



On Privacy-Preserving Protocols for Smart Metering Systems

Defense - Verteidigung - Seminário de Pós-Graduação

Fábio Borges

Laboratório Nacional de Computação Científica (LNCC)
Coordenação de Sistemas e Redes (CSR)



Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

PPP3 - Based on Asymmetric DC-Net (ADC-Net)

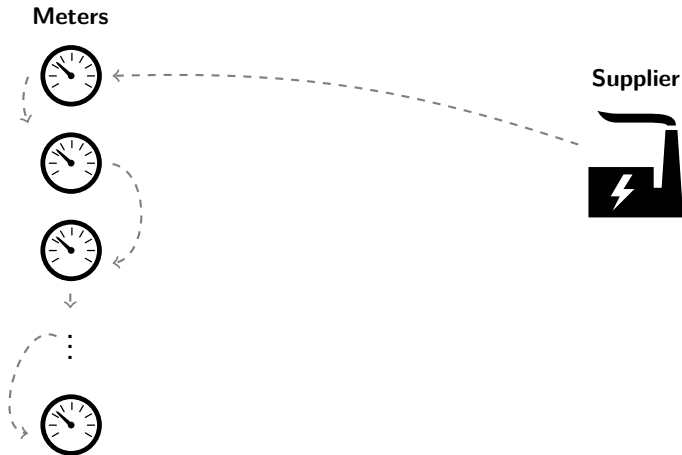
PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook





Meters

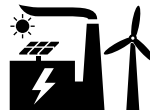


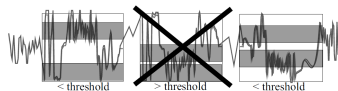
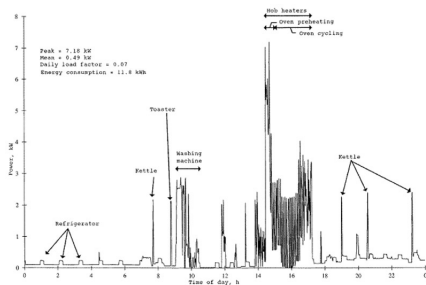
⋮



Year: 2015

Supplier





output matches to logfile

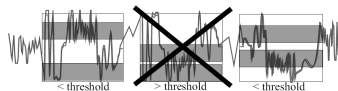
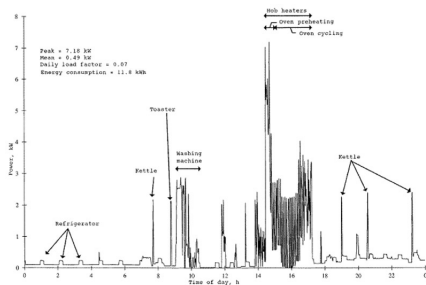


movie tng1
chunk 1 at 2103h

movie tng1
chunk 3 at 2113h

[NIST]

[GJL12]



output matches to logfile



movie tng1
chunk 1 at 2103h



movie tng1
chunk 3 at 2113h

[NIST]

[GJL12]

EU - Official Journal L No.315

80% of households equipped with smart meters by 2020 in EU

Meters

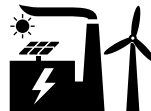


⋮



Round: j

Supplier



$m_{1,j}$

$m_{2,j}$

$m_{3,j}$

$m_{i,j}$

$m_{\tilde{i},j}$

Meters

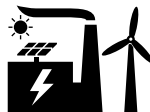


⋮



Round: j

Supplier



$m_{1,j}$

$m_{2,j}$

$m_{3,j}$

$m_{i,j}$

$m_{\tilde{i},j}$

Meters

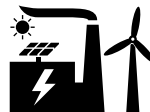


⋮



Round: j

Supplier



$m_{1,j}$

$m_{2,j}$

$m_{3,j}$

$m_{i,j}$

$m_{\tilde{i},j}$

Meters

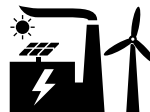


⋮



Round: j

Supplier



$Enc(m_{1,j})$

$Enc(m_{2,j})$

$Enc(m_{3,j})$

$Enc(m_{i,j})$

$Enc(m_{\tau,j})$

Meters



⋮



$Enc(m_{1,j})$

$Enc(m_{2,j})$

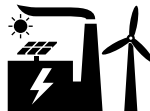
$Enc(m_{3,j})$

$Enc(m_{i,j})$

$Enc(m_{\tau,j})$

Round: j

Supplier



Meters



⋮



$Enc(m_{1,j})$

$Enc(m_{2,j})$

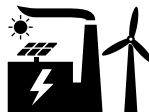
$Enc(m_{3,j})$

$Enc(m_{i,j})$

$Enc(m_{\tau,j})$

Round: j

Supplier



Consolidated Consumption versus Billing

Round	1	2	...	\tilde{j}	Billing
Meter 1	$m_{1,1}$	$m_{1,2}$...	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$...	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
⋮	⋮	⋮	⋮	⋮	⋮
Meter \tilde{i}	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$...	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidated	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$...	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	=

Round	1	2	...	\tilde{j}	Billing
Meter 1	$m_{1,1}$	$m_{1,2}$...	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$...	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
⋮	⋮	⋮	⋮	⋮	⋮
Meter \tilde{i}	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$...	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidated	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$...	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	=



PPPs only work with large aggregations

Aggregation

Meters



$Enc(m_{1,j})$



$Enc(m_{2,j})$



$Enc(m_{3,j})$

⋮

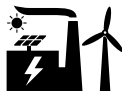
$Enc(m_{i,j})$




$Enc(m_{\tilde{i},j})$

$$c_j = \prod_{i=1}^{\tilde{i}} Enc(m_{i,j}) = Enc\left(\sum_{i=1}^{\tilde{i}} m_{i,j}\right)$$


