On Privacy-Preserving Protocols for Smart Metering Systems

UFRJ/COPPE

Fábio Borges

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

Table of Contents

Outline

Security

Introduction to PPP

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

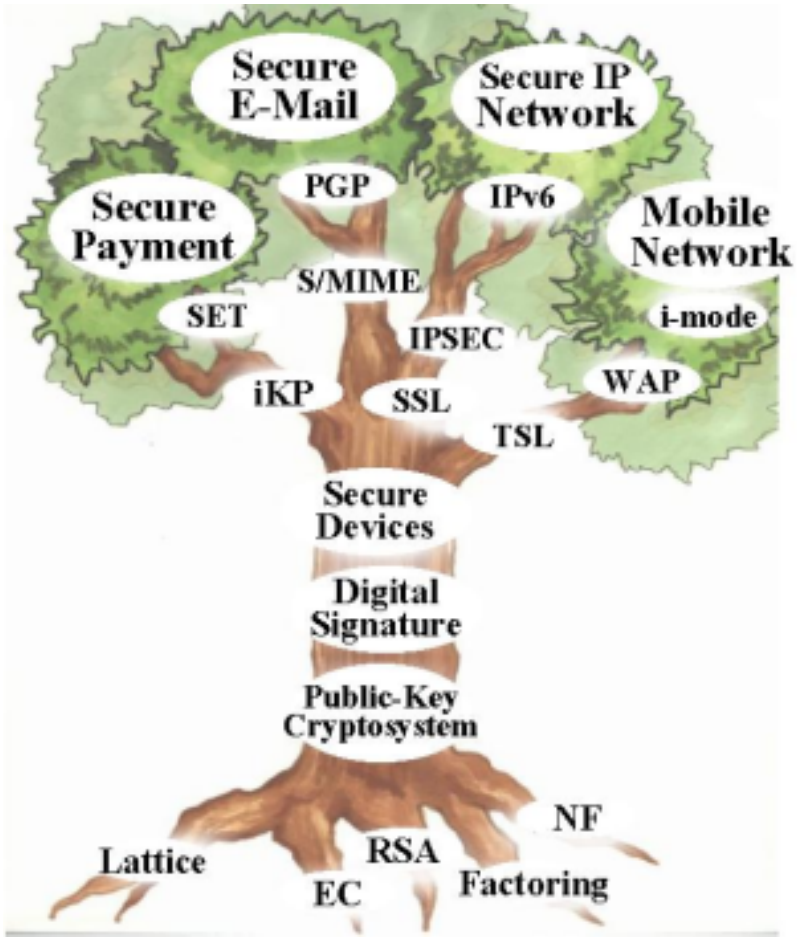
ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook

Security Tree

from bottom to top



Areas

Big Areas

- Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption
    - DC-Nets

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption
    - DC-Nets
    - ADC-Nets

Alert

Applications? Differences?

CSR
LNCC

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security

Introduction to PPP

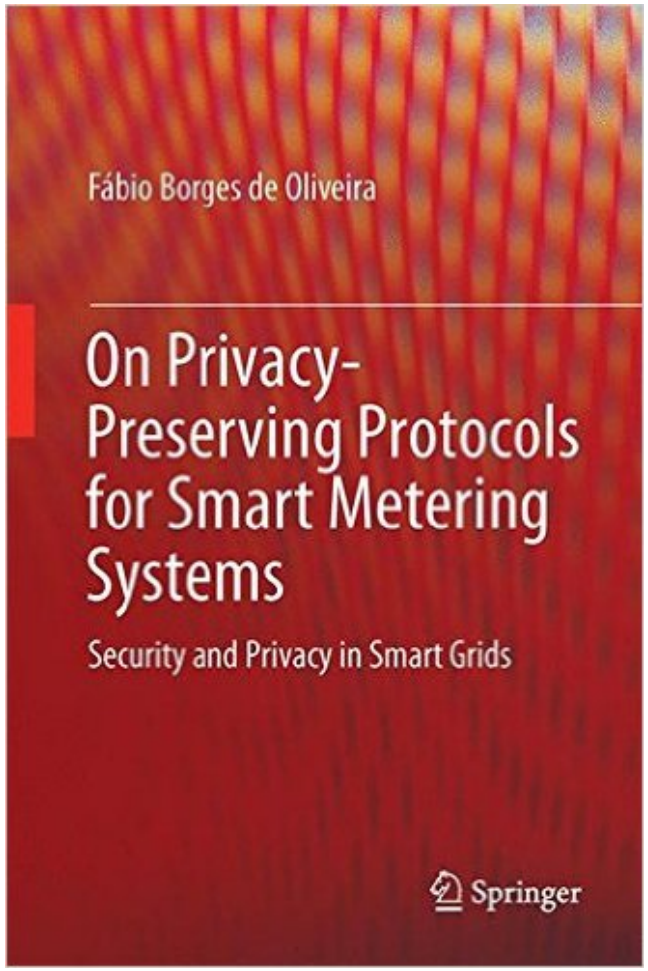
Privacy-Preserving Protocols (PPPs)
- PPP1 - Based on SDC-Nets
- PPP2 - Based on Commitment
- PPP3 - Based on Asymmetric DC-Net (ADC-Net)
- PPP4 - Based on Quantum Cryptography

ADC-Nets

Simulation Using Real-World Data

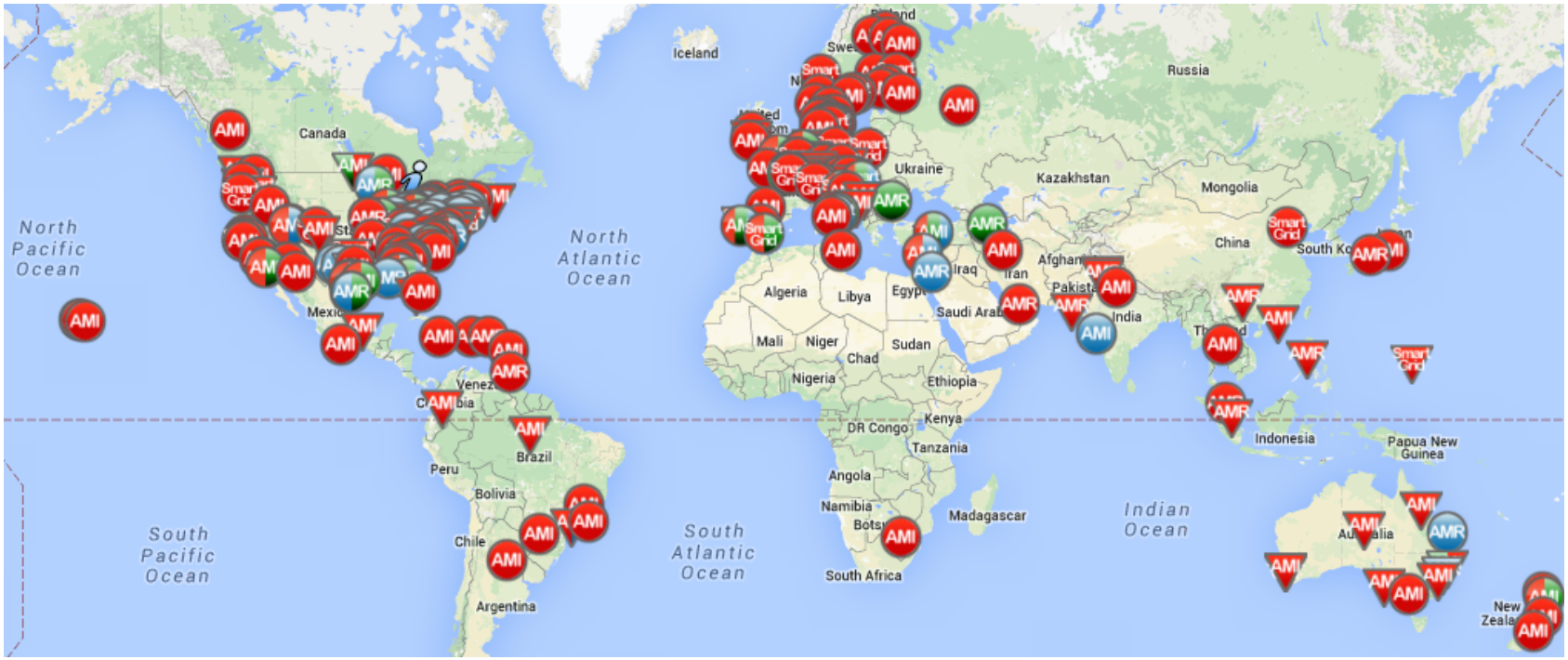
Conclusion and Outlook

Book

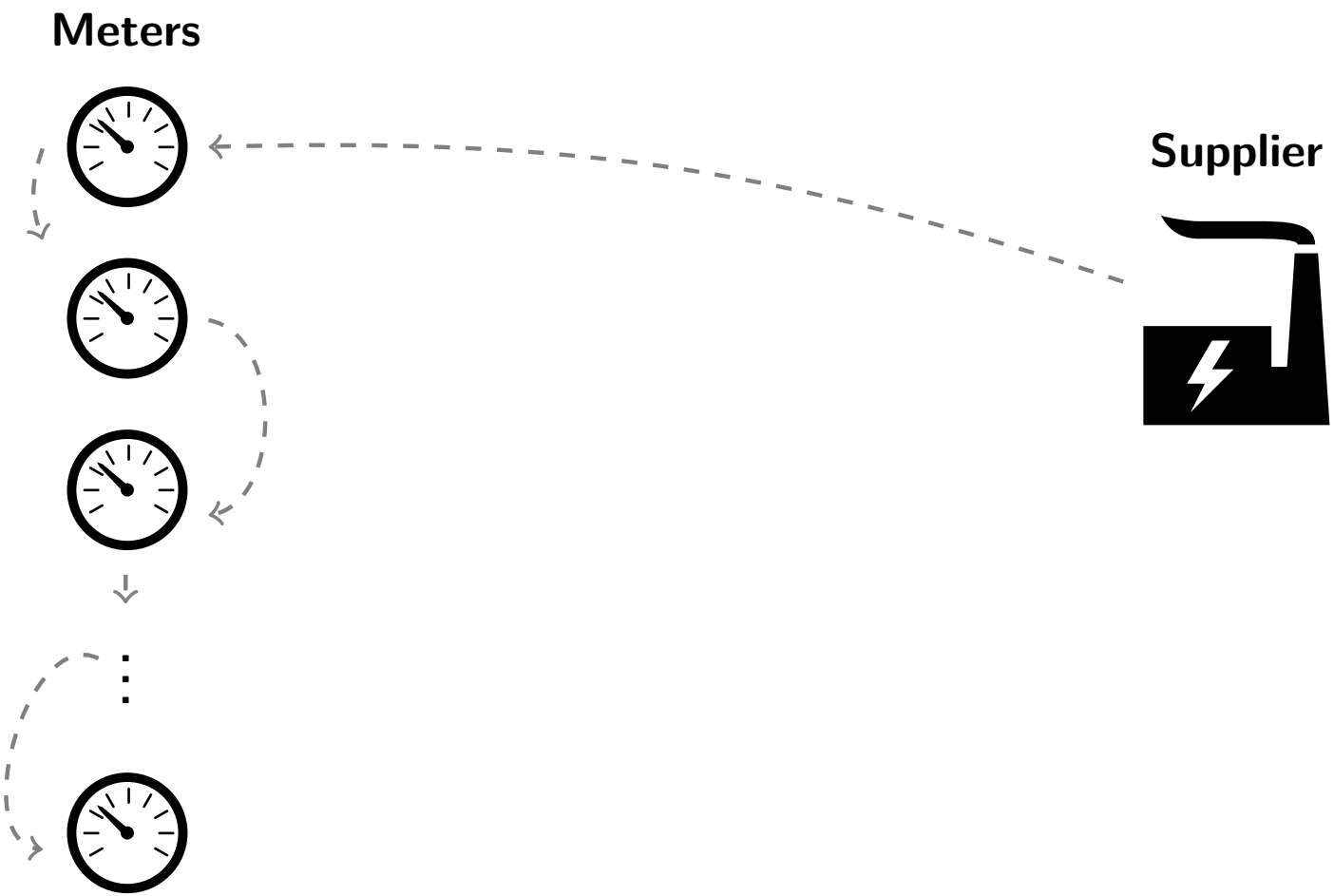

Fábio Borges de Oliveira
On Privacy-Preserving Protocols for Smart Metering Systems
Security and Privacy in Smart Grids
Springer

