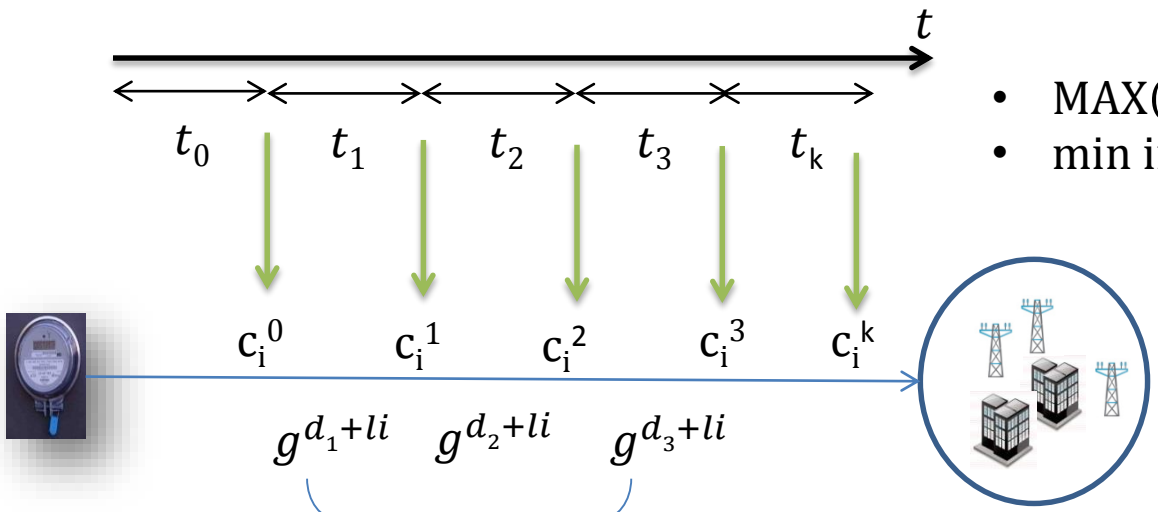
- Secure Delta encoding



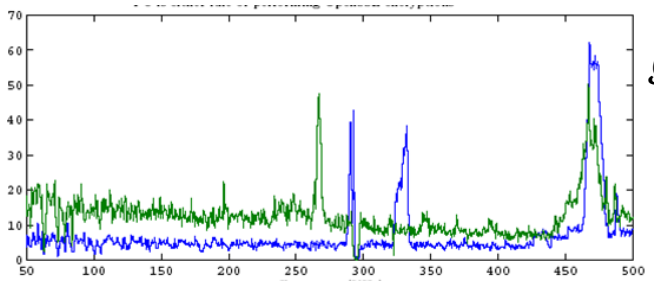


Our Scheme

$$E_{OPE}(sk_i, xij) = c_i^j$$



- MAX($\{c_i^j\}$) at tm
- min interval = n

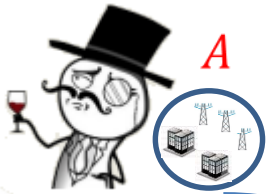


g^{nli}

$$\prod_{w_{start}}^{w_{end}} g^{d_i^j+l_i} = g^{\sum_{w_{start}}^{w_{end}} g^{d_i^j+l_i}} \stackrel{?}{=} (g^{l_i})^n$$

Third Party Obliviousness

C



A

$x_{i,t}$

$i \neq \{0,1,2,3\}$

$E_{OPE}(x_{i,t}, s_i) = c_{i,t}$

Learning phase

$d_0 = x_1 - x_0, d_1 = x_3 - x_2,$
$\{x_1, x_0\}, \{x_3, x_2\}$ same order

Challenge

$b \leftarrow \{0,1\}$

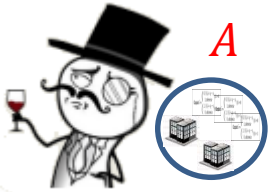
$\begin{cases} c_1, c_0 & if\ b=0 \\ c_3, c_2 & if\ b=1 \end{cases}$

Outputs b'. Is b'=b?

Reductionist proof to POPF-CCA

$Game^{POPF-CCA}$

B



A

$x_{i,t}$ $i \neq \{0,1,2,3\}$

$\{x_i\}_{i \neq 0,1}$

$\{c_i\}$

$\{ci\}$

x_0, x_1

$d_0 = x_2 - x_0, d_1 = x_2 - x_1,$
$\{x_1, x_0\}, \{x_3, x_2\}$ same order

$b^* \leftarrow \{0,1\}$

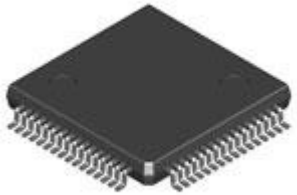
c_{b^*}

c_{b^*}, c_2

$$\text{Outputs } b^* = \begin{cases} \begin{cases} 0, & if\ d_0 = x_2 - x_0 \\ 1, & otherwise \end{cases} & if\ b = 0 \\ \begin{cases} 1, & if\ d_1 = x_2 - x_1 \\ 0, & otherwise \end{cases} & if\ b = 1 \end{cases}$$

Evaluation

- Data set [BMICSA2009]
  - 1700 square foot home
  - Maximum 2KB
- Device [Texas Instruments MSP430 Microcontrollers]
  - 16-bit RISC MSP430X MCU
  - 256KB Flash
  - 20 MHz clock rate
  - AES Accelerator



Encryption overhead

[GL12]

Frequency (seconds)	#Meterings	Flash(KB)	Time (Mcb)
1	86400	172.8	13.33
2	43200	86.4	6.32
3	28800	56.6	4.08
4	21600	43.2	2.99
5	17280	34.5	2.35
6	14400	28.8	1.93
7	12343	24.6	1.63
8	10800	21.6	1.41
9	9600	19.3	1.24
10	8640	17.2	1.10

TABLE III: Space and computation analysis. Mcb denotes megacycles per block

Recap

- Identify the time interval of the continuous maximum consumption
- With privacy guarantees where nothing but the time interval is revealed
- Solution : OPE + delta encodings
- Reductionist security proof to POPF-CCA

Questions?

Thank you!!!

Iraklis Leontiadis
leontiad@eurecom.fr

References

- [ET2012]: Private Computation of Spatial and Temporal Power Consumption with Smart Meters. ACNS 2012
- [JK2012]: Fault-Tolerant Privacy-Preserving Statistics. Privacy Enhancing Technologies 2012
- [CSS2012]: Privacy-Preserving Stream Aggregation with Fault Tolerance. Financial Cryptography 2012
- [RN2010]: Differentially private aggregation of distributed time-series with transformation and encryption. SIGMOD Conference 2010
- [SCRCS2011]: Privacy-Preserving Aggregation of Time-Series Data. NDSS 2011
- [JL2013]: A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data. Financial Cryptography 2013