Supplier




Requirement 1

Recoverability of consolidated consumption 


Requirement 1

Recoverability of consolidated consumption 


Requirement 2

Recoverability of bill based on dynamic pricing 


Requirement 1

Recoverability of consolidated consumption 


Requirement 2

Recoverability of bill based on dynamic pricing 


Requirement 3

Verification (auditability) 


Requirement 1

Recoverability of consolidated consumption 

Requirement 2

Recoverability of bill based on dynamic pricing 

Requirement 3

Verification (auditability) 

Requirement 4

Efficiency 

Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

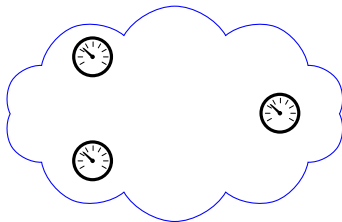
PPP3 - Based on Asymmetric DC-Net (ADC-Net)

PPP4 - Based on Quantum Cryptography

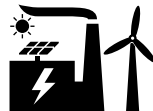
ADC-Nets

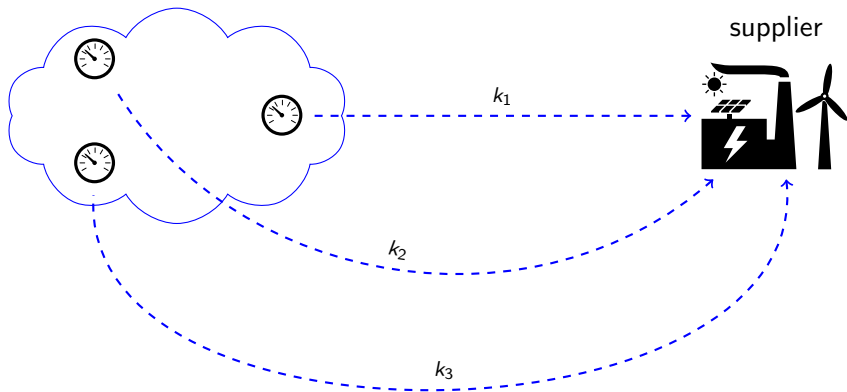
Simulation Using Real-World Data

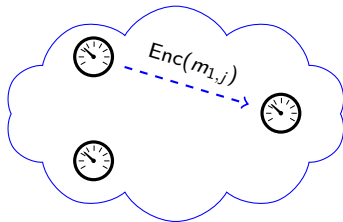
Conclusion and Outlook



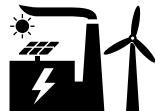
supplier

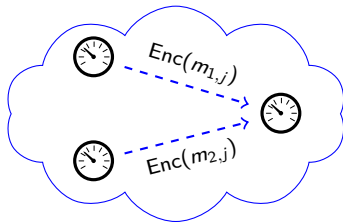




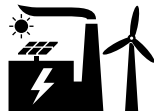


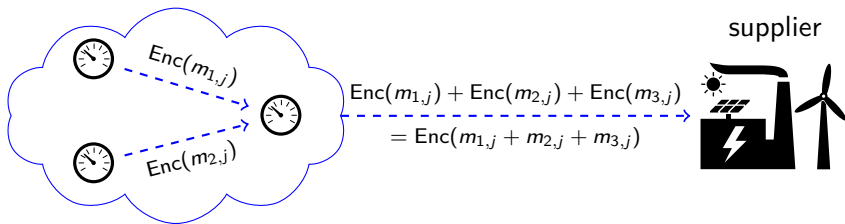
supplier

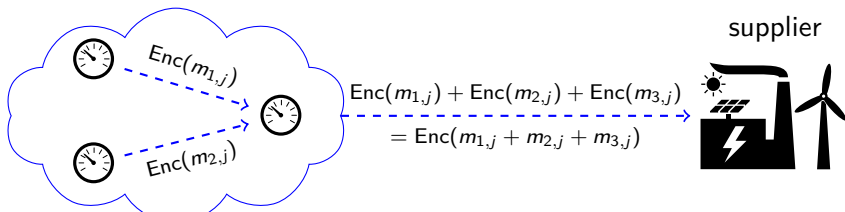




supplier

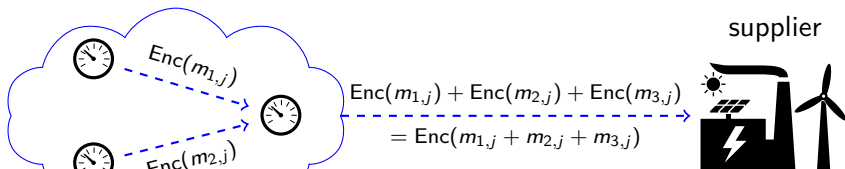






Encryption

$$\text{Enc}(m_{i,j}) = m_{i,j} + H(k_i || j)$$

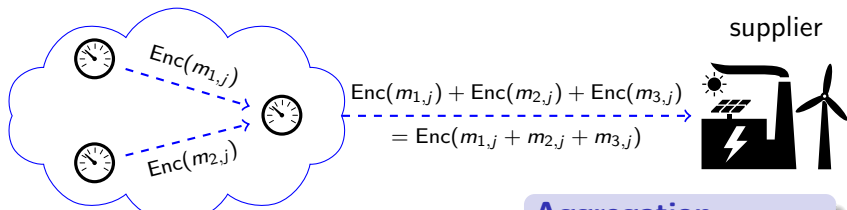


Encryption

$$\text{Enc}(m_{i,j}) = m_{i,j} + H(k_i || j)$$

Aggregation

$$C = \sum_{i=1}^N \text{Enc}(m_{i,j})$$



Encryption

$$\text{Enc}(m_{i,j}) = m_{i,j} + H(k_i || j)$$

Aggregation

$$C = \sum_{i=1}^N \text{Enc}(m_{i,j})$$


Decryption

$$\text{Dec}(C) = C - \sum_{i=1}^N H(k_i || j) = \sum_{i=1}^N m_{i,j}$$


Requirement 1 - ✓

Recoverability of consolidated consumption 


Requirement 2 - ✗

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✗

Verification (auditability) 