Smart Metering Projects Map

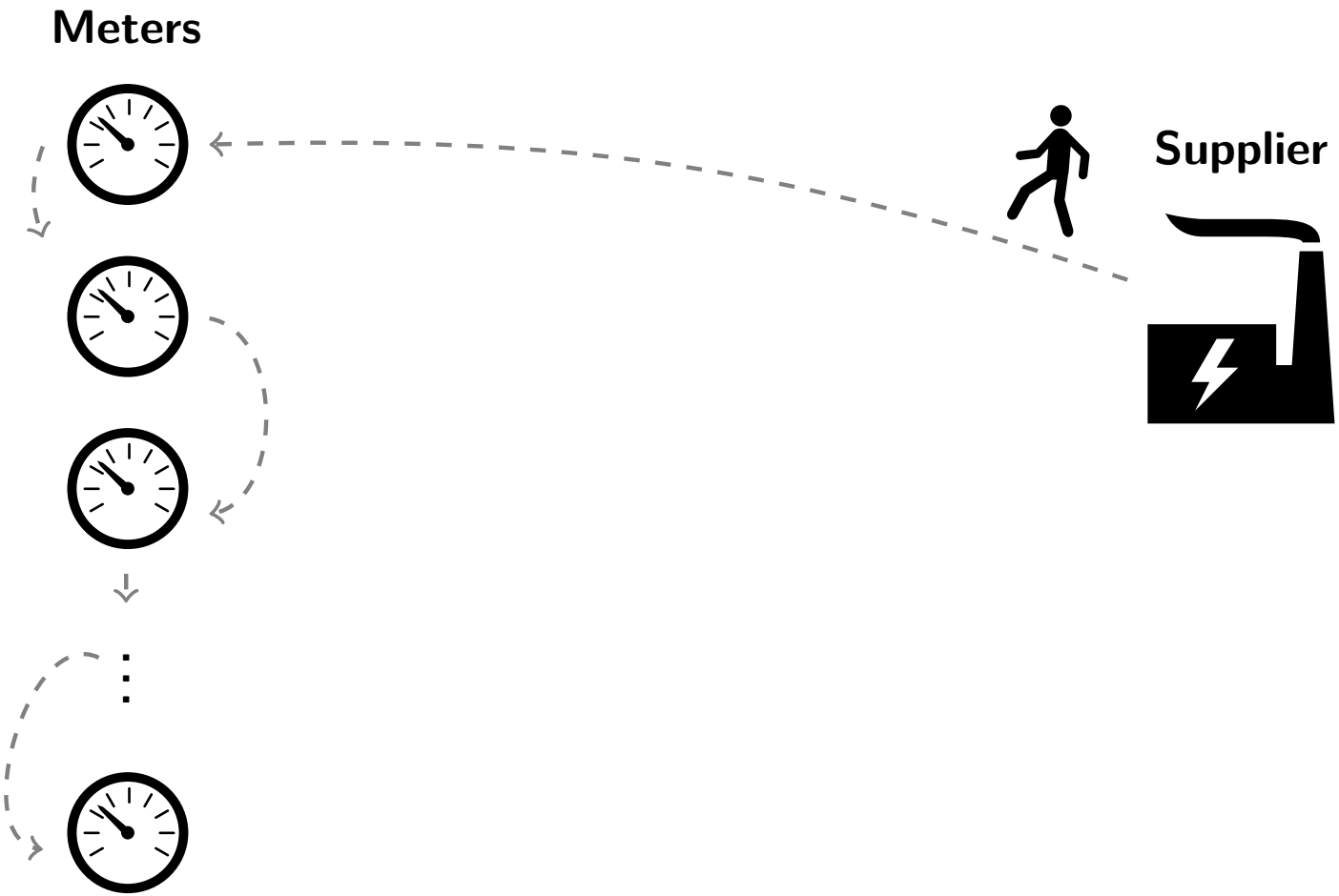
Google Maps



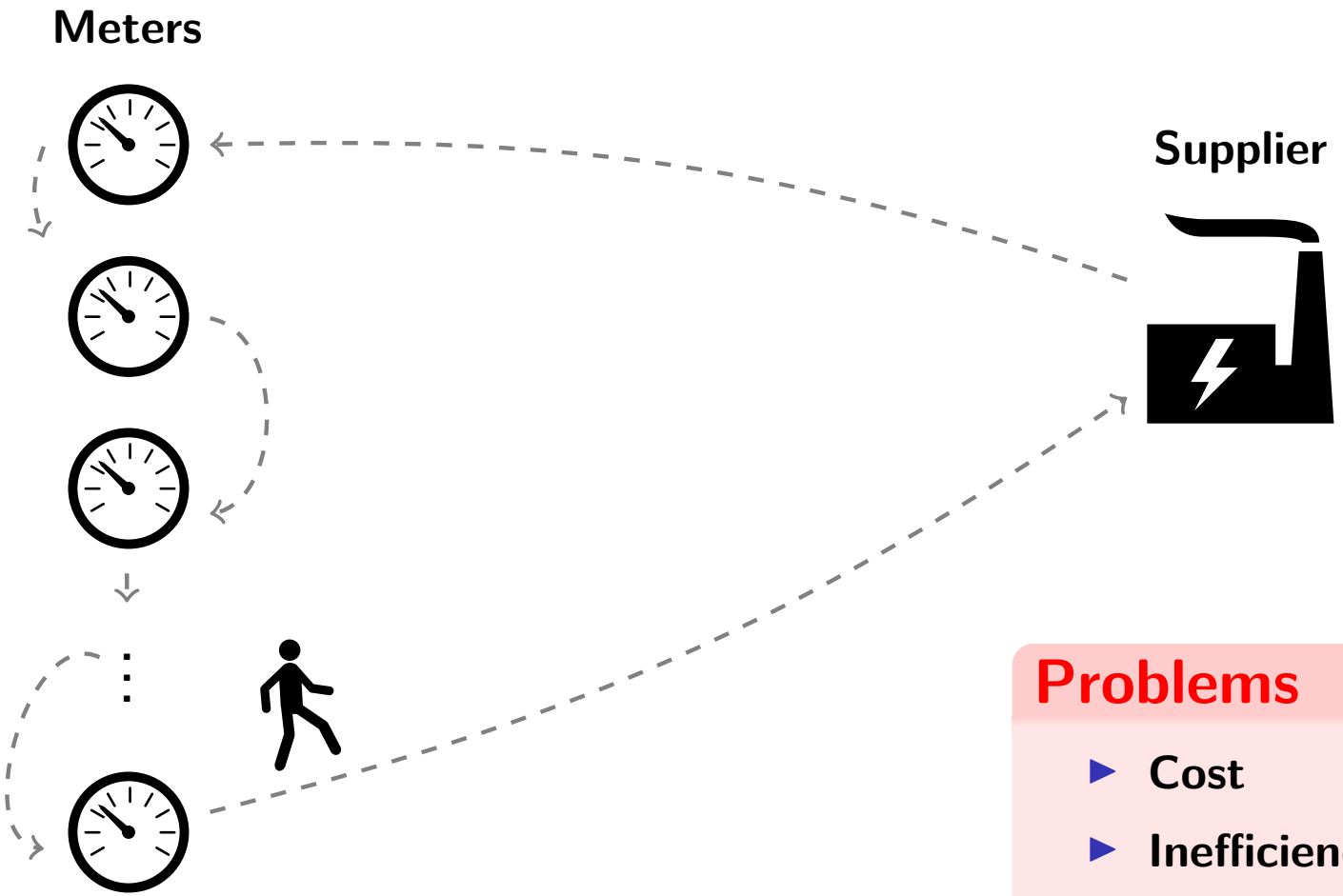
Non-smart Grid



Non-smart Grid



Non-smart Grid

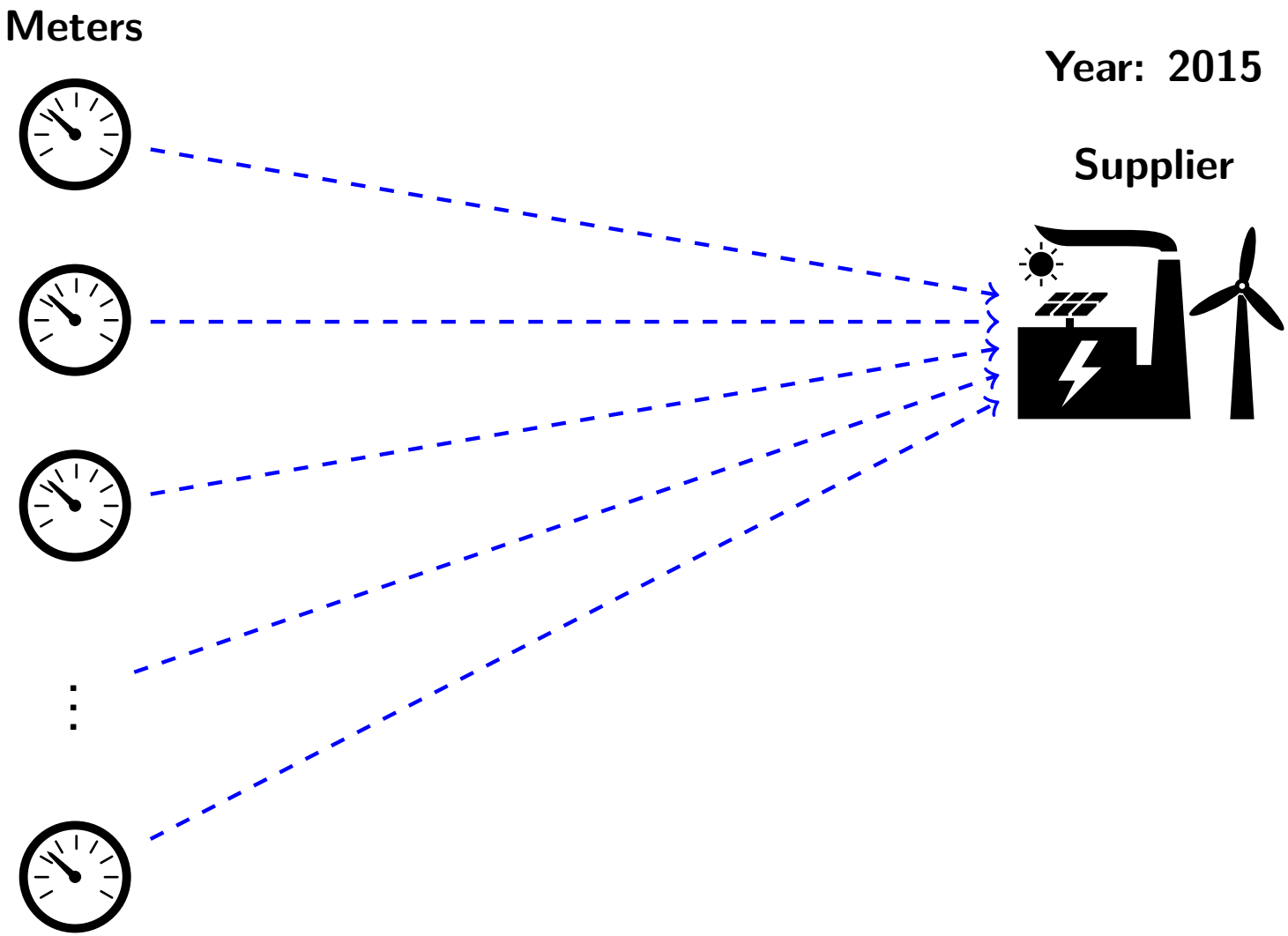


Problems

- Cost
- Inefficiency
- Fraud

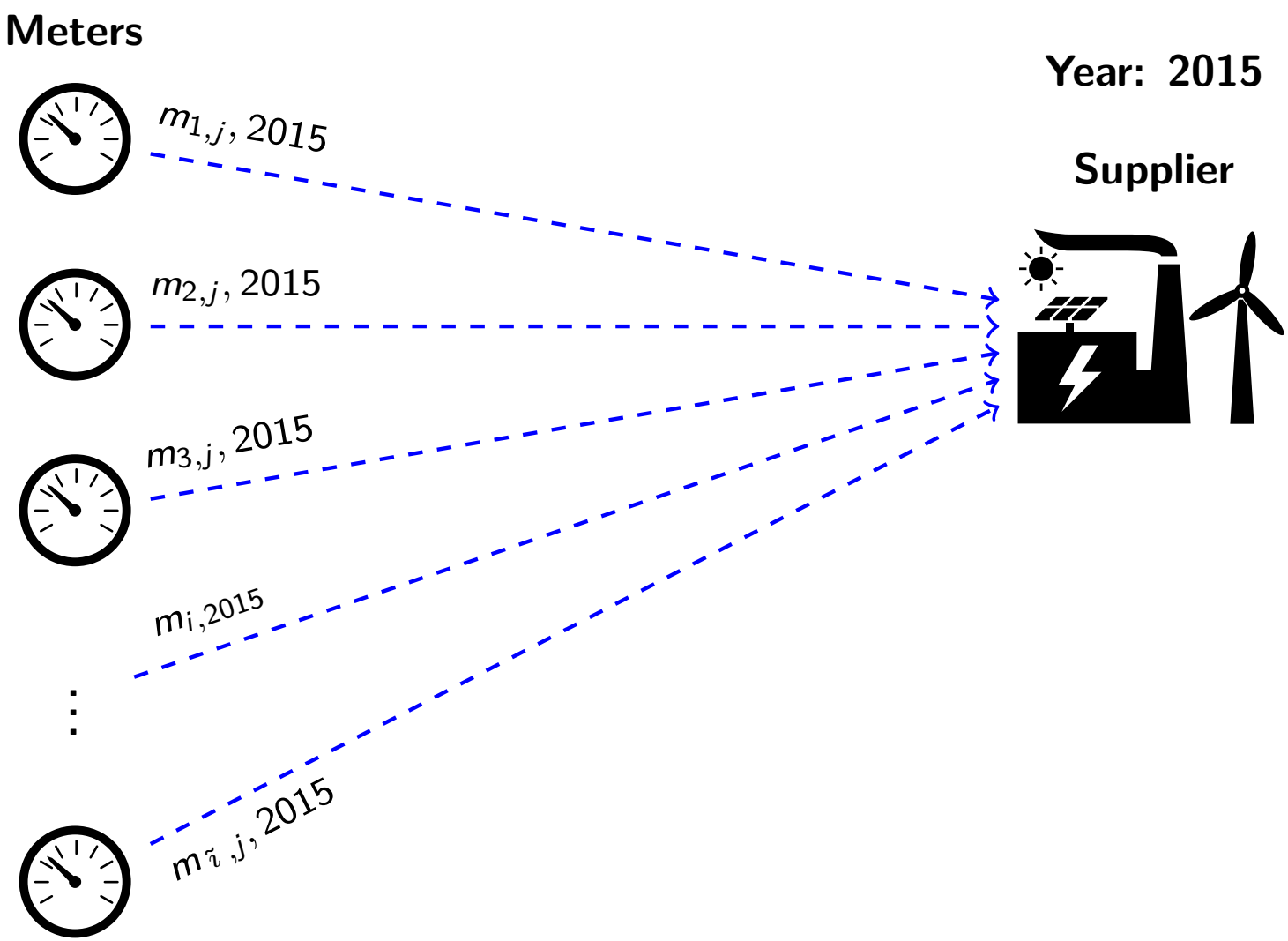
Getting Smart

Collecting on a yearly basis



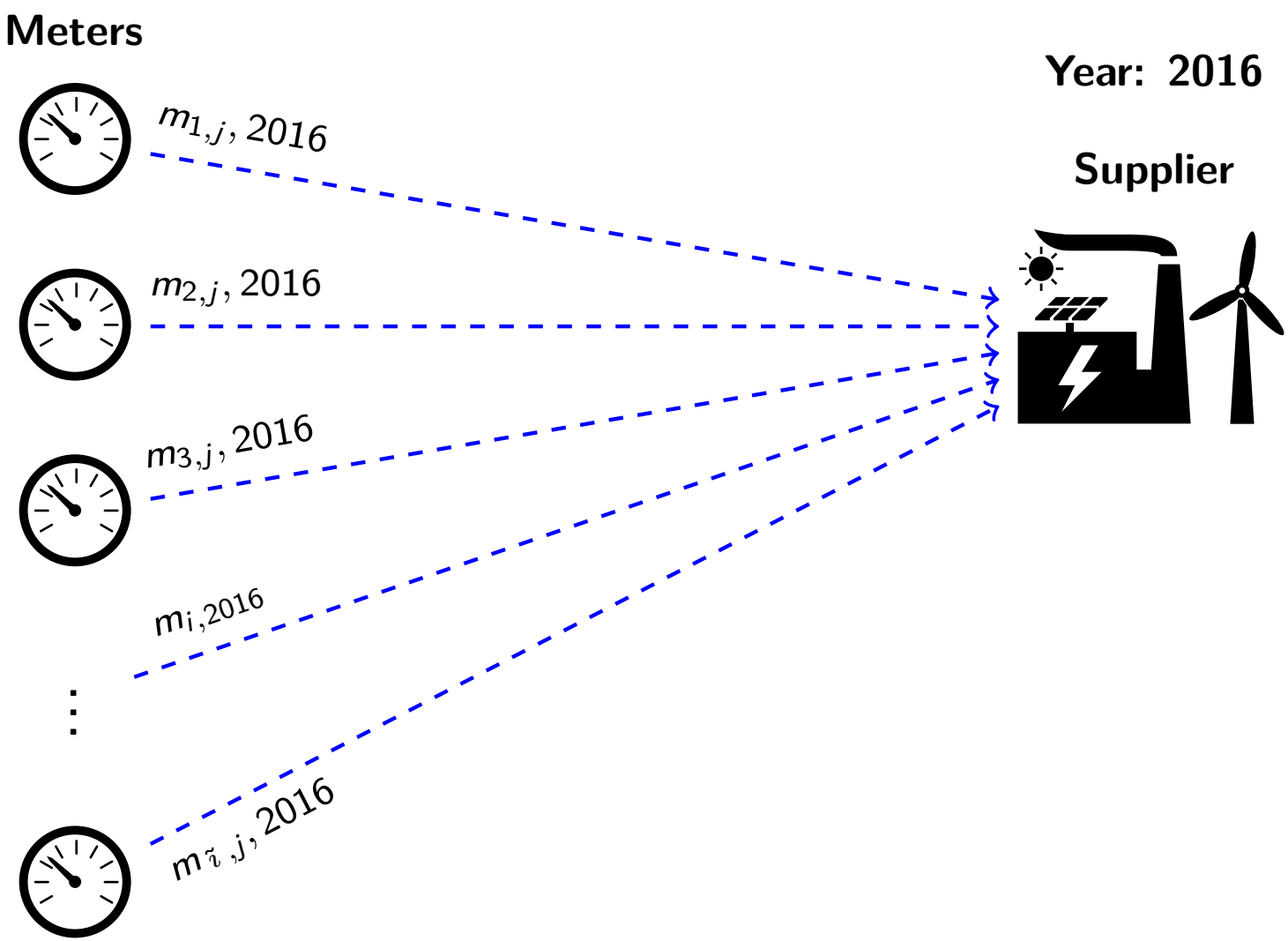
Getting Smart

Collecting on a yearly basis



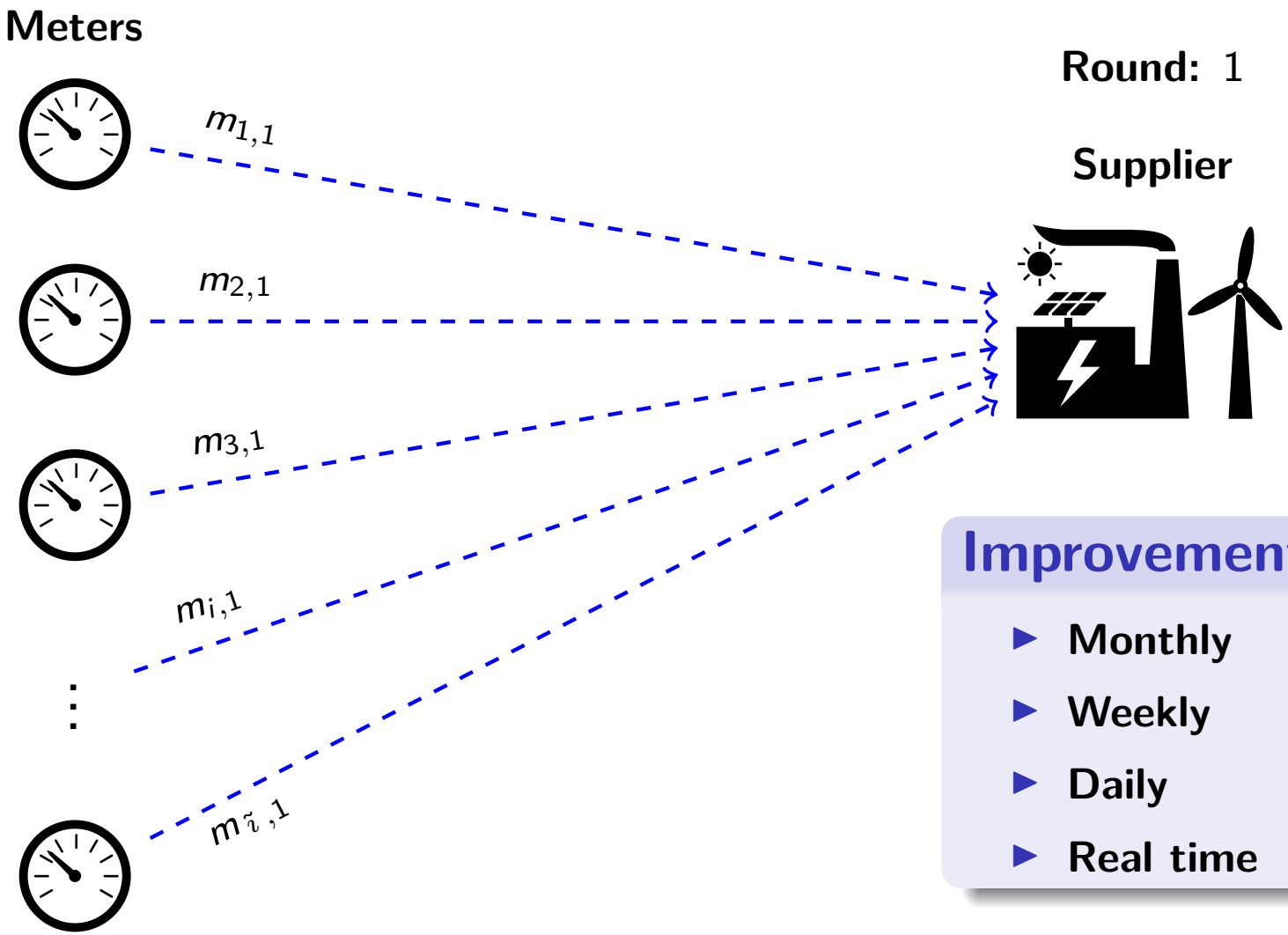
Getting Smart

Collecting on a yearly basis



Getting Smart

Collecting per round

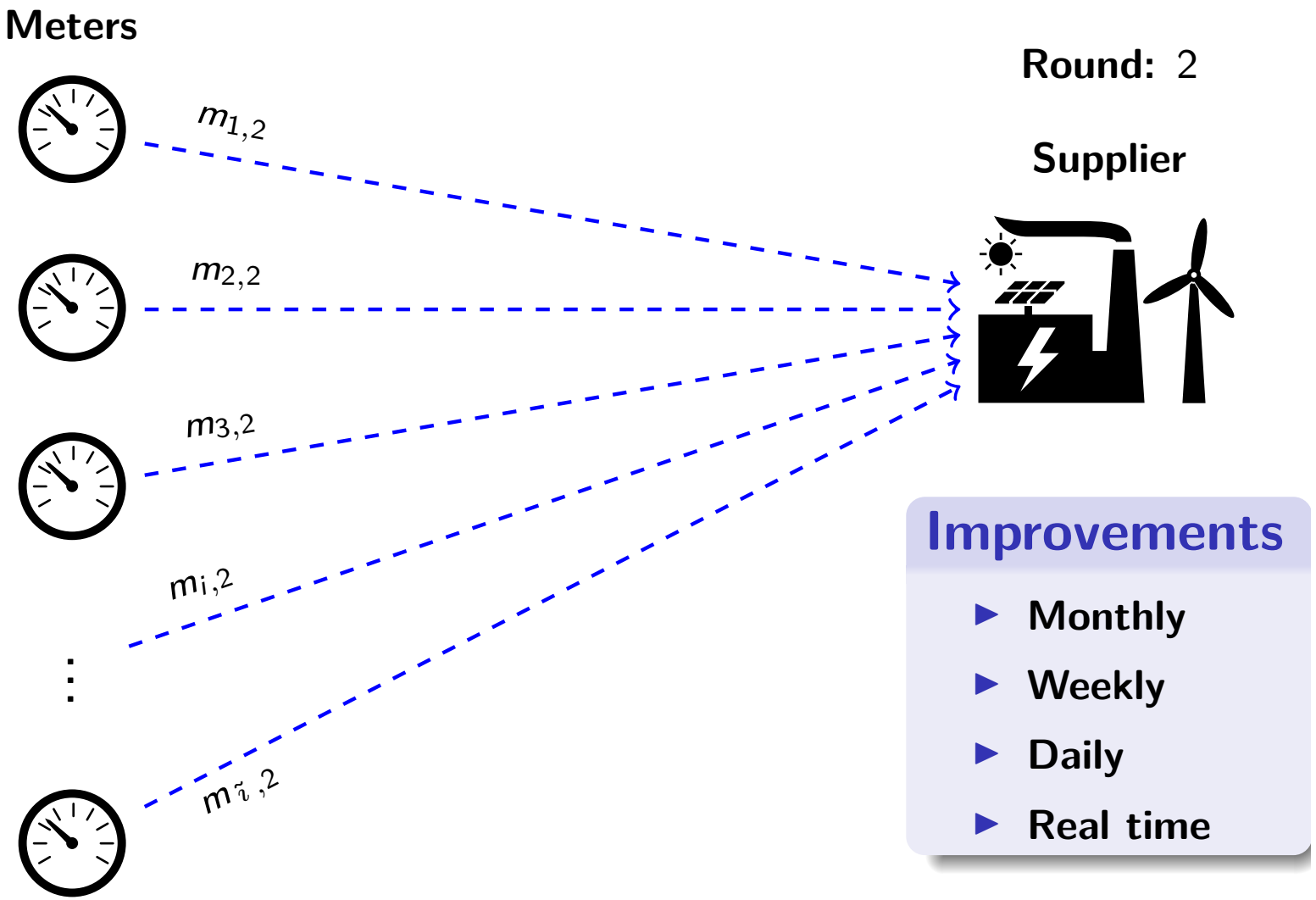


Improvements

- Monthly
- Weekly
- Daily
- Real time

Getting Smart

Collecting per round

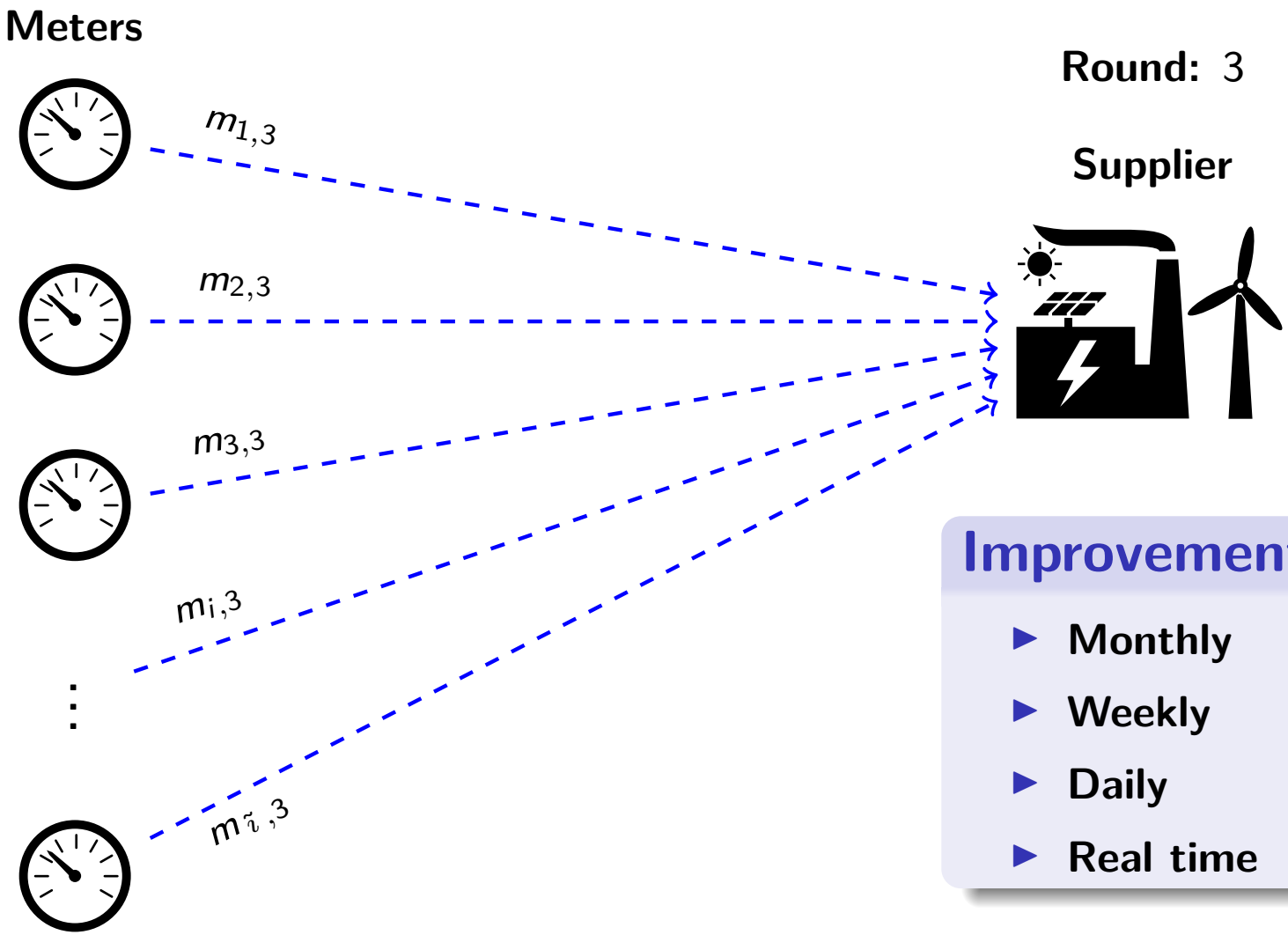


Improvements

- Monthly
- Weekly
- Daily
- Real time

Getting Smart

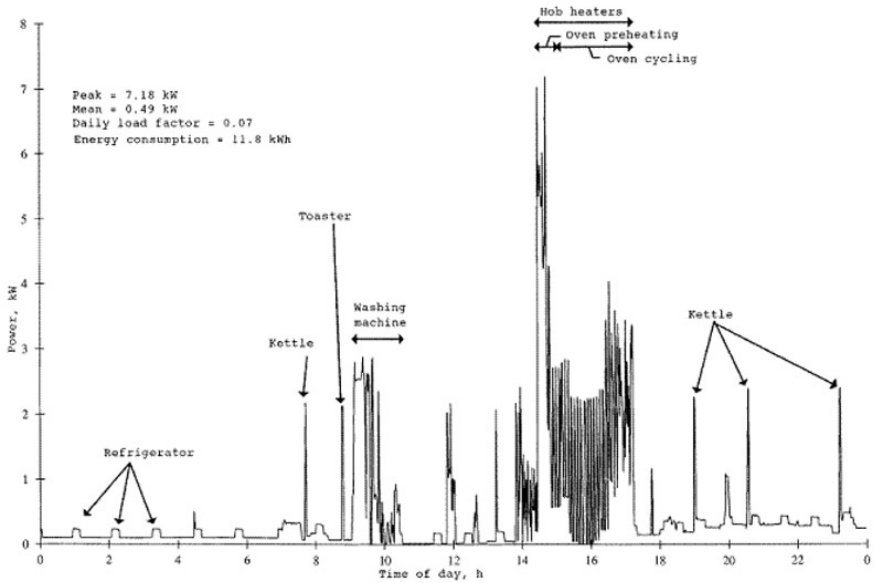
Collecting per round



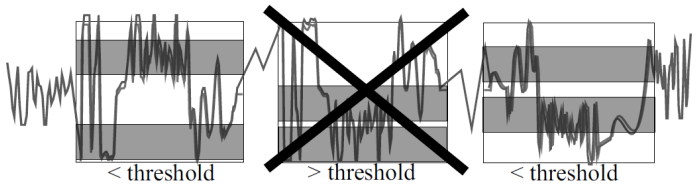
Improvements

- Monthly
- Weekly
- Daily
- Real time

Privacy Problem



[NIST]



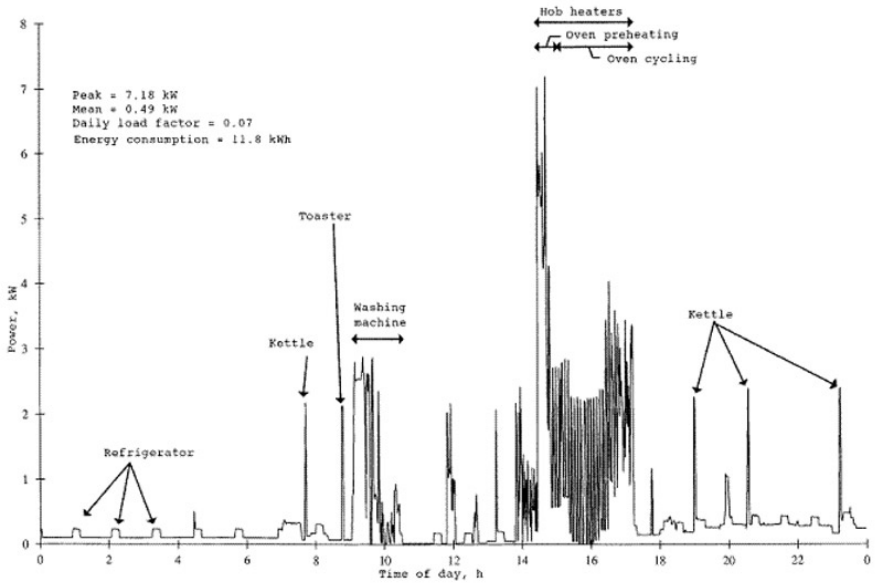
output matches to logfile

movie tng1
chunk 1 at 2103h

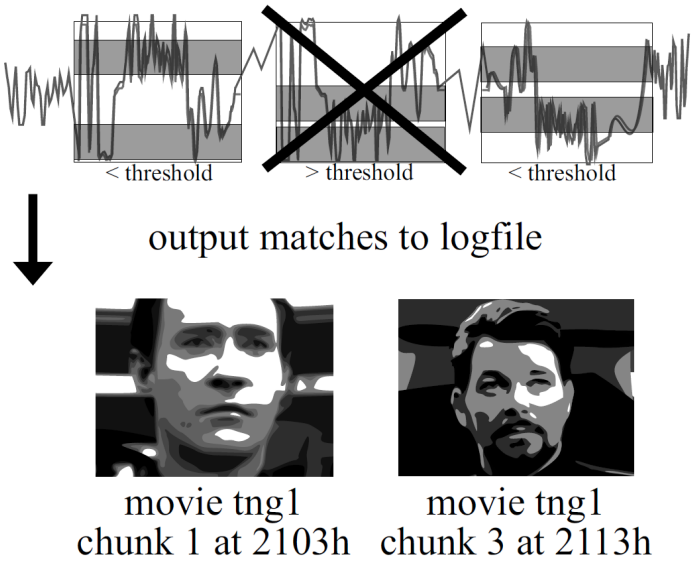
movie tng1
chunk 3 at 2113h

[GJL12]

Privacy Problem



[NIST]



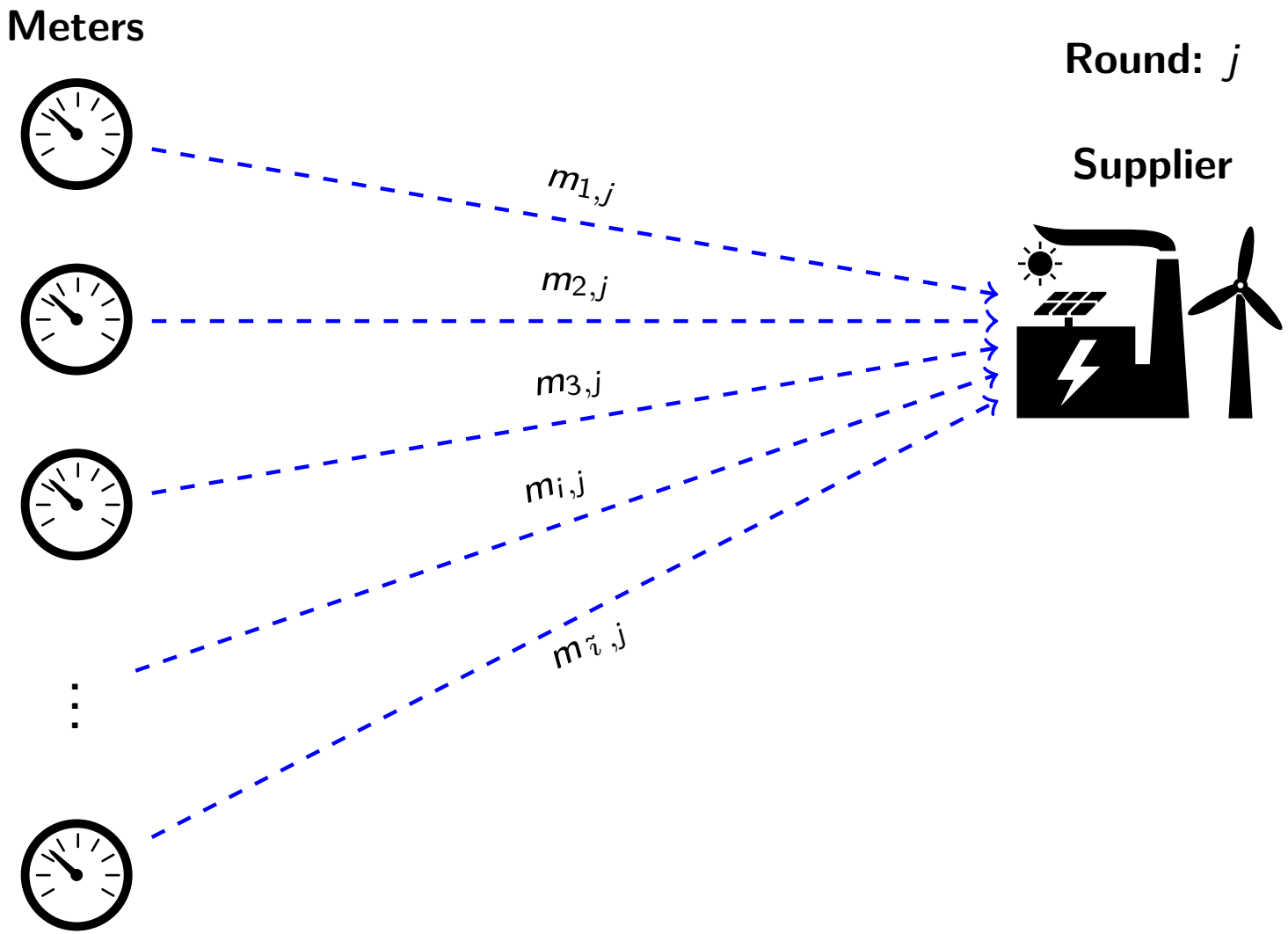
[GJL12]