Requirement 4 - ✓

Efficiency 

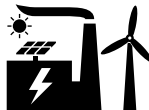
Meters



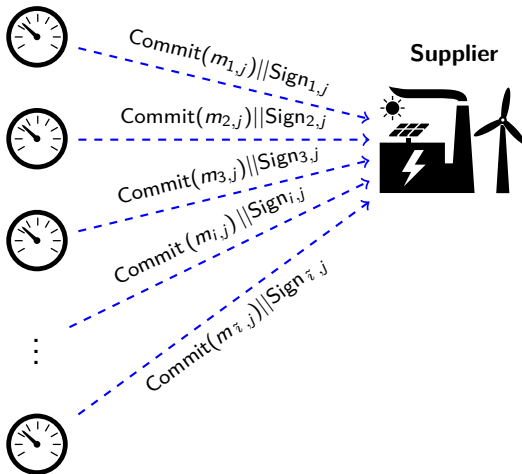
⋮




Supplier




Meters




Requirement 1 - ✗

Recoverability of consolidated consumption 


Requirement 2 - ✓

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✓

Verification (auditability) 

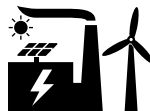
Requirement 4 - ✓

Efficiency 

Meter *i*



Supplier

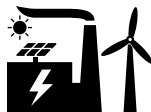


Meter i



$\text{Enc}(m_{i,j}), \text{Enc}(m_{i,j+1}), \dots$

Supplier

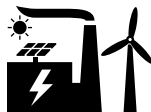


Meter i



$\text{Enc}(m_{i,j}), \text{Enc}(m_{i,j+1}), \dots$

Supplier



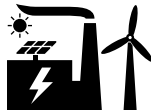
$$Q = \sum_j \text{Enc}(m_{i,j}) = \sum_j k_i \cdot H_\Omega(j) + m_{i,j} \cdot P$$

$$v = \sum_j m_{i,j} \text{ and } V = \sum_j k_i \cdot H_{\Omega}(j)$$

Meter i



Supplier



$\text{Enc}(m_{i,j}), \text{Enc}(m_{i,j+1}), \dots$

$$Q = \sum_j \text{Enc}(m_{i,j}) = \sum_j k_i \cdot H_{\Omega}(j) + m_{i,j} \cdot P$$

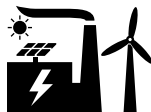
$$v = \sum_j m_{i,j} \text{ and } V = \sum_j k_i \cdot H_{\Omega}(j)$$

Meter i



$\text{Enc}(m_{i,j}), \text{Enc}(m_{i,j+1}), \dots$

Supplier

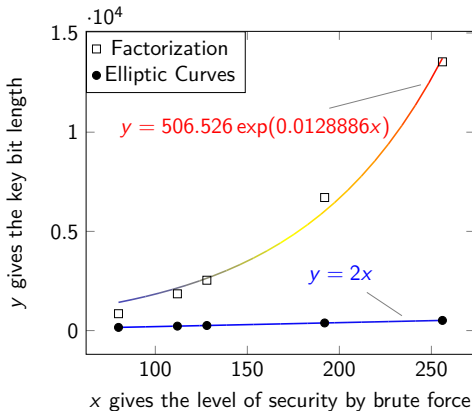


$$Q = \sum_j \text{Enc}(m_{i,j}) = \sum_j k_i \cdot H_{\Omega}(j) + m_{i,j} \cdot P$$

Verification

$$v \cdot P \stackrel{?}{=} Q - V$$

$$\exp\left(\left(\left(\frac{64}{9}\right)^{1/3} + O(1)\right) (\ln n)^{1/3} (\ln \ln n)^{2/3}\right) = 2^x = \sqrt{\frac{\pi O}{2}},$$



Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

PPP3 - Based on ADC-Net

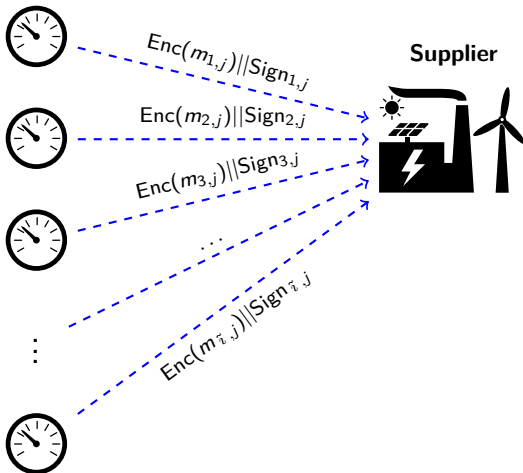
PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook

Meters



Meters



Enc

Encryption

$$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{n^2}$$

$$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \pmod{n^2}$$



Enc(m_{2,j}) || Sign_{2,j}



Enc(m_{3,j}) || Sign_{3,j}



⋮

Enc(m_{i,j}) || Sign_{i,j}



Meters



Enc

Encryption

$$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{n^2}$$

$$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \pmod{n^2}$$



Enc(m_{2,j}) || Sign_{2,j}

Enc(m_{3,j}) || Sign_{3,j}



...

Enc(m_{i,j}) || Sign_{i,j}

⋮



Aggregation

$$\mathcal{C}_j = \prod_{i=1}^{\bar{i}} \text{Enc}_i(m_{i,j})$$

Meters



Enc

Encryption

$$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{n^2}$$

$$\text{Enc}_i(m_{i,j}) \mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \pmod{n^2}$$



Enc(m_{2,j}) || Sign_{12,j}

Enc(m_{3,j}) || Sign_{3,j}



Aggregation

$$\mathcal{C}_j = \prod_{i=1}^{\bar{i}} \text{Enc}_i(m_{i,j})$$



...

Decryption

$$\text{Dec} : \mathbb{Z}_{n^2} \rightarrow \mathbb{Z}_n$$


$$\text{Dec}(\mathcal{C}_j) \mapsto \frac{(\mathcal{C}_j \cdot g^{-h_t \cdot s} \pmod{n^2}) - 1}{n}$$

⋮


Enc(m_{i,j})




Requirement 1 - ✓

Recoverability of consolidated consumption 


Requirement 2 - ✓

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✓

Verification (auditability) 

Requirement 4 - ✓

Efficiency 

No Keys [BSM14; BPP12]

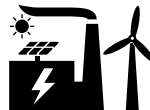
Meters

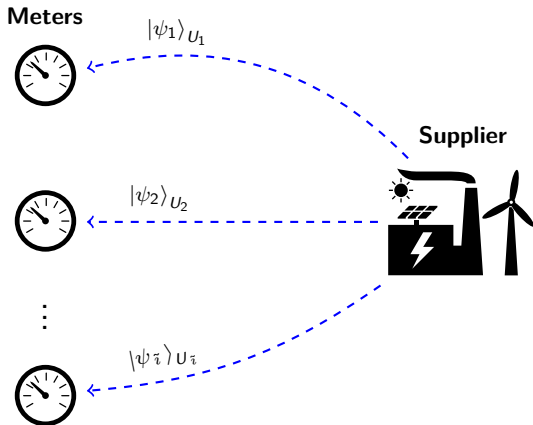


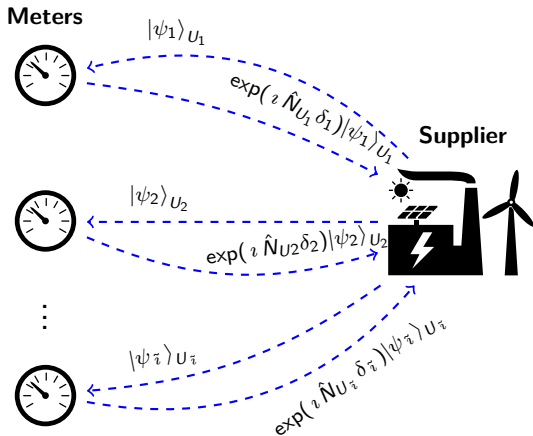
⋮



Supplier









Requirement 1 - ✓

Recoverability of consolidated consumption 


Requirement 2 - ✗

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✗

Verification (auditability) 

Requirement 4 - depends on quantum devices

Efficiency 

Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

PPP3 - Based on Asymmetric DC-Net (ADC-Net)

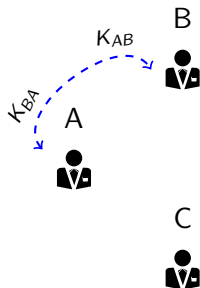
PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