EU - Official Journal L No.315

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

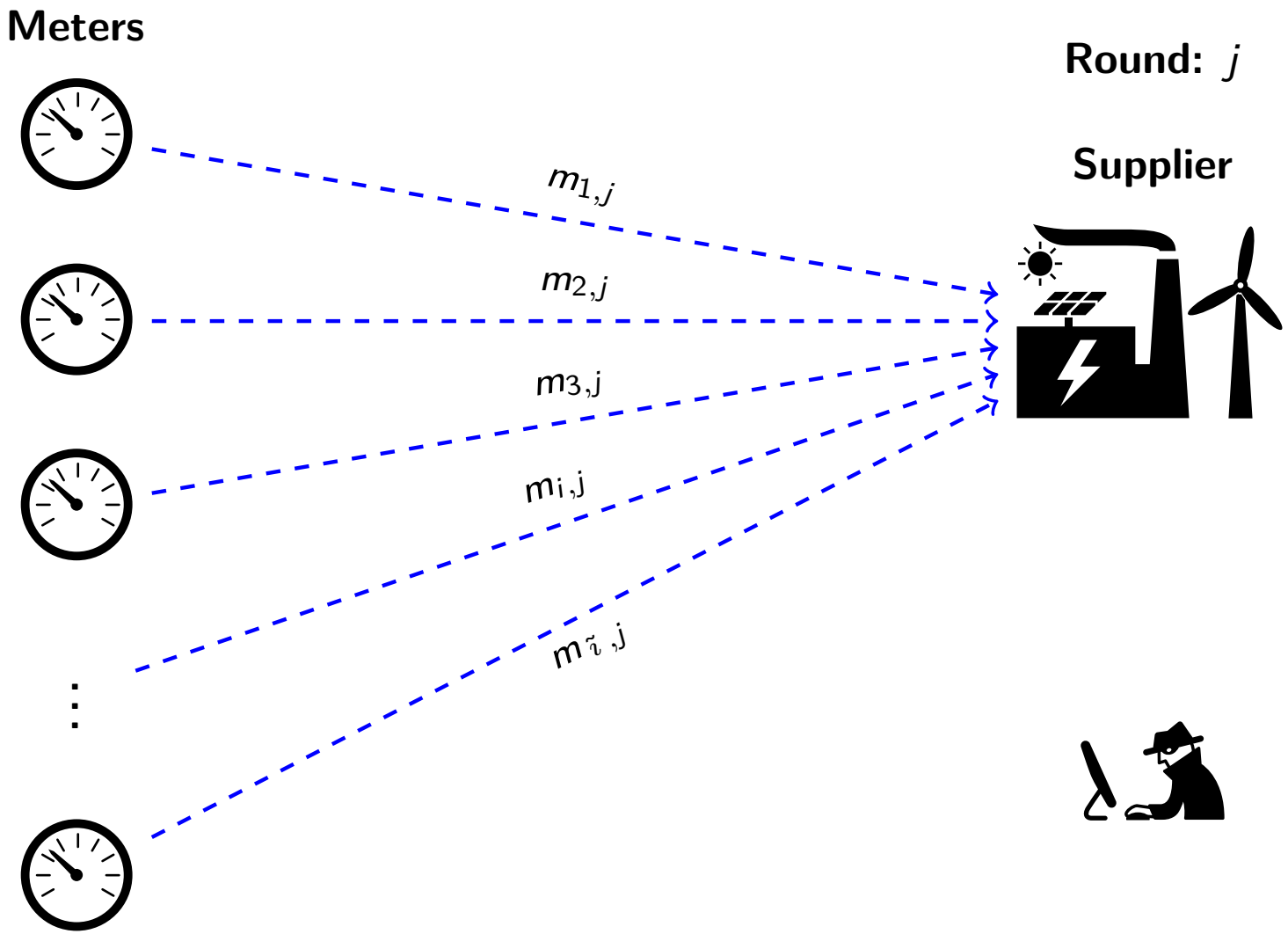
Need for Encryption

Intercepting all measurements per round



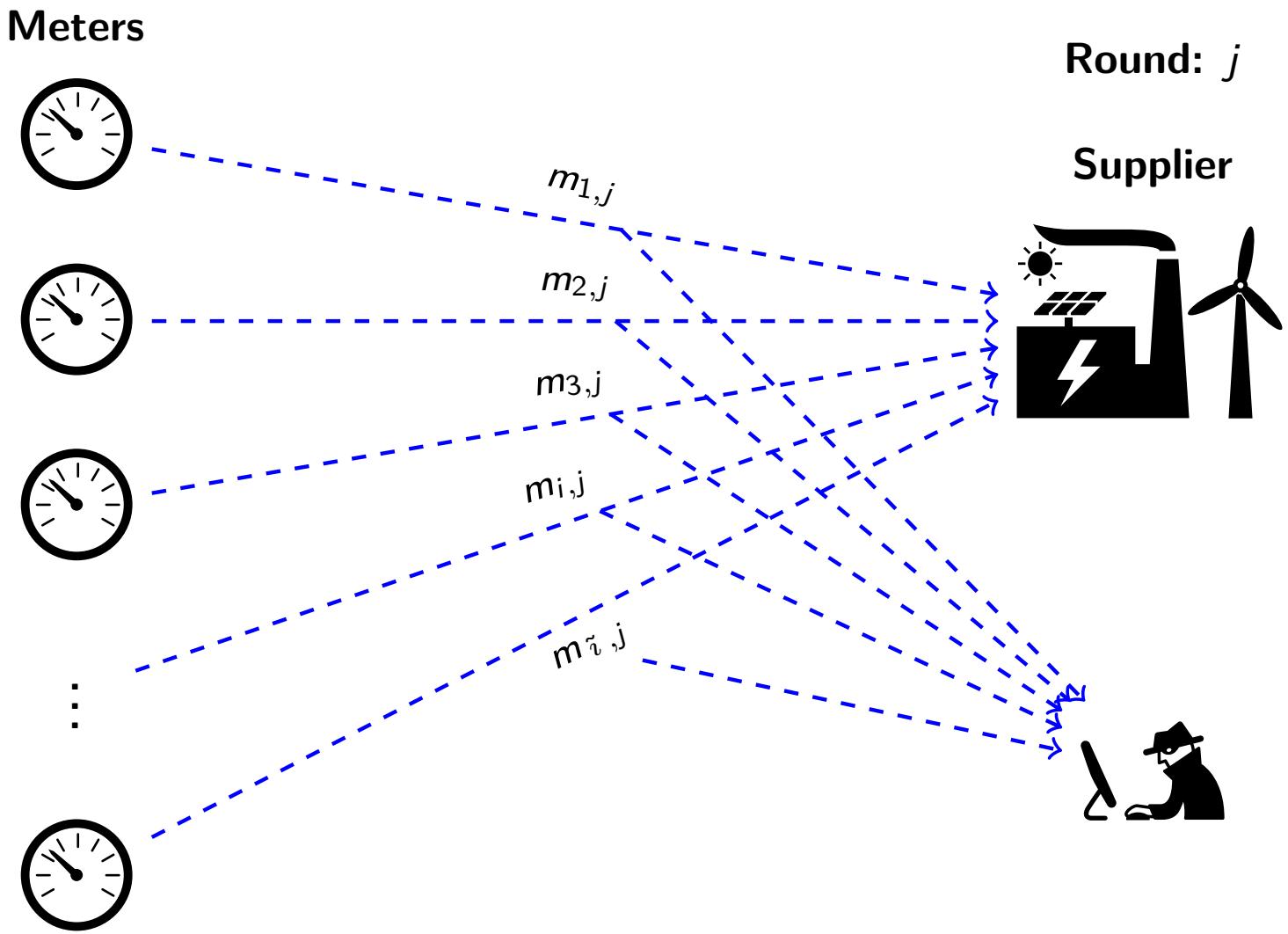
Need for Encryption

Intercepting all measurements per round

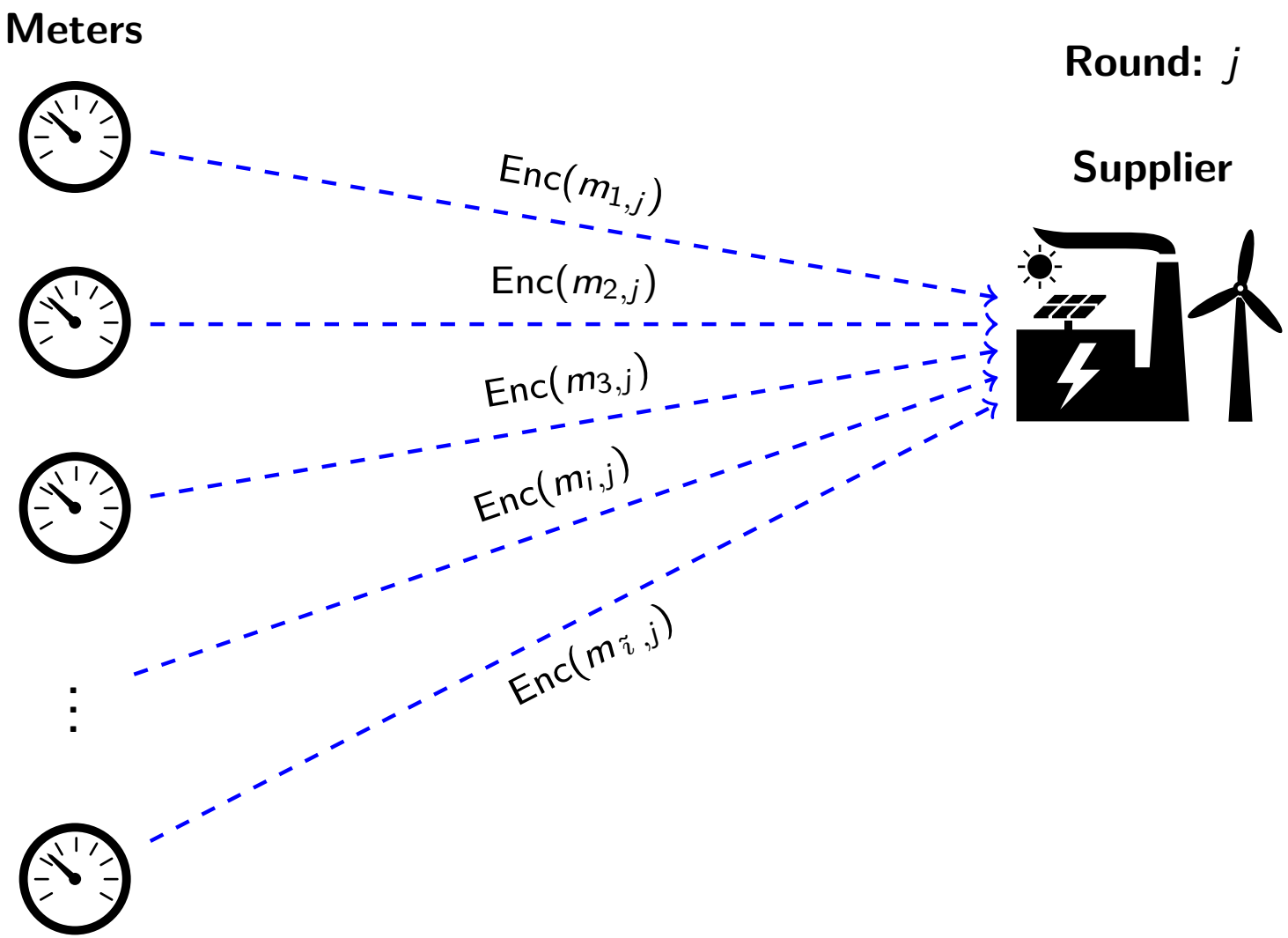


Need for Encryption

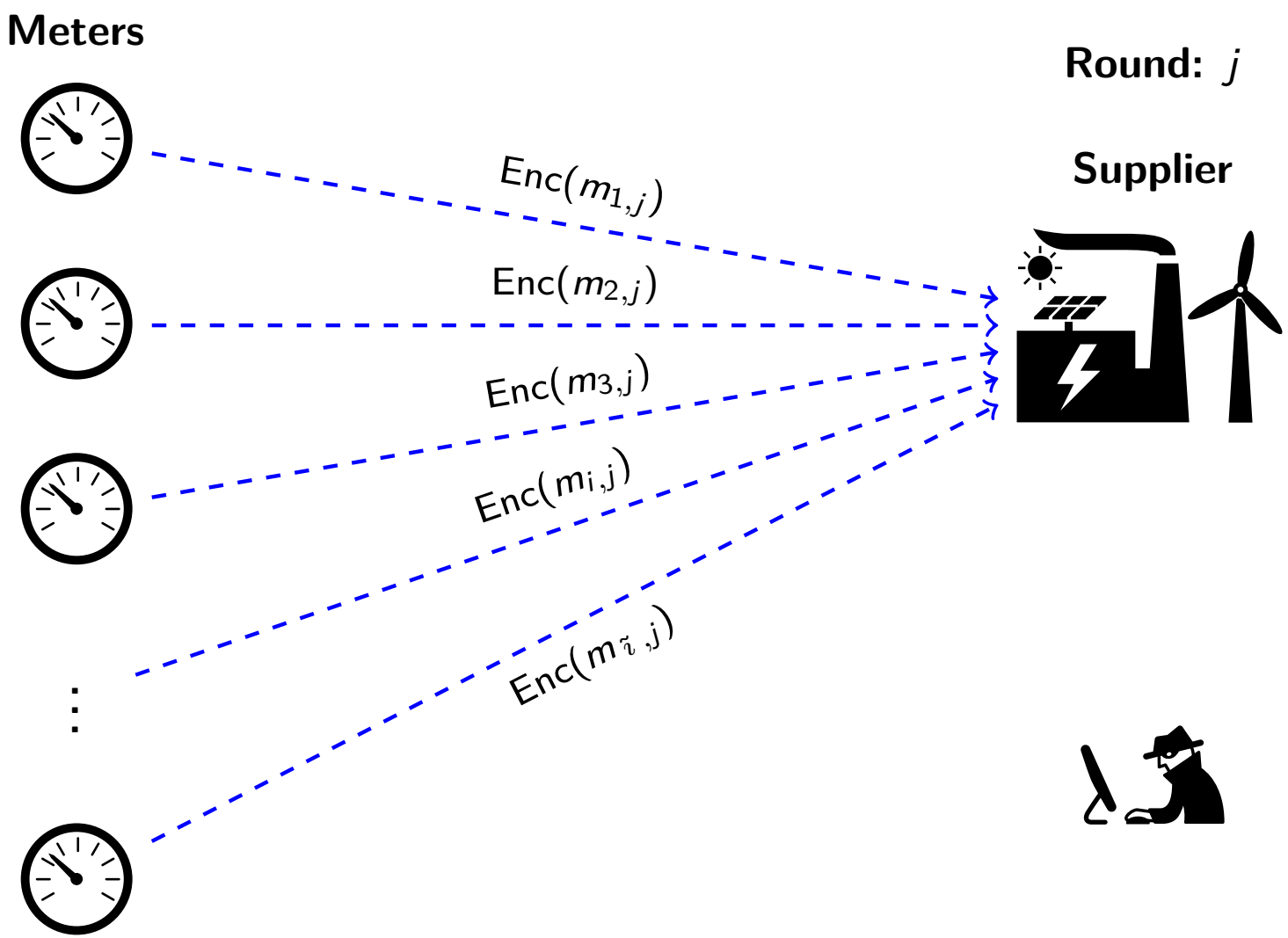
Intercepting all measurements per round



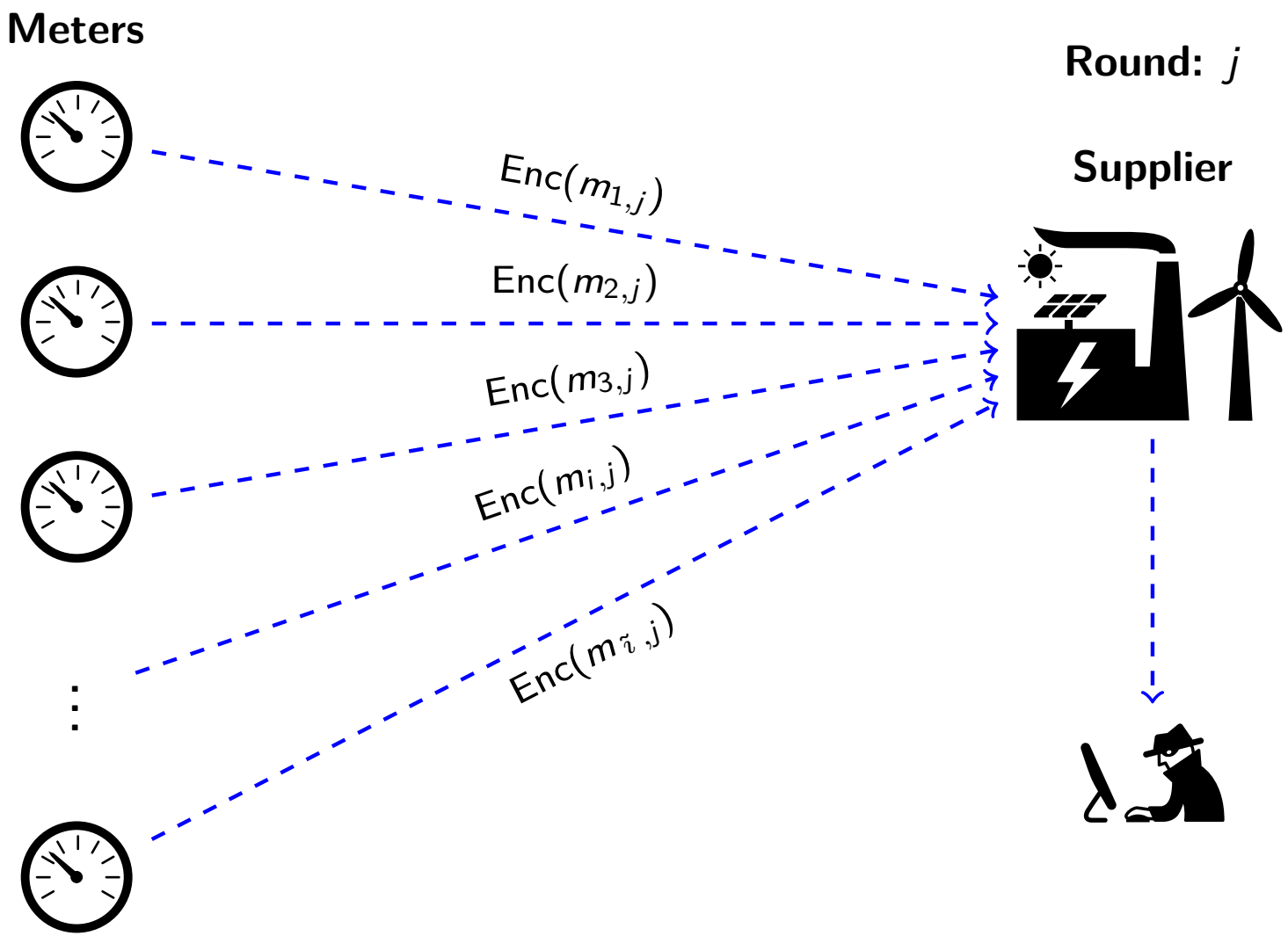
Need for Aggregation



Need for Aggregation



Need for Aggregation



What Does the Supplier Need?

Consolidated Consumption versus Billing

Round	1	2	$\cdots$	$\tilde{j}$	**Billing**
Meter 1	$m_{1,1}$	$m_{1,2}$	$\cdots$	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$	$\cdots$	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Meter $\tilde{i}$	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$	$\cdots$	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidated	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$	$\cdots$	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	$=$

What Does the Supplier Need?

Consolidated Consumption versus Billing

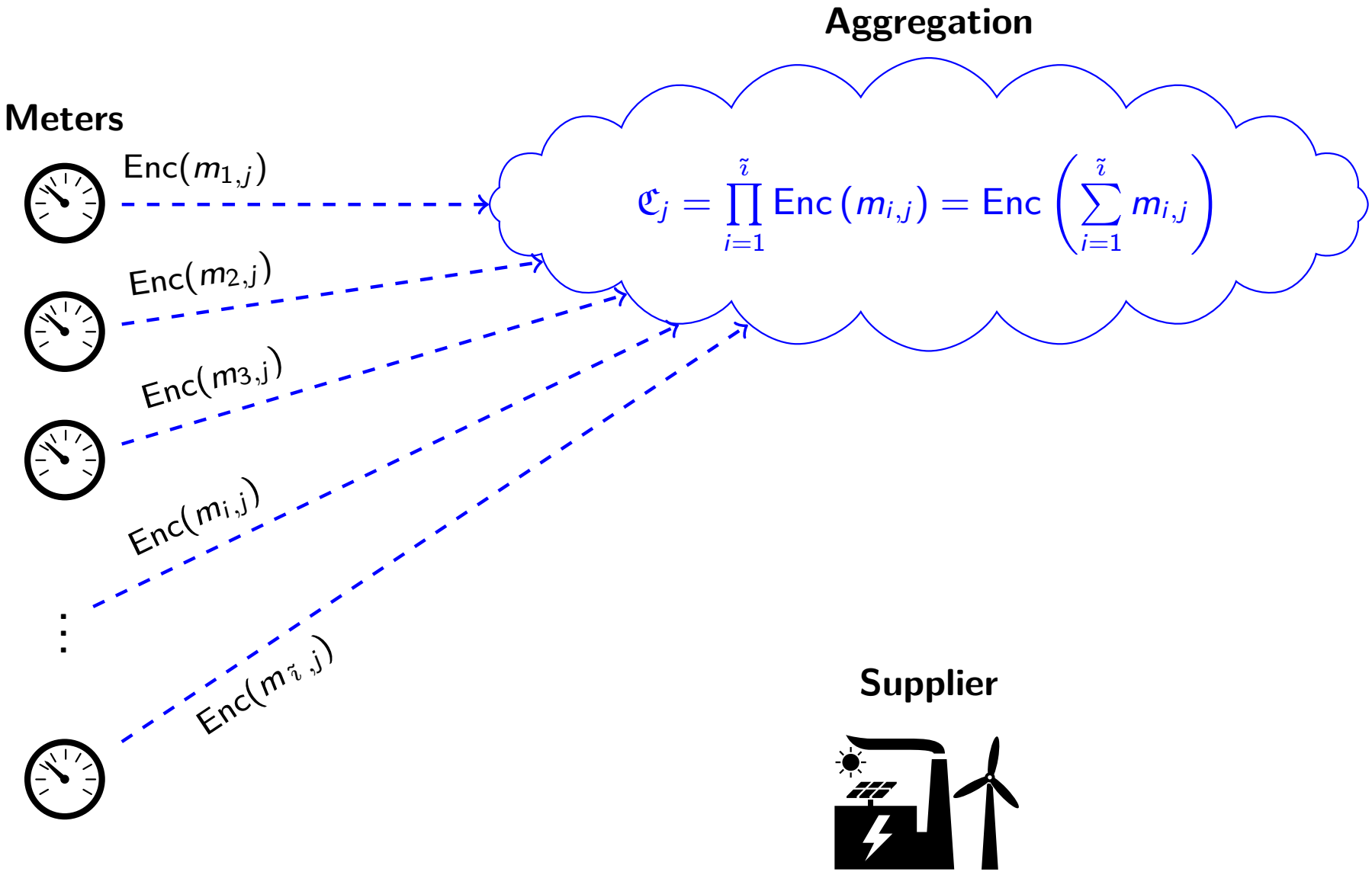
Round	1	2	$\cdots$	$\tilde{j}$	**Billing**
Meter 1	$m_{1,1}$	$m_{1,2}$	$\cdots$	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$	$\cdots$	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Meter $\tilde{i}$	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$	$\cdots$	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidated	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$	$\cdots$	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	$=$