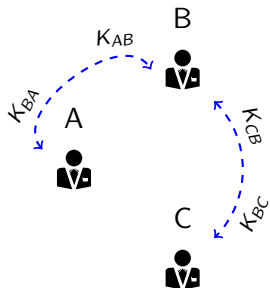
Conclusion and Outlook





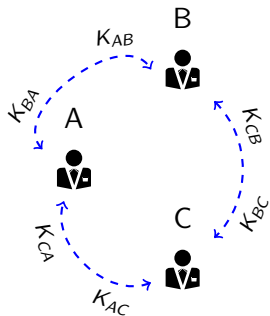
Agent





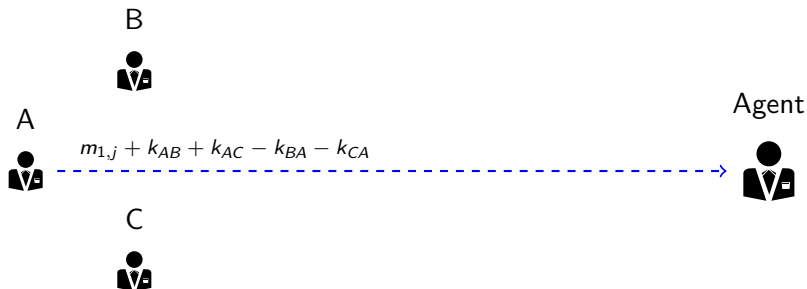
Agent

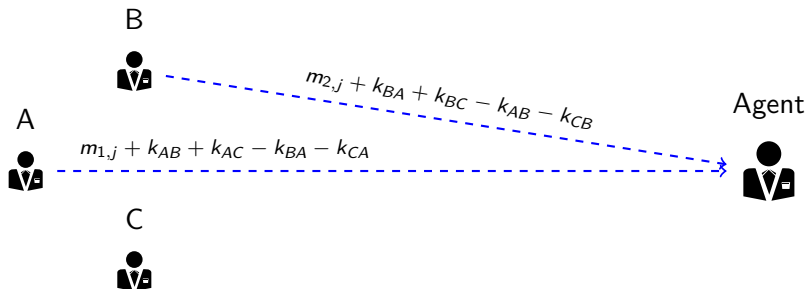


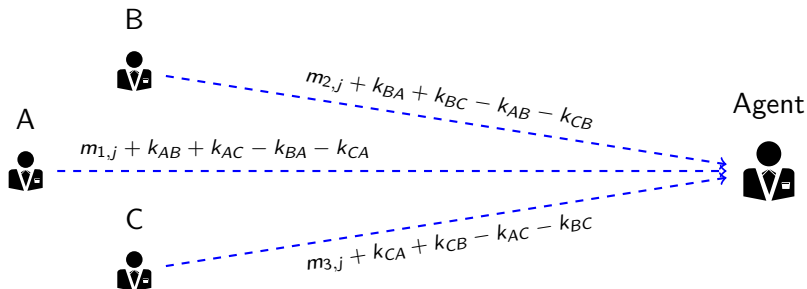


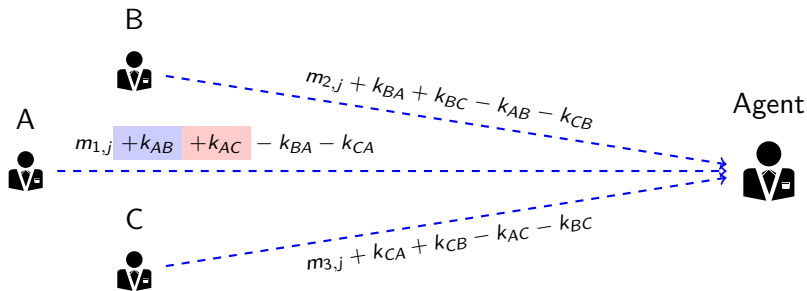
Agent

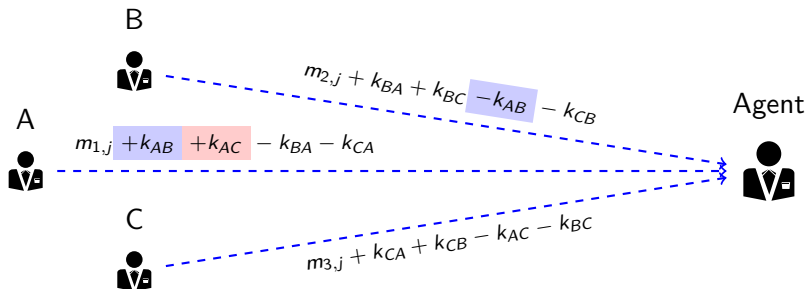


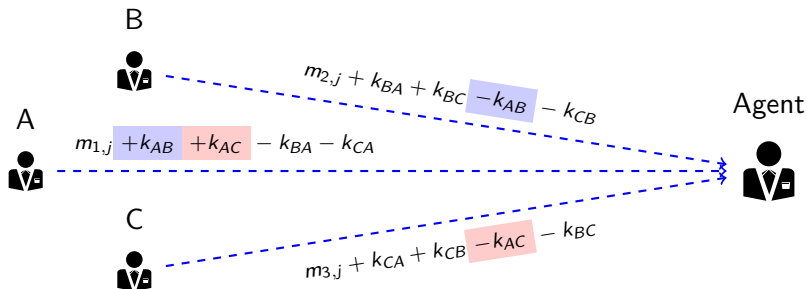




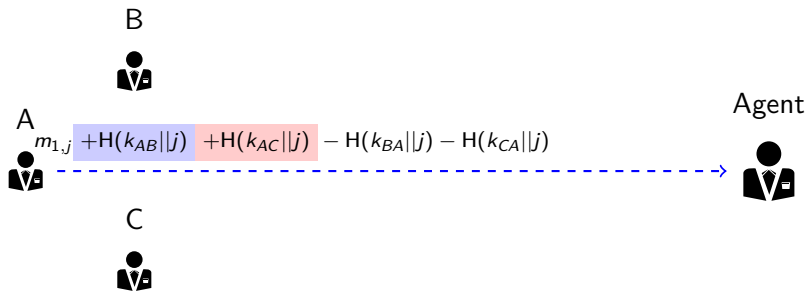


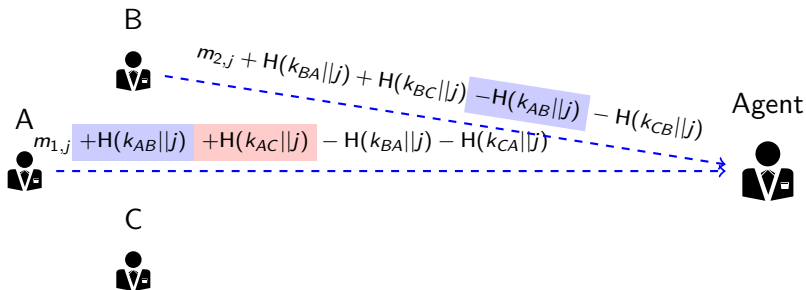


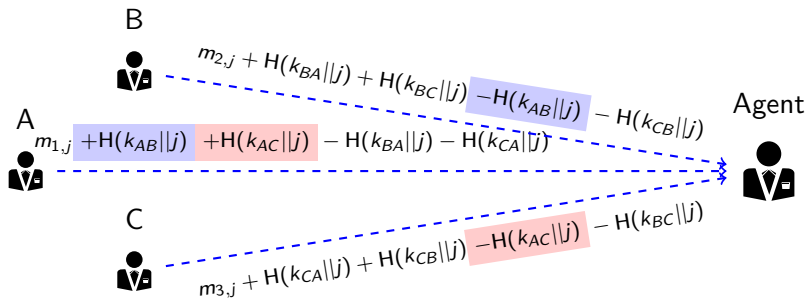


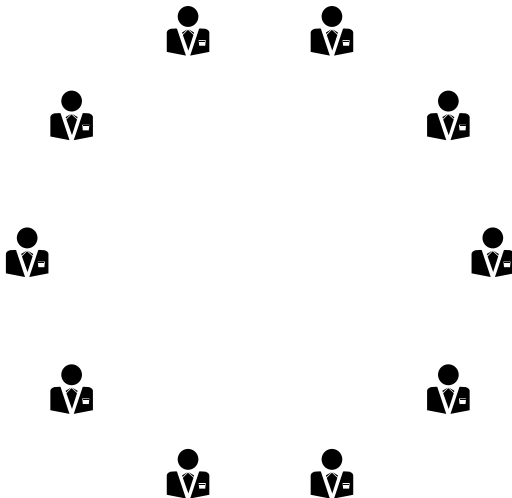


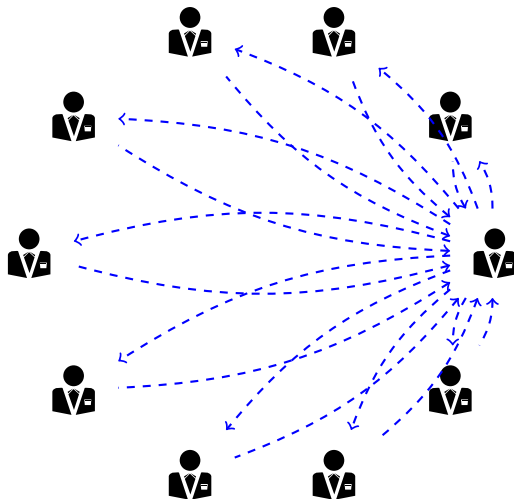


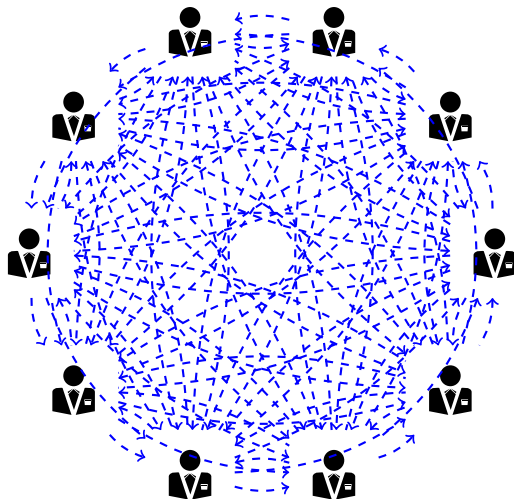




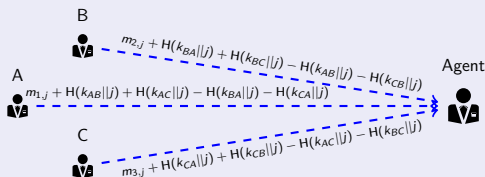




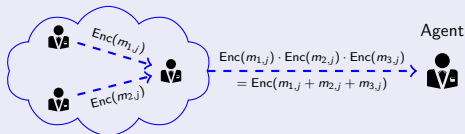




Symmetric DC-Nets (SDC-Nets)



Additive homomorphic encryption primitives (AHEPs)



Properties	SDC-Nets	AHEPs	ADC-Net
Collusion of $O(\tilde{i})$	✓	✗	
Set of trusted users	✓	✗	
Messages to the counting agent	✓	✗	
Minimum number of messages	✓	✓	
Scalable	✗	✓	
Permanent keys	✓	✓	
Based on trapdoors	✓	✓	