✗ ✓

PPPs only work with large aggregations

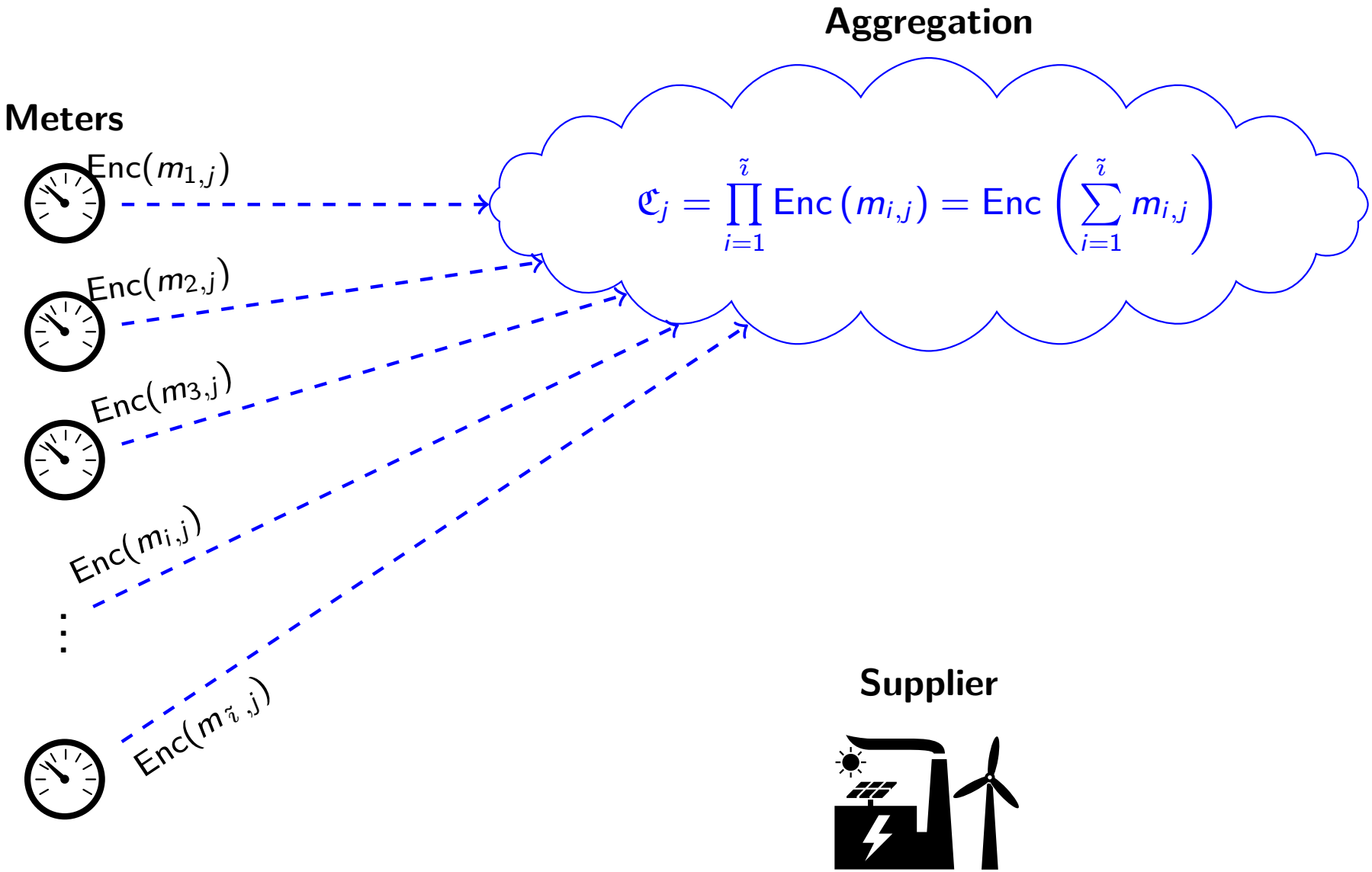
Aggregation

Additive homomorphic encryption primitives (AHEPs)



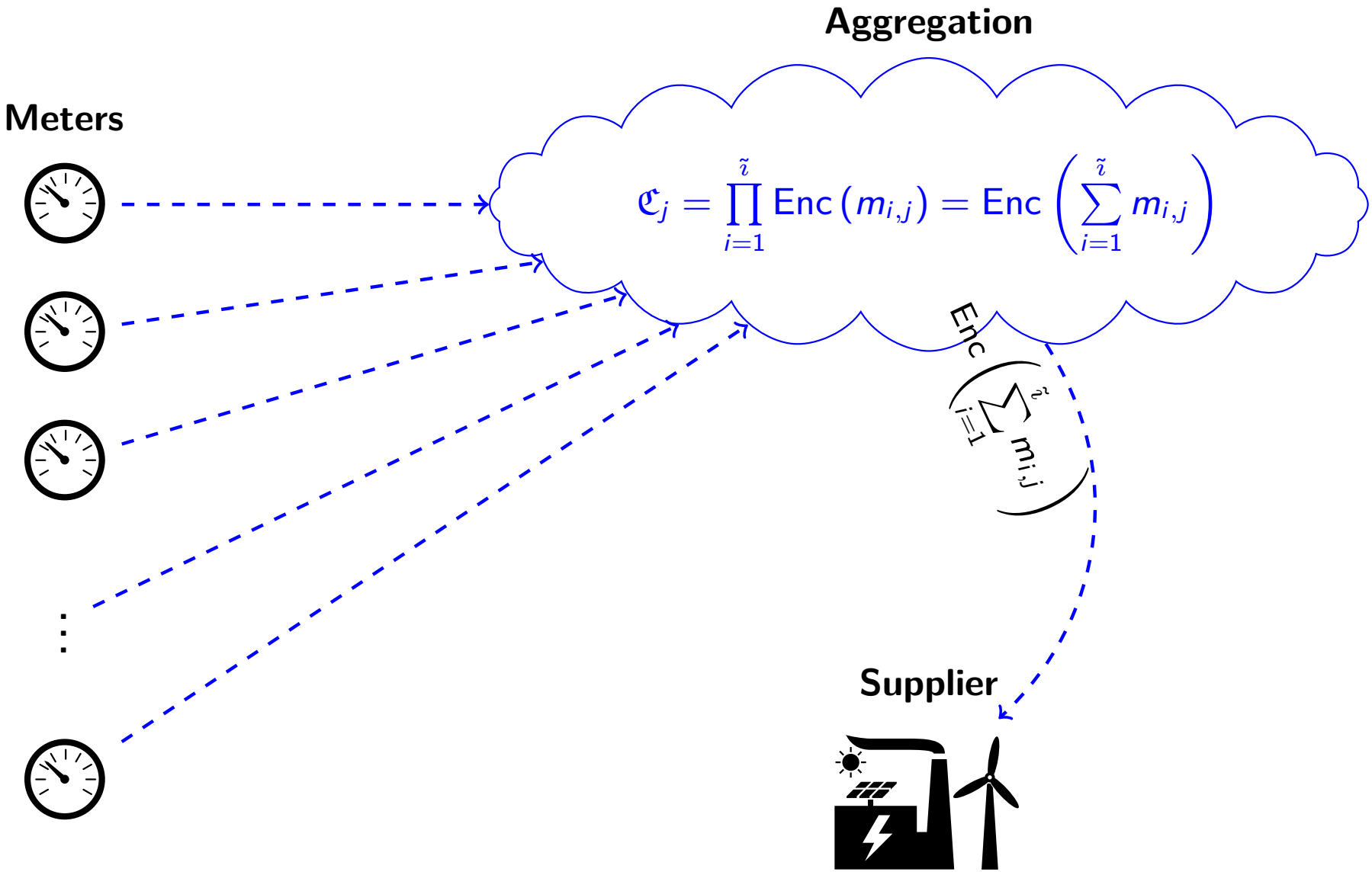
Aggregation

AHEPs



Aggregation

AHEPs



Requirement 1

Recoverability of consolidated consumption 

Requirements

Requirements for Smart Grids

Requirement 1

Recoverability of consolidated consumption 

Requirement 2

Recoverability of bill based on dynamic pricing 

Requirements

Requirements for Smart Grids

Requirement 1

Recoverability of consolidated consumption 

Requirement 2

Recoverability of bill based on dynamic pricing 

Requirement 3

Verification (auditability) 

Requirements

Requirements for Smart Grids

Requirement 1

Recoverability of consolidated consumption 

Requirement 2

Recoverability of bill based on dynamic pricing 

Requirement 3

Verification (auditability) 

Requirement 4

Efficiency 

CSR
LNCC

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security

Introduction to PPP

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

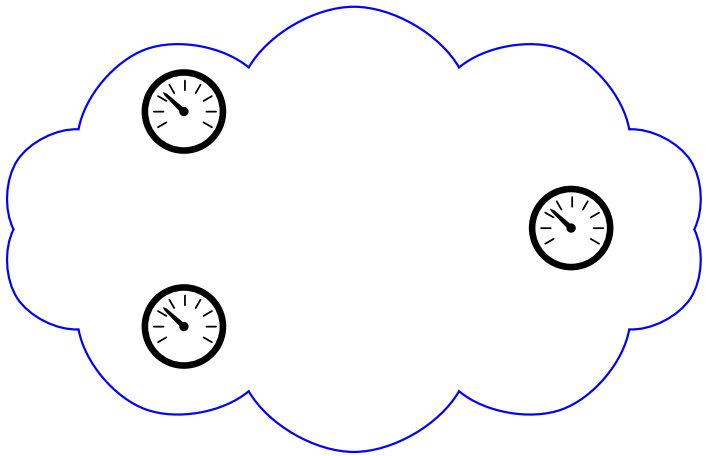
ADC-Nets

Simulation Using Real-World Data

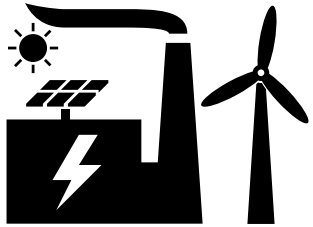
Conclusion and Outlook

PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]

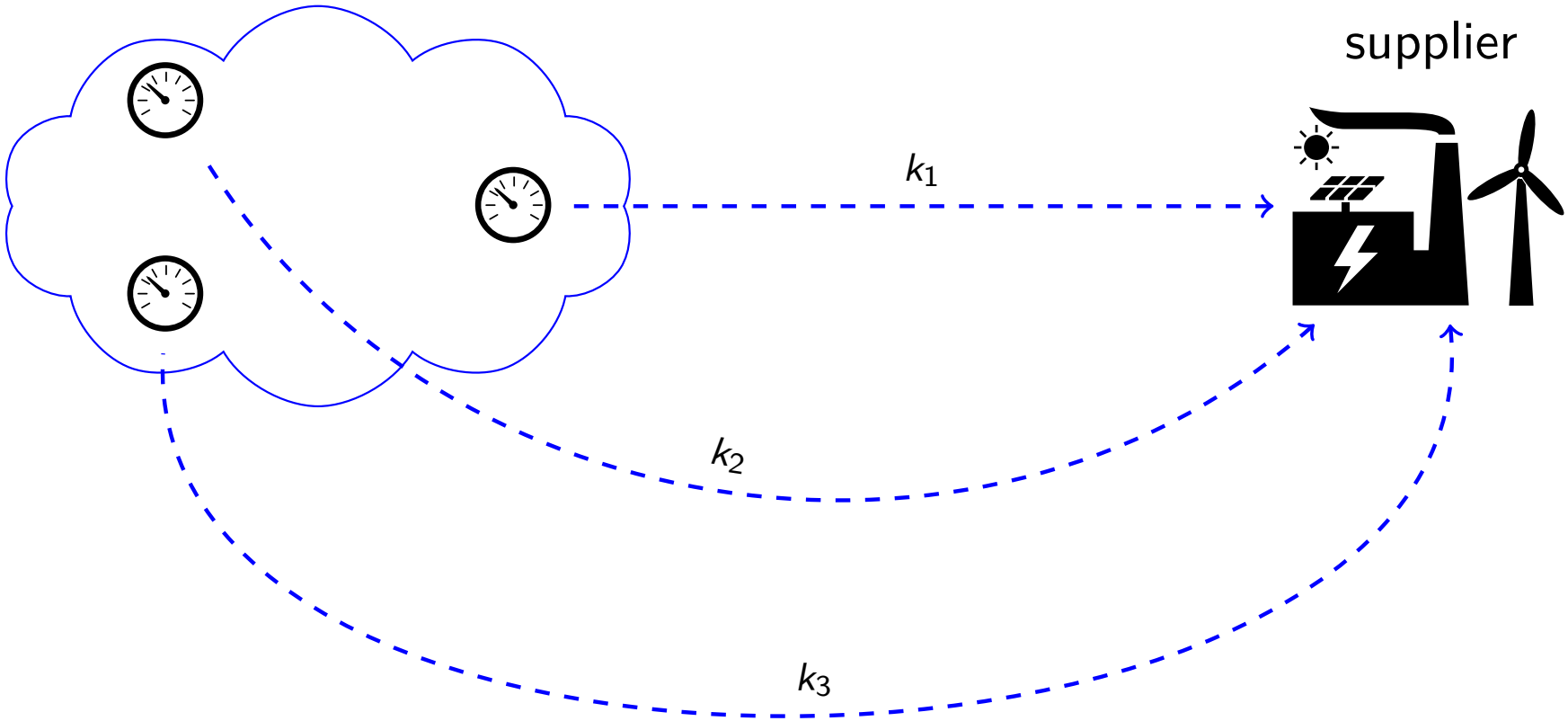


supplier



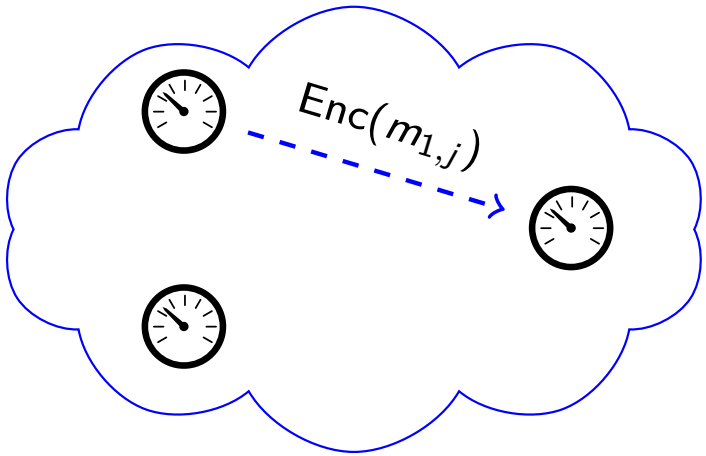
PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]

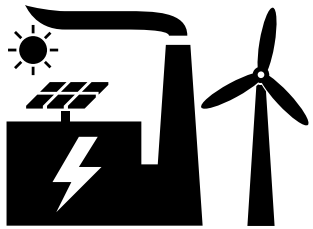


PPP1 -   - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]

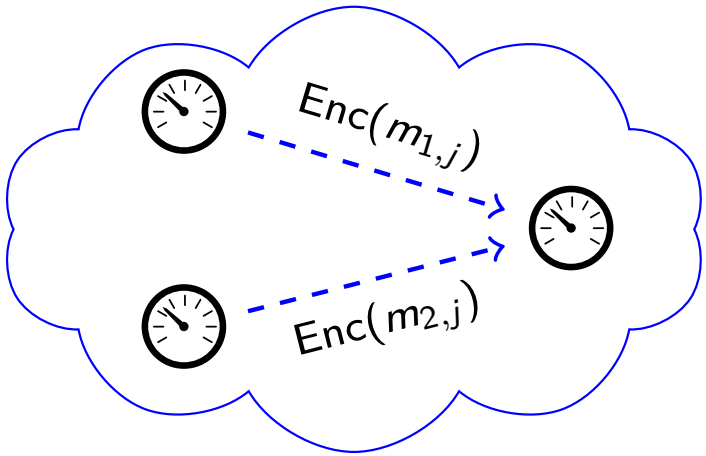


supplier

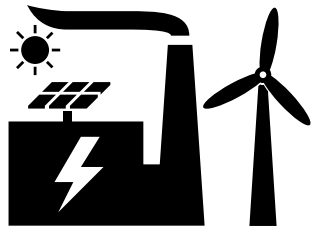


PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]

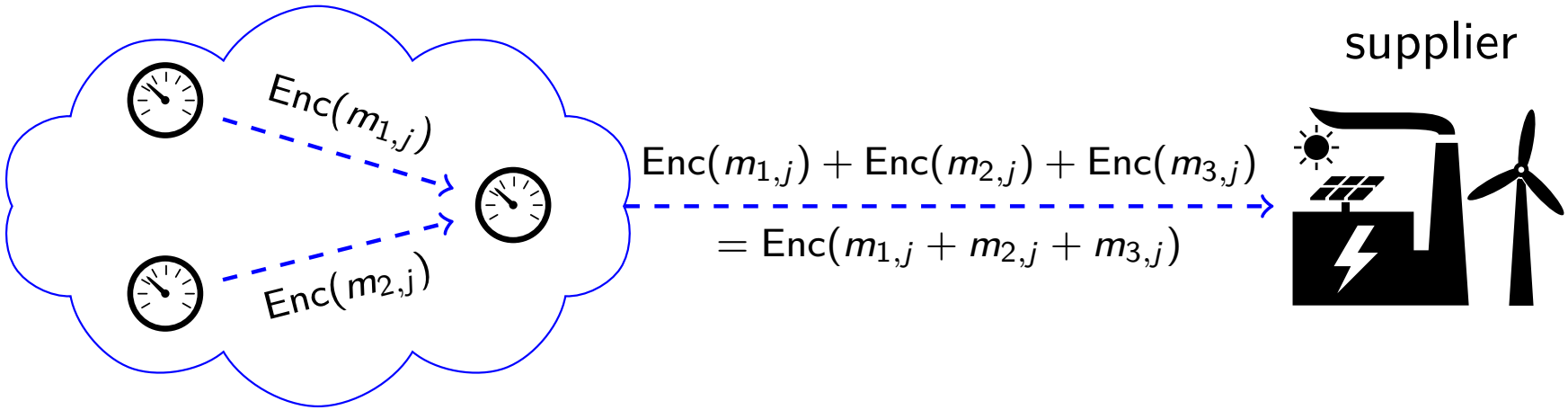


supplier



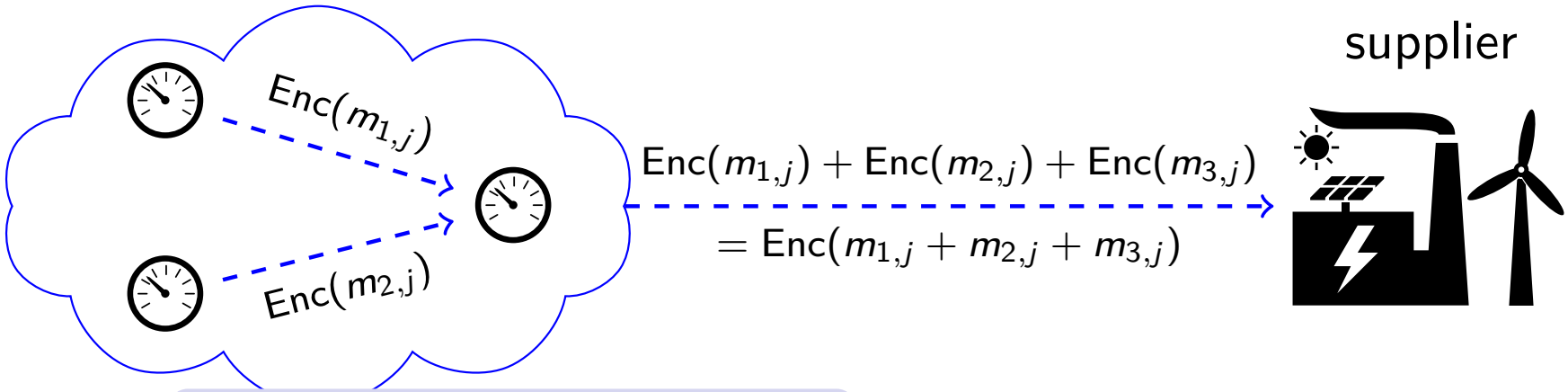
PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]



PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]

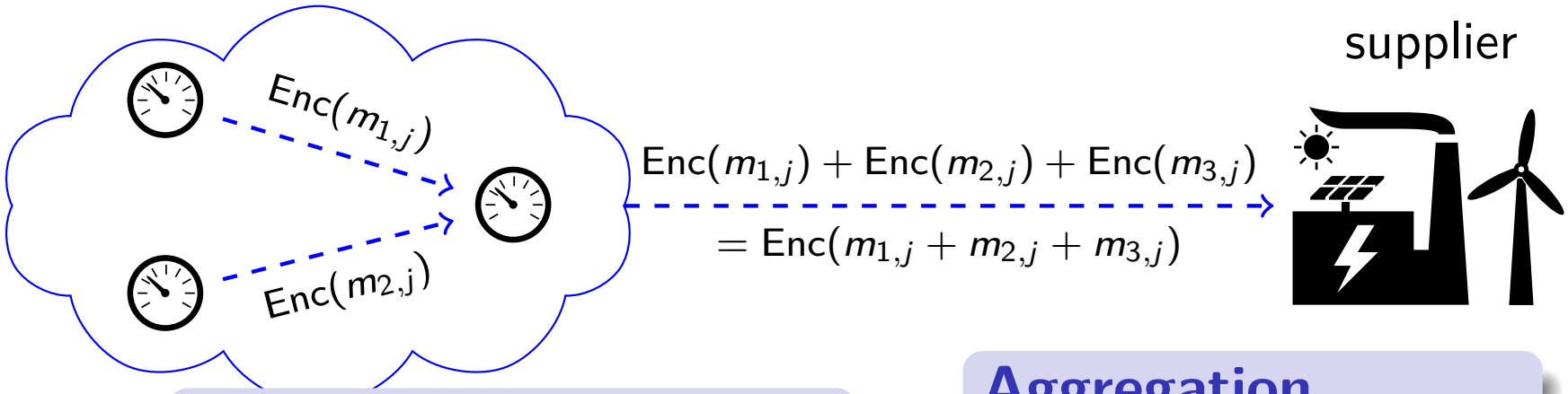


Encryption

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

PPP1 -  - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]



Encryption

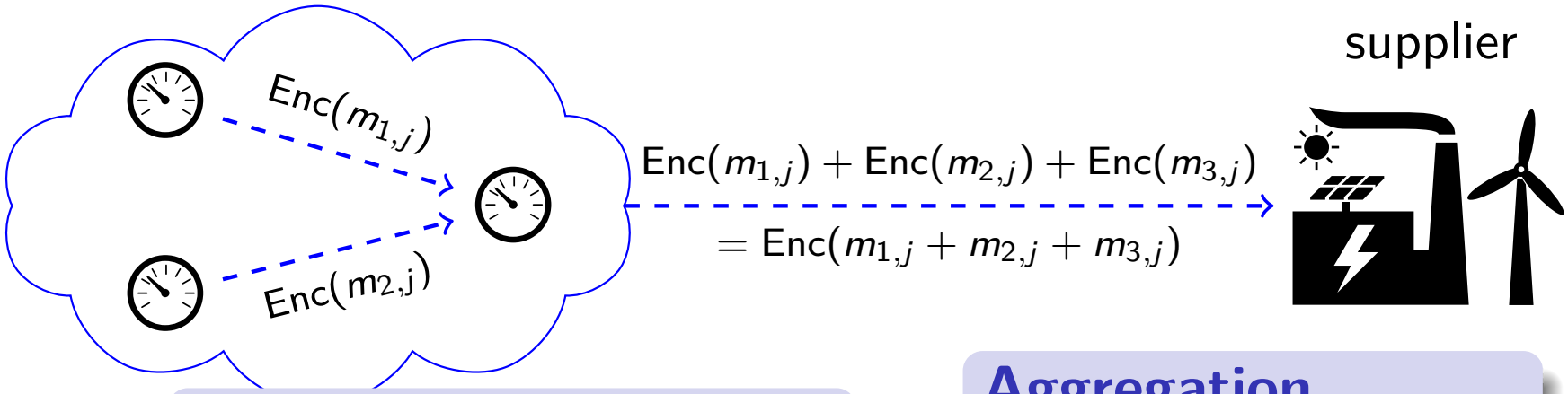
$$Enc(m_{i,j}) = m_{i,j} + H(k_i||j)$$

Aggregation

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

PPP1 - - SDC-Nets

SDC-Nets Using In-Network Aggregation [BM14a]



Encryption

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

Aggregation

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

Decryption

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

PPP1

PPP1 meets the following requirements

Requirement 1 - ✓

Recoverability of consolidated consumption 

Requirement 2 - ✗

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✗

Verification (auditability) 

Requirement 4 - ✓

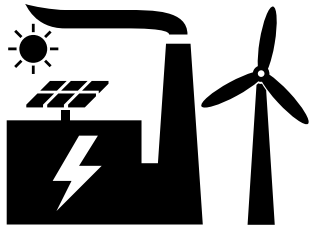
Efficiency 

PPP2 - - Commitment

Commitment Based on ECC [BM14a]

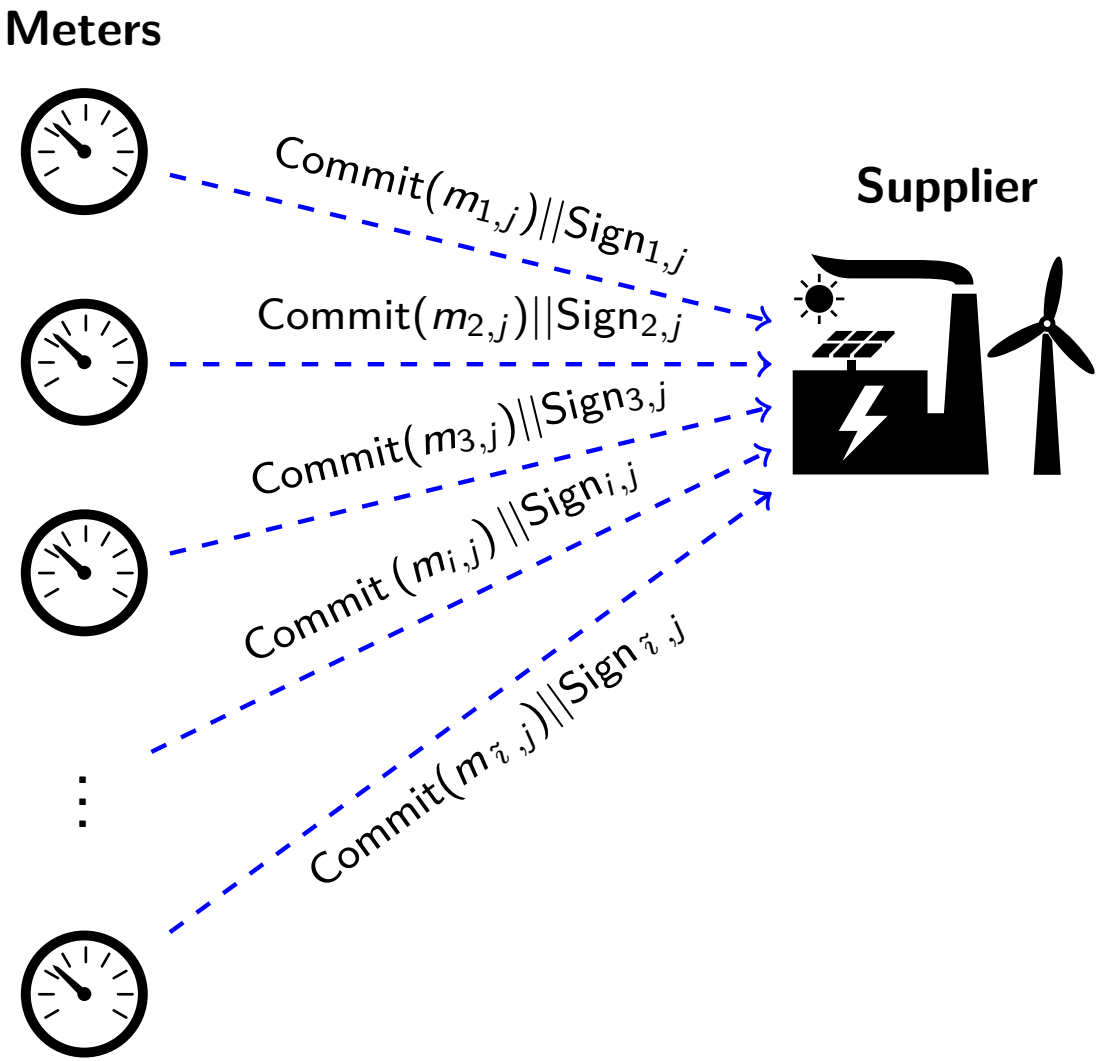
Meters

Supplier



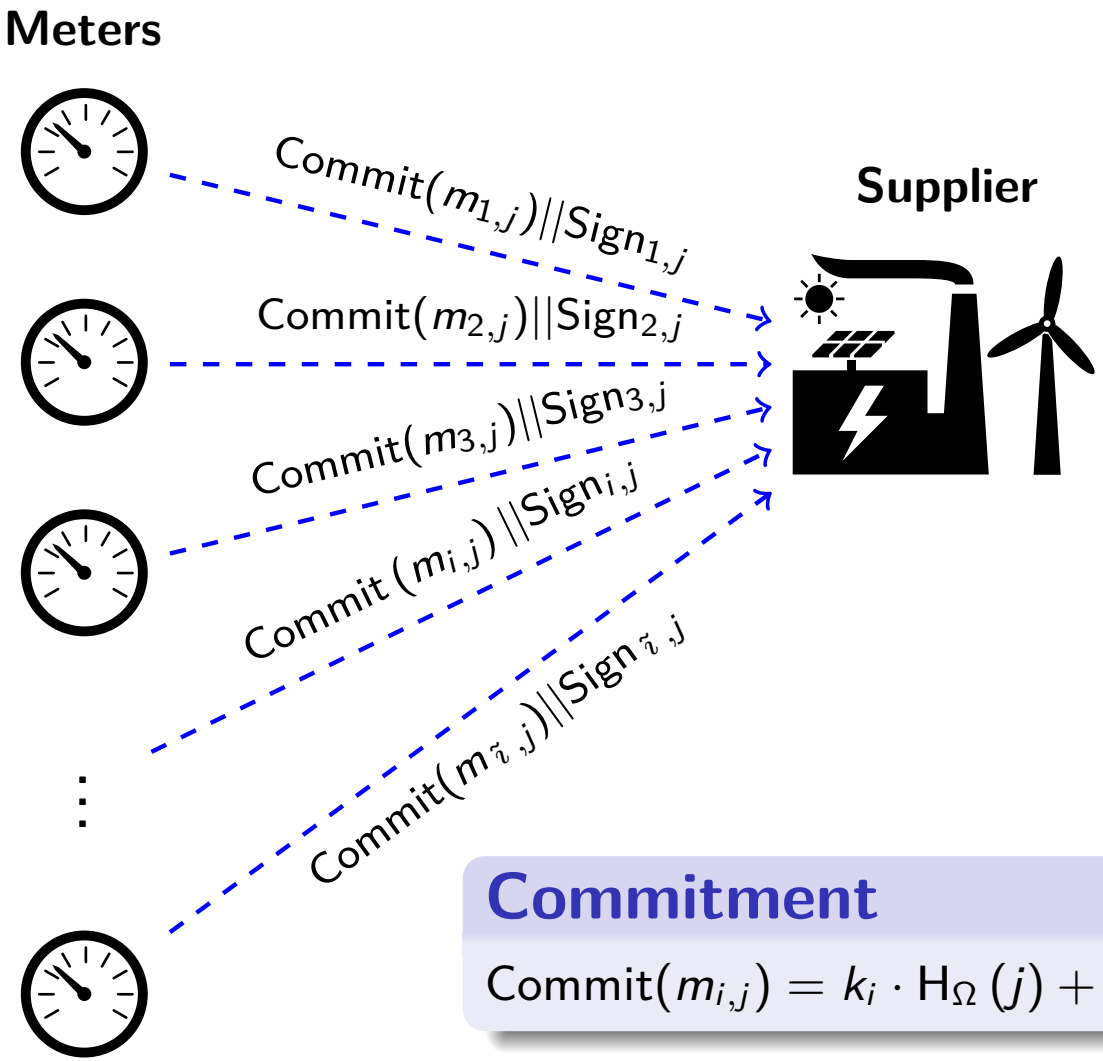
PPP2 -  - Commitment

Commitment Based on ECC [BM14a]



PPP2 -  - Commitment

Commitment Based on ECC [BM14a]



Commitment

$$\text{Commit}(m_{i,j}) = k_i \cdot \text{H}_\Omega(j) + m_{i,j} \cdot P$$

PPP2

PPP2 meets the following requirements

Requirement 1 - ✗

Recoverability of consolidated consumption 

Requirement 2 - ✓

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✓

Verification (auditability) 

Requirement 4 - ✓

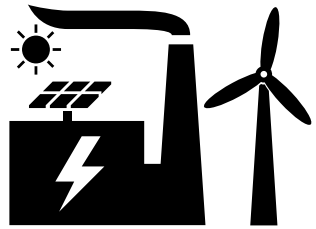
Efficiency 

PPP2 - Verification

[BDBBM14; BM14b; BM14a; BBM14; BVM15]

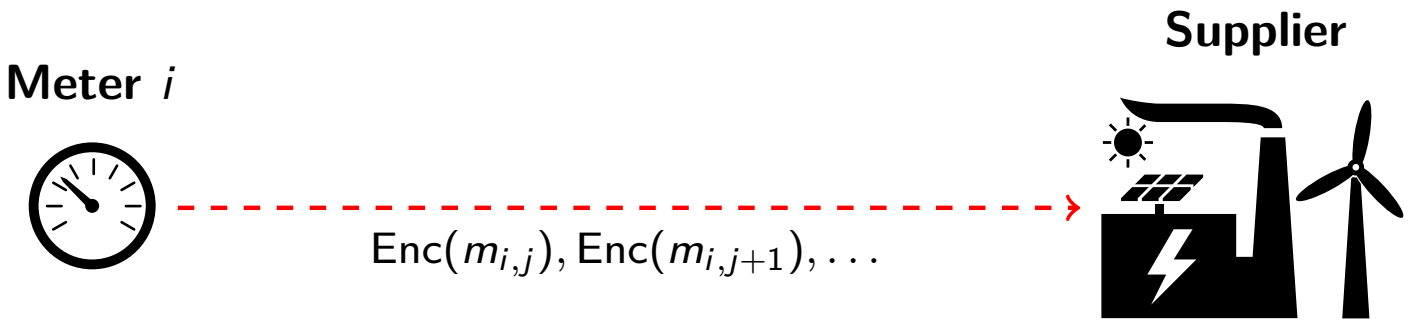
Meter *i*

Supplier



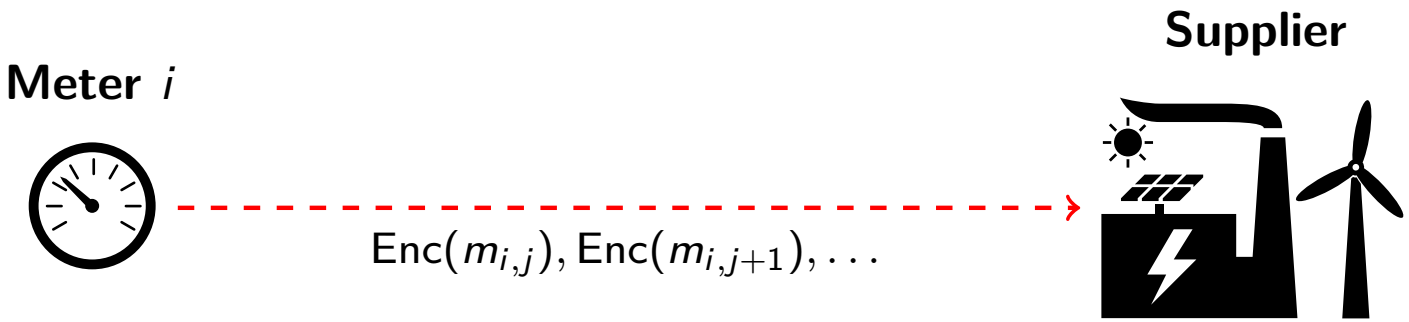
PPP2 - Verification

[BDBBM14; BM14b; BM14a; BBM14; BVM15]



PPP2 - Verification

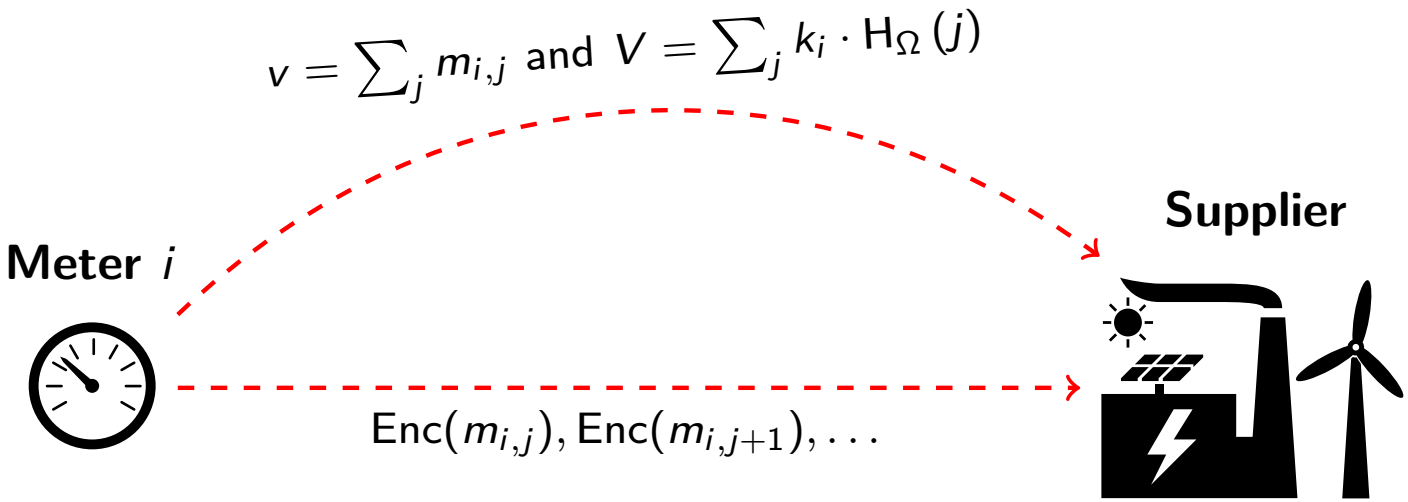
[BDBBM14; BM14b; BM14a; BBM14; BVM15]



$$Q = \sum_j \mathsf{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

PPP2 - Verification

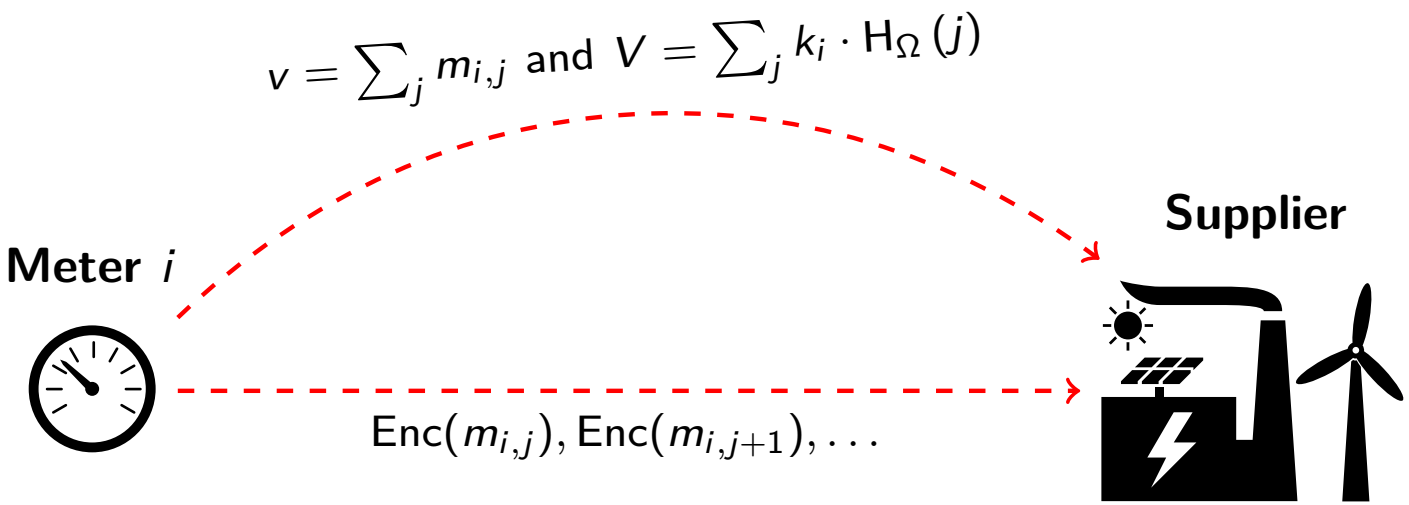
[BDBBM14; BM14b; BM14a; BBM14; BVM15]



$$Q = \sum_j \mathrm{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

PPP2 - Verification

[BDBBM14; BM14b; BM14a; BBM14; BVM15]



$$Q = \sum_j \mathrm{Enc}(m_{i,j}) = \sum_j k_i \cdot \mathrm{H}_\Omega(j) + m_{i,j} \cdot P$$

Verification

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

PPP2 - Performance

[BM14b; BM14a; BVM15; BDBBM14; LBPN12]

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

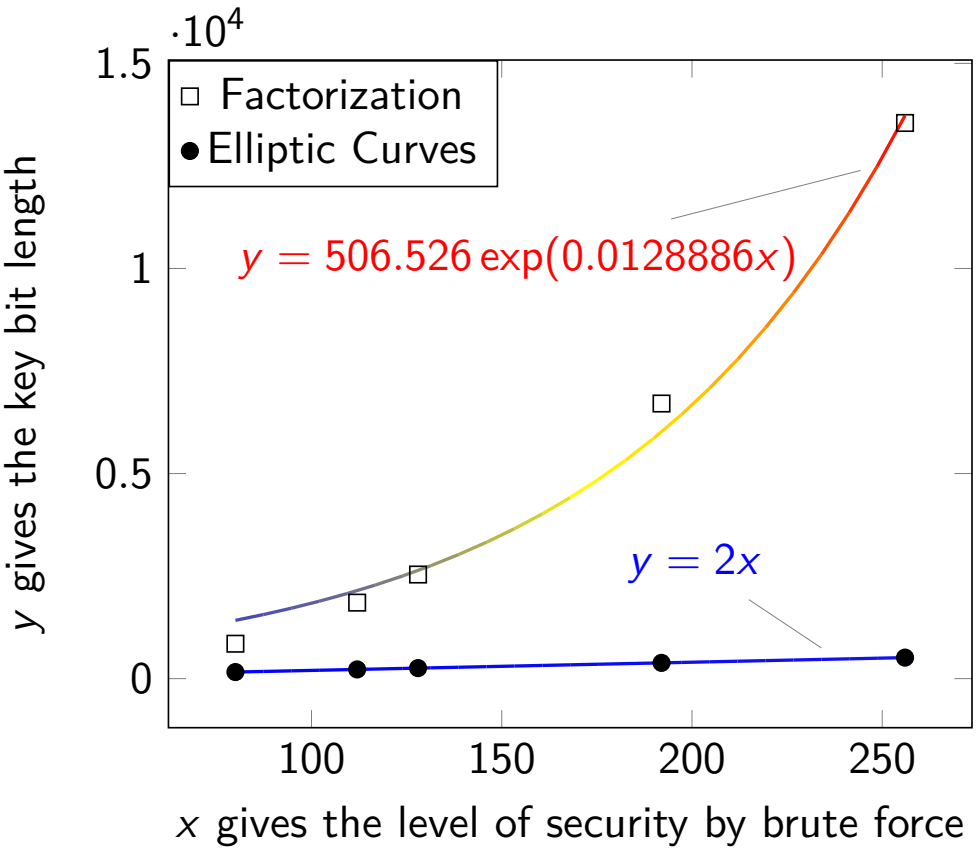


Table of Contents

Outline

Security

Introduction to PPP

Privacy-Preserving Protocols (PPPs)

- PPP1 - Based on SDC-Nets
- PPP2 - Based on Commitment
- PPP3 - Based on ADC-Net
- PPP4 - Based on Quantum Cryptography

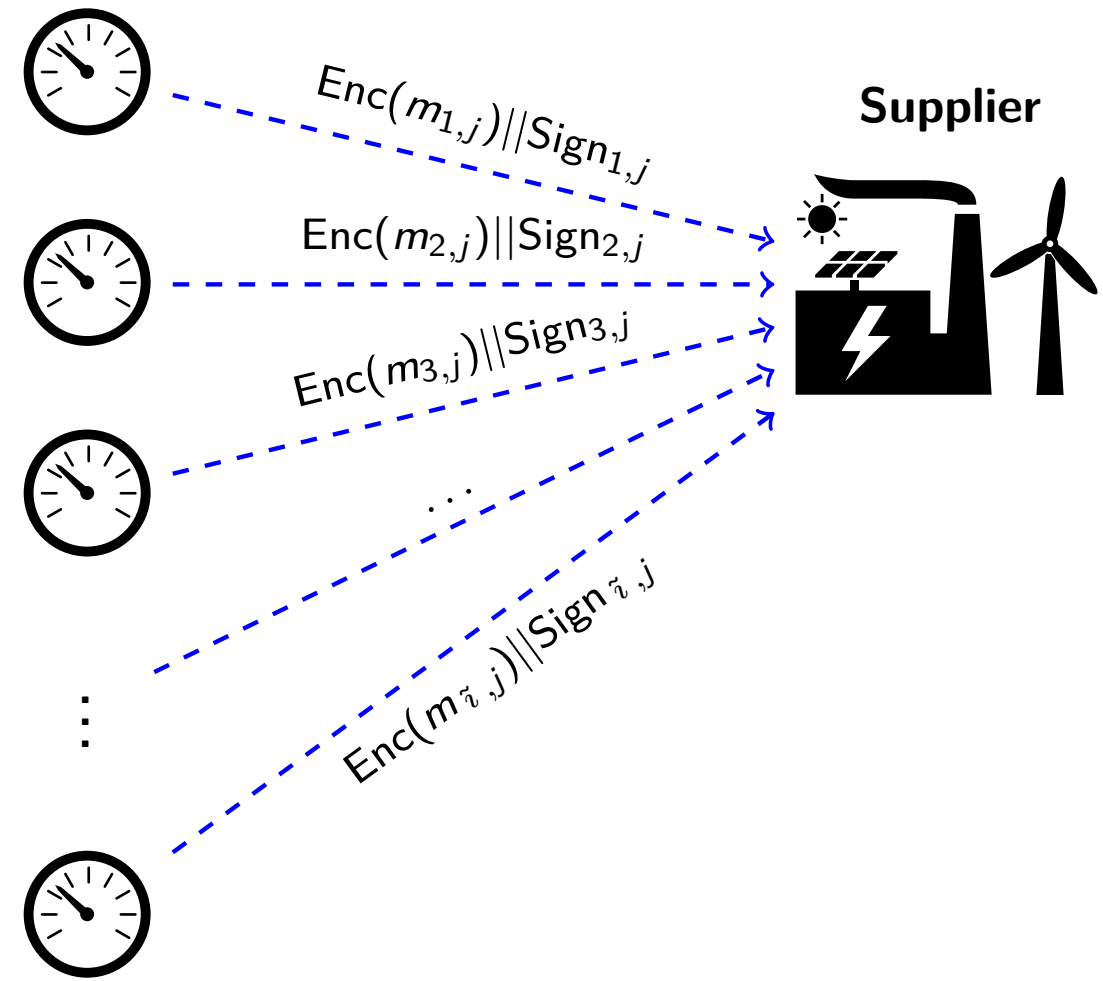
ADC-Nets

Simulation Using Real-World Data

Conclusion and Outlook

PPP3 -  - New Concept

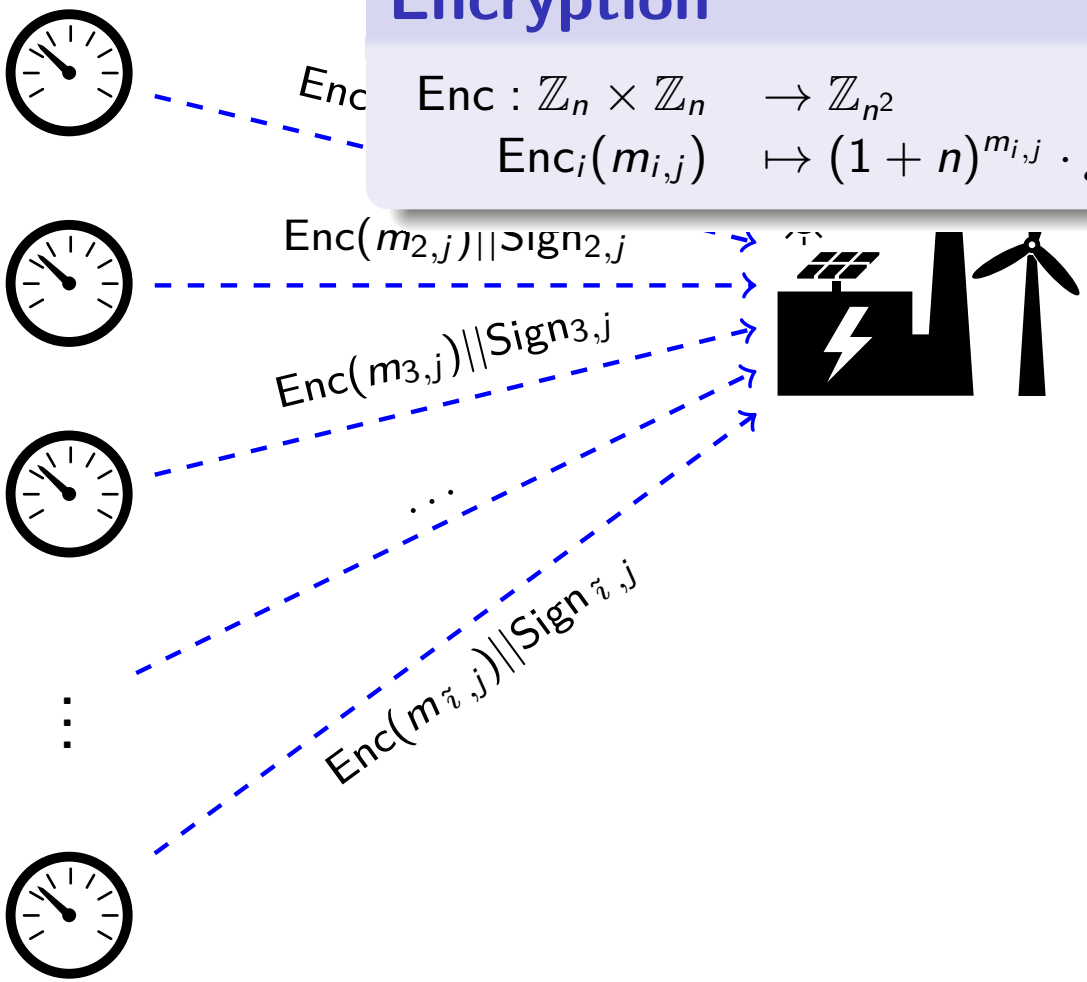
ADC-Net - [BBM14; BM14b; BVM15]



PPP3 -  - New Concept

ADC-Net - [BBM14; BM14b; BVM15]

Meters

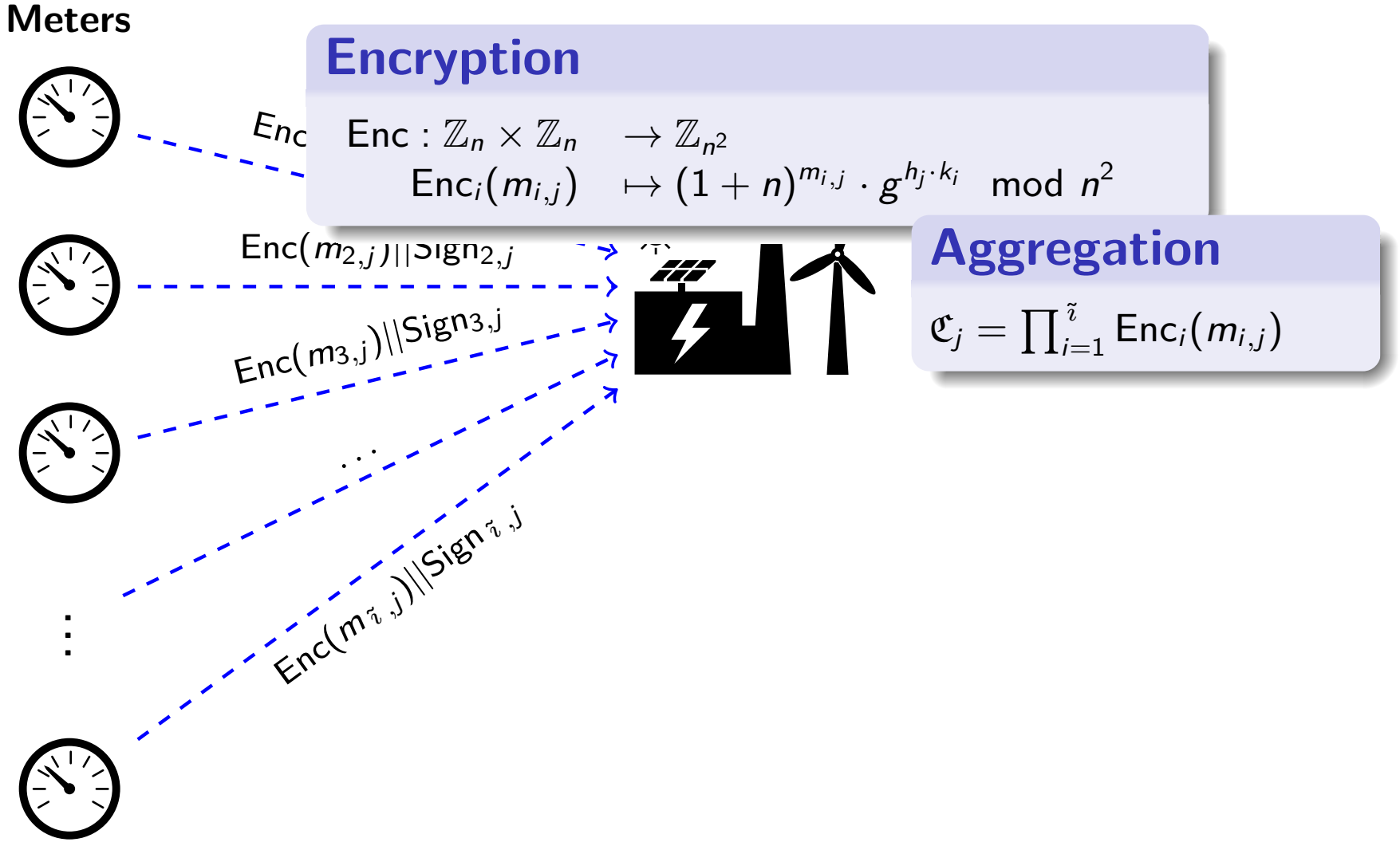


Encryption

$$\begin{aligned} \mathrm{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_{n^2} \\ \mathrm{Enc}_i(m_{i,j}) &\mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2 \end{aligned}$$

PPP3 -  - New Concept

ADC-Net - [BBM14; BM14b; BVM15]



PPP3 -  - New Concept

ADC-Net - [BBM14; BM14b; BVM15]

Meters




$\mathrm{Enc}(m_{2,j})||\mathrm{Sign}_{2,j}$

$\mathrm{Enc}(m_{3,j})||\mathrm{Sign}_{3,j}$

$\vdots$

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

Encryption

$$\begin{aligned} \mathrm{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_{n^2} \\ \mathrm{Enc}_i(m_{i,j}) &\mapsto (1+n)^{m_{i,j}} \cdot g^{h_j \cdot k_i} \mod n^2 \end{aligned}$$

Aggregation

$$\mathfrak{C}_j = \prod_{i=1}^{\tilde{i}} \mathrm{Enc}_i(m_{i,j})$$

Decryption

$$\begin{aligned} \mathrm{Dec} : \mathbb{Z}_{n^2} &\to \mathbb{Z}_n \\ \mathrm{Dec}\,(\mathfrak{C}_j) &\mapsto \frac{\left(\mathfrak{C}_j \cdot g^{-h_t \cdot s} \mod n^2\right) - 1}{n} \end{aligned}$$

PPP3

PPP3 meets the following requirements

Requirement 1 - ✓

Recoverability of consolidated consumption 

Requirement 2 - ✓

Recoverability of bill based on dynamic pricing 

Requirement 3 - ✓

Verification (auditability) 