Keys stored per user	$2(\tilde{i} - 1)$	1	
Total of keys	$O(\tilde{i}^2)$	2	
Polynomial time	✓	✓	
One cannot disrupt	✗	✗	
Verification as commitment	✗	✗	

Properties	SDC-Nets	AHEPs	ADC-Net
Collusion of $O(\tilde{i})$	✓	✗	✓
Set of trusted users	✓	✗	✓
Messages to the counting agent	✓	✗	✓
Minimum number of messages	✓	✓	✓
Scalable	✗	✓	✓
Permanent keys	✓	✓	✓
Based on trapdoors	✓	✓	✓
Keys stored per user	$2(\tilde{i} - 1)$	1	1
Total of keys	$O(\tilde{i}^2)$	2	$O(\tilde{i})$
Polynomial time	✓	✓	✓
One cannot disrupt	✗	✗	✓
Verification as commitment	✗	✗	✓

Result:

Asymmetric DC-Nets are abstractions of Symmetric DC-Nets

[BBM14]

Result:

Asymmetric DC-Nets are abstractions of Symmetric DC-Nets

[BBM14]

Result:

AHEPs are particular cases of ADC-Nets

Result:

Asymmetric DC-Nets are abstractions of Symmetric DC-Nets

[BBM14]

Result:

AHEPs are particular cases of ADC-Nets

Example

Paillier is a particular case of an ADC-Net

Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

PPP3 - Based on Asymmetric DC-Net (ADC-Net)

PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook

Raw Dataset **X**

The raw dataset has inconsistencies

Raw Dataset ✗

The raw dataset has inconsistencies

Sanitized Dataset ✓

- ▶ 6 435 meters
- ▶ 25 726 rounds
- ▶ 165 546 810 measurements

Raw Dataset ✗





The raw dataset has inconsistencies

Sanitized Dataset ✓

- ▶ 6 435 meters
- ▶ 25 726 rounds
- ▶ 165 546 810 measurements

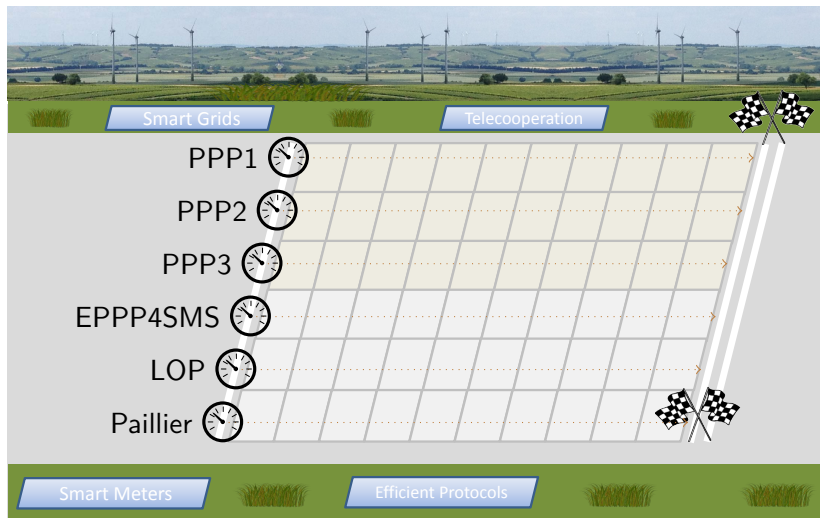
Verification

Inconsistencies ⇒ measurements collected without verification

Protocol				Efficiency 		
				Enc	Agg	Dec
PPP1	✓	✗	✗	$O(1)$	$O(\tilde{i})$	$O(\tilde{i})$
PPP2	✗	✓	✓	$O(\log(k))$	$O(\tilde{i})$	$O(k)$
PPP3	✓	✓	✓	$O(\log(k))$	$O(\tilde{i})$	$O(\log(k))$
EPPP4SMS	✓	✓	✓	$2O(\log(k))$	$O(\tilde{i})$	$O(\log(n))$
LOP - SDC-Net	✓	✗	✗	$O(\tilde{i})$	NA	$O(\tilde{i})$
Paillier - AHEP	✓	✗	✗	$O(\log(n))$	$O(\tilde{i})$	$O(\log(n))$

IEEE Trans. Smart Grid - Impact Factor: 4.334

“EPPP4SMS: Efficient Privacy-Preserving Protocol for Smart Metering Systems and Its Simulation Using Real-World Data”



Introduction

Privacy-Preserving Protocols (PPPs)

PPP1 - Based on SDC-Nets

PPP2 - Based on Commitment

PPP3 - Based on Asymmetric DC-Net (ADC-Net)

PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook

- ▶ Privacy-Preserving Protocols (PPPs) only work for large aggregations

- ▶ PPPs only work for large aggregations
- ▶ PPP1 has the fastest Enc ($m_{i,j}$)

- ▶ PPPs only work for large aggregations
- ▶ PPP1 has the fastest Enc ($m_{i,j}$)
- ▶ **PPP2 and PPP3 are exponentially faster than others**

- ▶ PPPs only work for large aggregations
- ▶ PPP1 has the fastest Enc ($m_{i,j}$)
- ▶ PPP2 and PPP3 are exponentially faster than others
- ▶ **PPP4 is resistant against quantum attacks**

- ▶ PPPs only work for large aggregations
- ▶ PPP1 has the fastest Enc ($m_{i,j}$)
- ▶ PPP2 and PPP3 are exponentially faster than others
- ▶ PPP4 is resistant against quantum attacks
- ▶ **The concept of ADC-Nets is introduced**

- [BM14b] [Fábio Borges and Max Mühlhäuser](#). EPPP4SMS: efficient privacy-preserving protocol for smart metering systems and its simulation using real-world data. *IEEE trans. smart grid*, 5(6):2701–2708, 2014
- Impact Factor 4.334
h5-index 54
- [BSM14] [Fábio Borges, Raqueline A. M. Santos, and Franklin L. Marquezino](#). Preserving privacy in a smart grid scenario using quantum mechanics. *Security and communication networks:n/a–n/a*, 2014
- Impact Factor 0.433
h5-index 19
- [LBPN12] [Pedro Lara, Fábio Borges, Renato Portugal, and Nadia Nedjah](#). Parallel modular exponentiation using load balancing without precomputation. *Journal of computer and system sciences*, 78(2):575–582, 2012
- Impact Factor 1.091
h5-index 30

- [BBM14] Fábio Borges, Johannes Buchmann, and Max Mühlhäuser. Introducing asymmetric dc-nets. In *Communications and network security (CNS), 2014 IEEE conference on*, 2014, pages 508–509

Best Poster Award - IEEE Communications Society

- [BBM14] Fábio Borges, Johannes Buchmann, and Max Mühlhäuser. Introducing asymmetric dc-nets. In *Communications and network security (CNS), 2014 IEEE conference on*, 2014, pages 508–509
- [BM14a] Fábio Borges and Leonardo A. Martucci. iKUP keeps users' privacy in the smart grid. In *Communications and network security (CNS), 2014 IEEE conference on*, 2014, pages 310–318
- [BDBBM14] Fábio Borges, Denise Demirel, Leon Böck, Johannes Buchmann, and Max Mühlhäuser. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In *Computers and communication (ISCC), 2014 IEEE symposium on*, 2014, pages 1–6
- [BMBM14] Fábio Borges, Leonardo A. Martucci, Filipe Beato, and Max Mühlhäuser. Secure and privacy-friendly public key generation and certification. In *Trust, security and privacy in computing and communications (TrustCom), 2014 IEEE 13th international conference on*, 2014, pages 114–121
- [BMM12] Fábio Borges, Leonardo A. Martucci, and Max Mühlhäuser. Analysis of privacy-enhancing protocols based on anonymity networks. In *Smart grid communications (SmartGridComm), 2012 IEEE third international conference on*, 2012, pages 378–383
- [BPP12] Fábio Borges, Albrecht Petzoldt, and Renato Portugal. Small private keys for systems of multivariate quadratic equations using symmetric cryptography. In *XXXIV CNMAC - congresso nacional de matemática aplicada e computacional. Águas de Lindóia - SP*, 2012, pages 1085–1091
- [BVM15] Fábio Borges, Florian Volk, and Max Mühlhäuser. Efficient, verifiable, secure, and privacy-friendly computations for the smart grid. In *Innovative smart grid technologies conference (ISGT), 2015 IEEE power energy society*, 2015, pages 1–5

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ **electronic voting**

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems
 - ▶ **sensor networks**

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems
 - ▶ sensor networks
 - ▶ **electronic money**

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems
 - ▶ sensor networks
 - ▶ electronic money
 - ▶ **mobile sensing**

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems
 - ▶ sensor networks
 - ▶ electronic money
 - ▶ mobile sensing
 - ▶ multi-party computation

ADC-Nets can be used in applications that require:

- ▶ SDC-Nets
- ▶ AHEPs
 - ▶ electronic voting
 - ▶ reputation systems
 - ▶ sensor networks
 - ▶ electronic money
 - ▶ mobile sensing
 - ▶ multi-party computation
 - ▶ **image processing**



All comments and suggestions are welcomed.
Contact: borges@lncc.de

1. Detection of profile in protocols based on noise
2. Reasons for frequent measurements
 - ▶ Detection of fraud and energy loss
 - ▶ Virtualization of a commodity network
 - ▶ Fair Distribution (challenge)
3. Minimal requirements for PPPs
4. Limitations for all PPPs
 - ▶ Algebraic properties
 - ▶ Probabilistic properties
5. The concept of ADC-Nets
 - ▶ Abstractions of SDC-Nets
 - ▶ Generalization of AHEPs
6. Four new PPPs
 - ▶ PPP1 is the fastest
 - ▶ PPP2 uses commitment with elliptic curve
 - ▶ PPP3 is an ADC-Net
 - ▶ PPP4 is resistant against quantum attacks
7. An SDC-Net that behaves as AHEPs
8. Detection of inconsistencies in the dataset
9. Theoretical analysis validated with simulation



Fábio Borges, Johannes Buchmann, and Max Mühlhäuser. Introducing asymmetric dc-nets. In *Communications and network security (CNS), 2014 IEEE conference on*, 2014, pages 508–509.



Fábio Borges, Denise Demirel, Leon Böck, Johannes Buchmann, and Max Mühlhäuser. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In *Computers and communication (ISCC), 2014 IEEE symposium on*, 2014, pages 1–6.



Fábio Borges and Leonardo A. Martucci. iKUP keeps users' privacy in the smart grid. In *Communications and network security (CNS), 2014 IEEE conference on*, 2014, pages 310–318.



Fábio Borges and Max Mühlhäuser. EPPP4SMS: efficient privacy-preserving protocol for smart metering systems and its simulation using real-world data. *IEEE trans. smart grid*, 5(6):2701–2708, 2014.



Fábio Borges, Leonardo A. Martucci, Filipe Beato, and Max Mühlhäuser. Secure and privacy-friendly public key generation and certification. In *Trust, security and privacy in computing and communications (TrustCom), 2014 IEEE 13th international conference on*, 2014, pages 114–121.



Fábio Borges, Leonardo A. Martucci, and Max Mühlhäuser. Analysis of privacy-enhancing protocols based on anonymity networks. In *Smart grid communications (SmartGridComm), 2012 IEEE third international conference on*, 2012, pages 378–383.



Fábio Borges, Albrecht Petzoldt, and Renato Portugal. Small private keys for systems of multivariate quadratic equations using symmetric cryptography. In *XXXIV CNMAC - congrasso nacional de matemática aplicada e computacional. Águas de Lindóia - SP*, 2012, pages 1085–1091.



Fábio Borges, Raqueline A. M. Santos, and Franklin L. Marquezino. Preserving privacy in a smart grid scenario using quantum mechanics. *Security and communication networks:n/a–n/a*, 2014.



Fábio Borges, Florian Volk, and Max Mühlhäuser. Efficient, verifiable, secure, and privacy-friendly computations for the smart grid. In *Innovative smart grid technologies conference (ISGT), 2015 IEEE power energy society*, 2015, pages 1–5.



D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *J. cryptol.*, 1(1):65–75, March 1988.



Philippe Golle and Ari Juels. Dining cryptographers revisited. English. In Christian Cachin and JanL. Camenisch, editors, *Advances in cryptology - eurocrypt 2004*. Volume 3027, in Lecture Notes in Computer Science, pages 456–473. Springer Berlin Heidelberg, 2004.



Ulrich Greveler, Benjamin Justus, and Dennis Löhr. Identifikation von videoinhalten über granulare stromverbrauchsdaten. In *Sicherheit*. Neeraj Suri and Michael Waidner, editors. Volume 195. In LNI. GI, 2012, pages 35–45.



Pedro Lara, Fábio Borges, Renato Portugal, and Nadia Nedjah.
Parallel modular exponentiation using load balancing without
precomputation. *Journal of computer and system sciences*,
78(2):575–582, 2012.