Requirement 4 - ✓

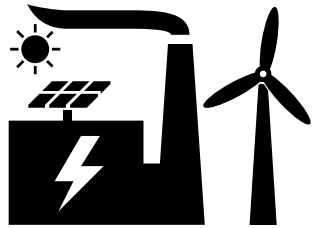
Efficiency 

PPP4 -  - Quantum Cryptography

No Keys [BSM14; BPP12]

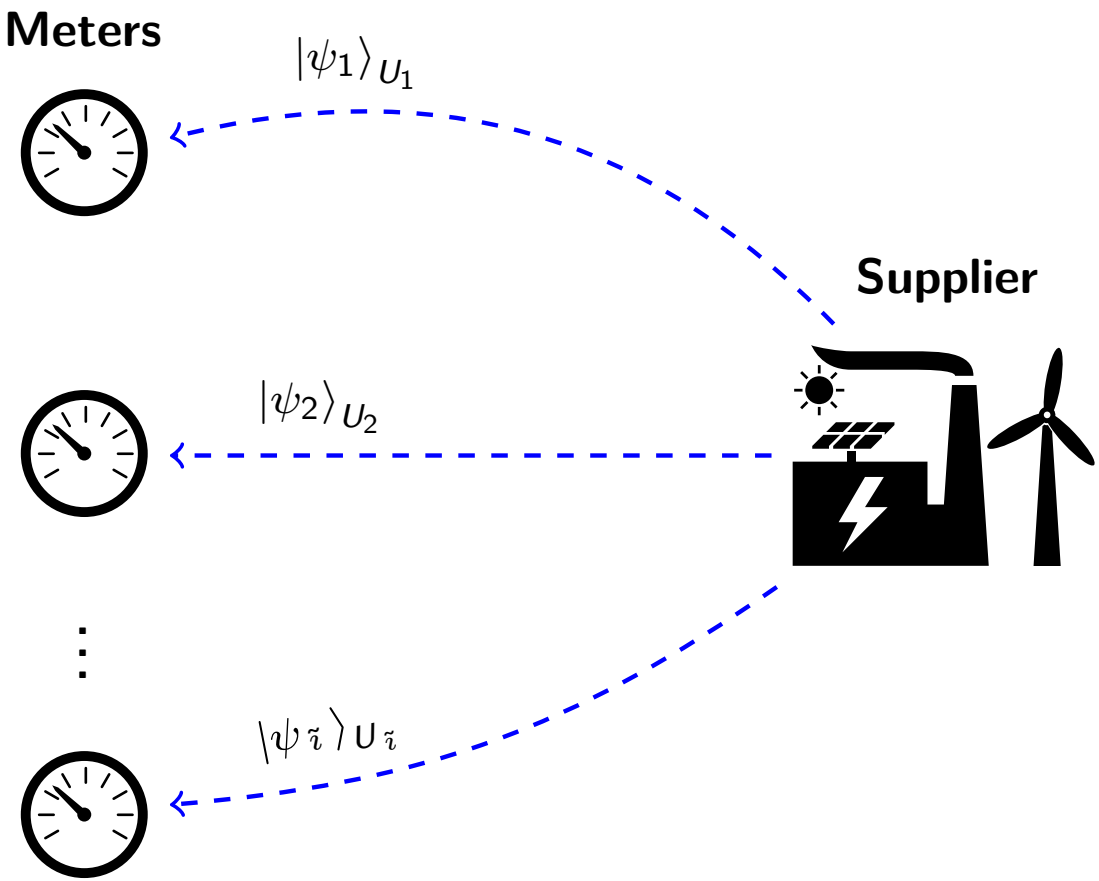
Meters

Supplier



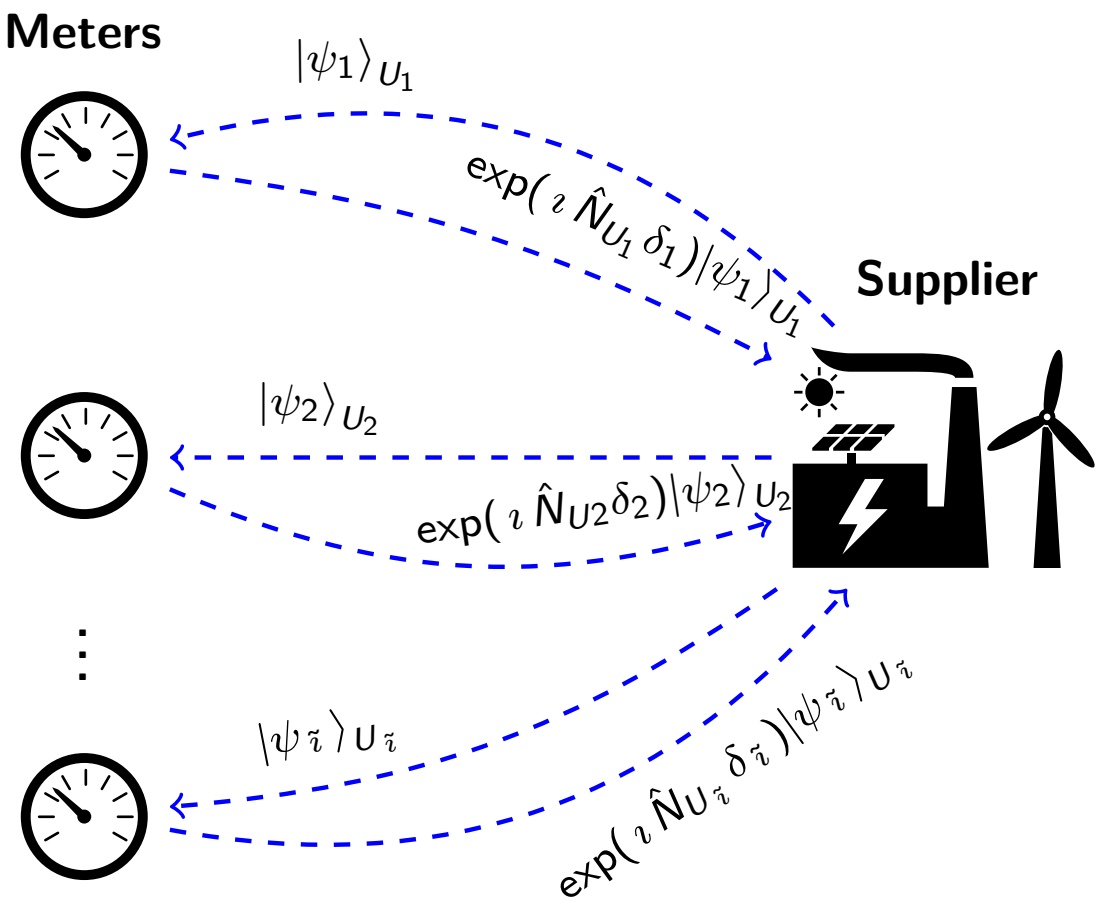
PPP4 -  - Quantum Cryptography

No Keys [BSM14; BPP12]



PPP4 - - Quantum Cryptography

No Keys [BSM14; BPP12]



PPP4

PPP4 meets the following requirements

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 

CSR
LNCC

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security

Introduction to PPP

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

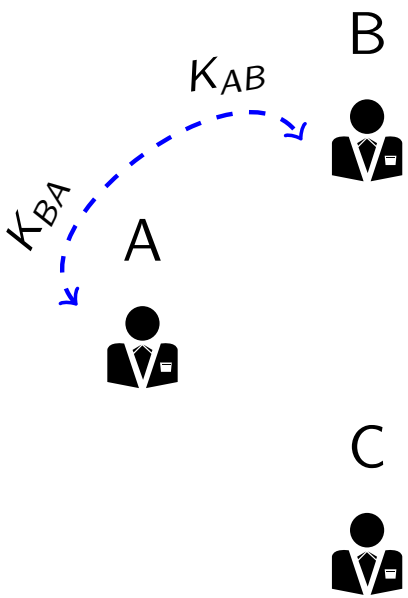
Conclusion and Outlook

Symmetric DC-Nets (SDC-Nets)

[Cha88] - Dining Cryptographers Problem

SDC-Nets

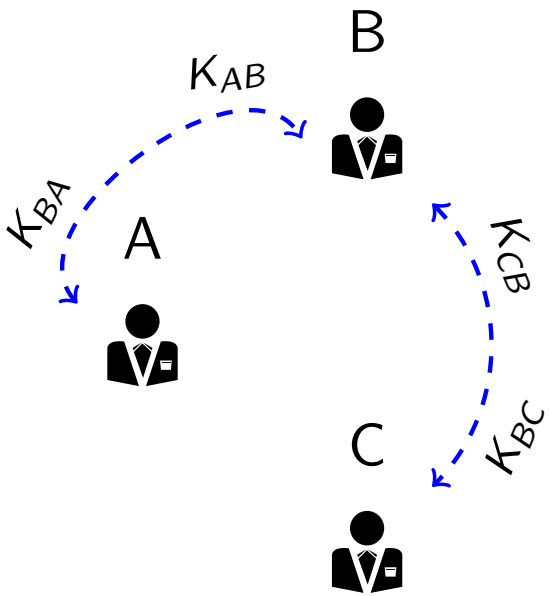
[Cha88] - Dining Cryptographers Problem



Agent

SDC-Nets

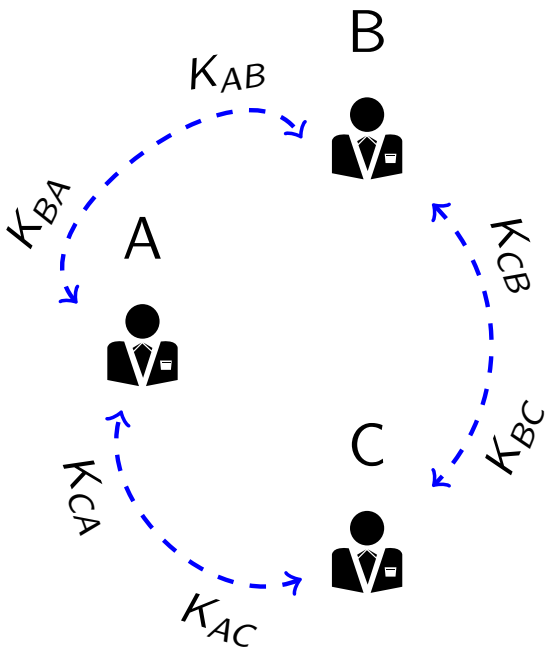
[Cha88] - Dining Cryptographers Problem



Agent

SDC-Nets

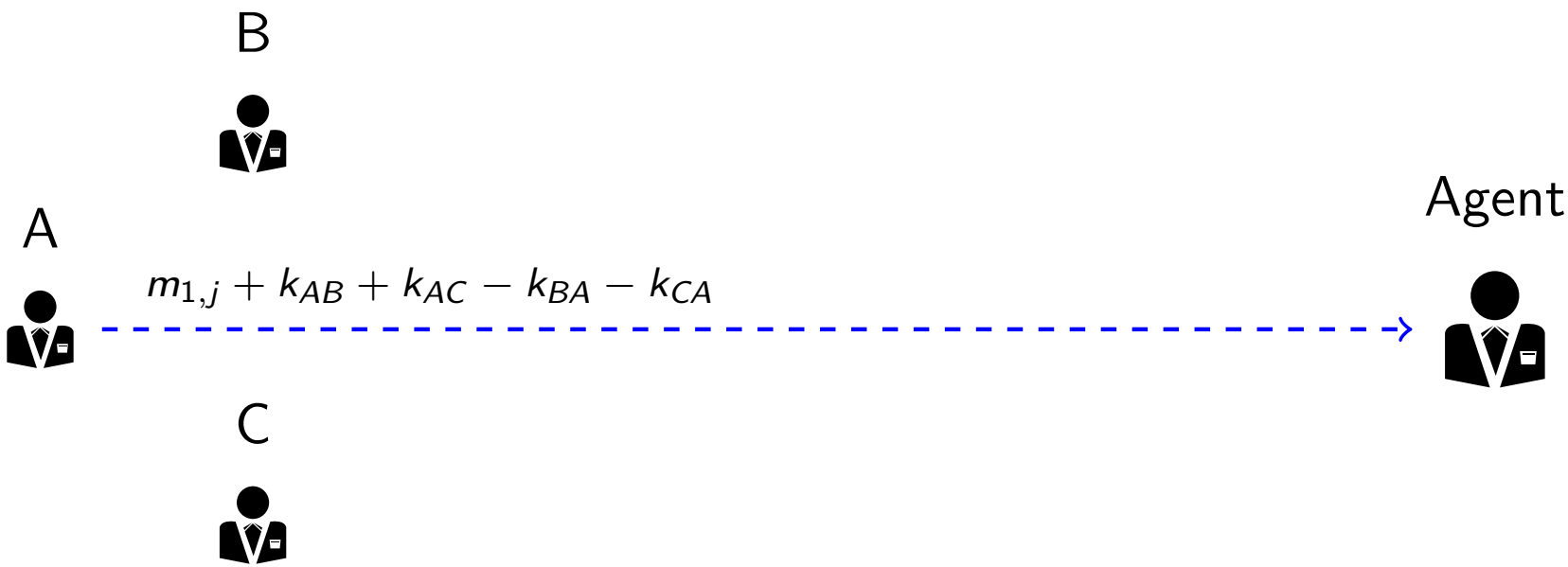
[Cha88] - Dining Cryptographers Problem



Agent

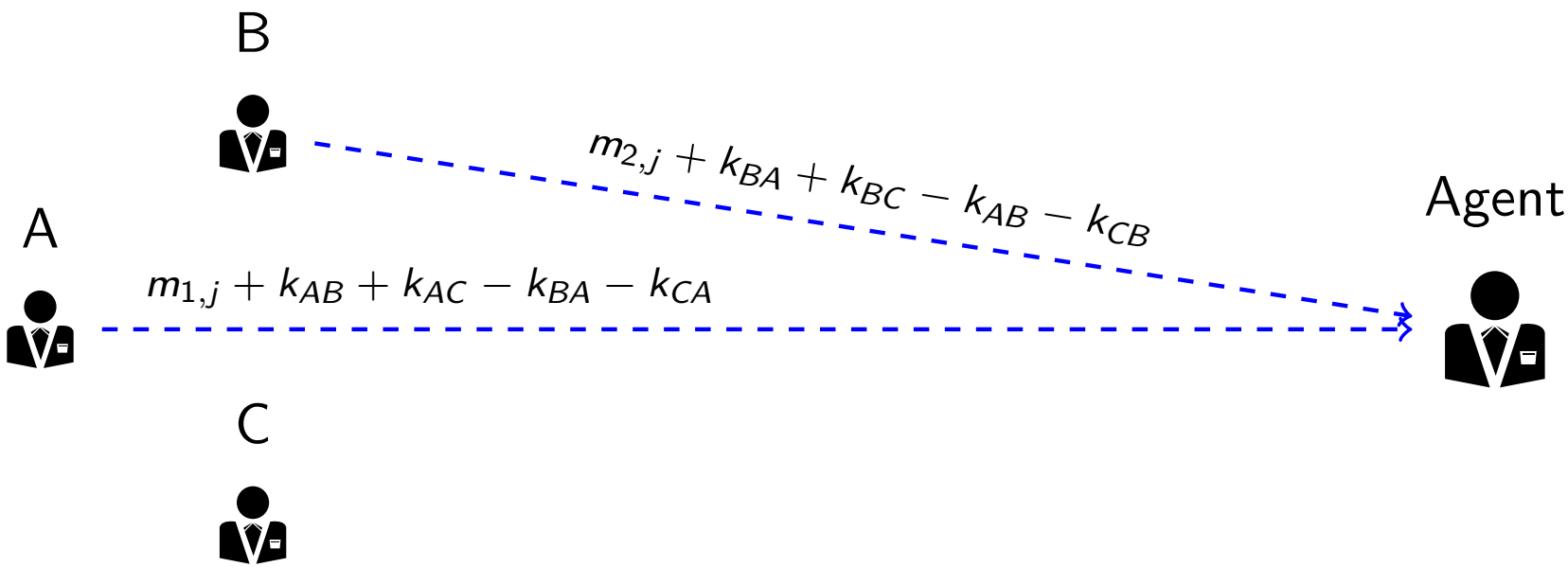
SDC-Nets

Unconditional Secure [Cha88]



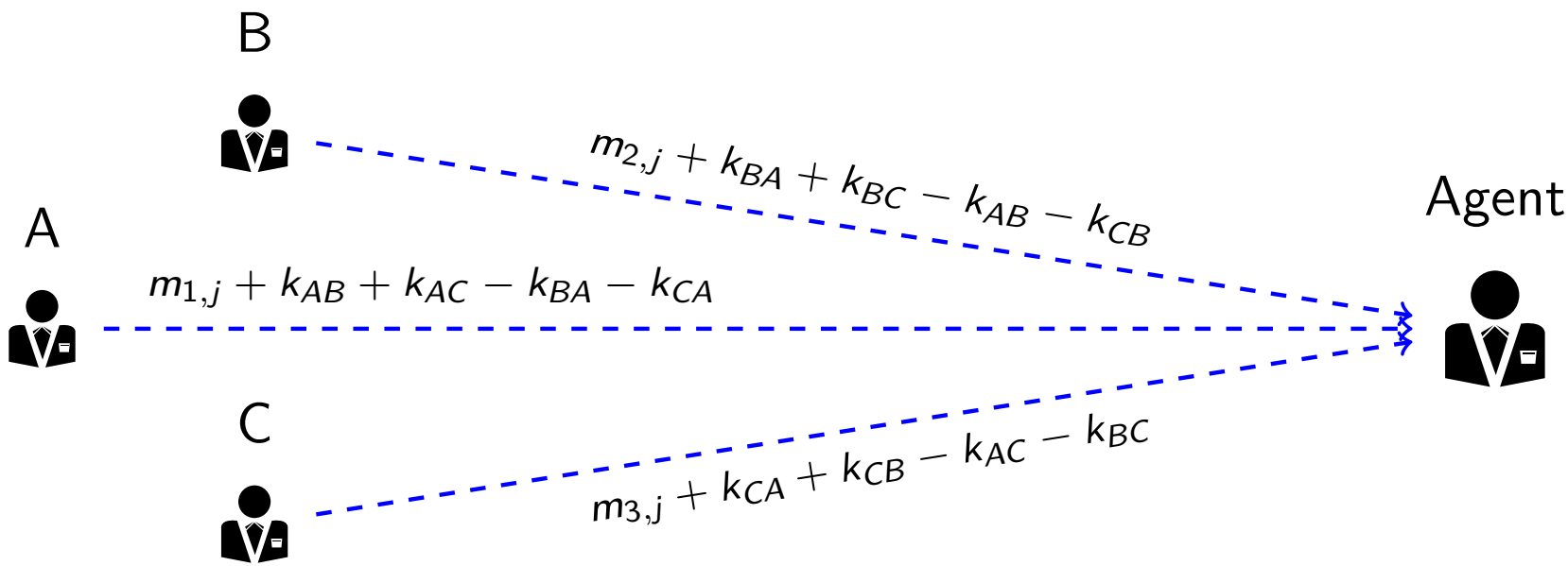
SDC-Nets

Unconditional Secure [Cha88]



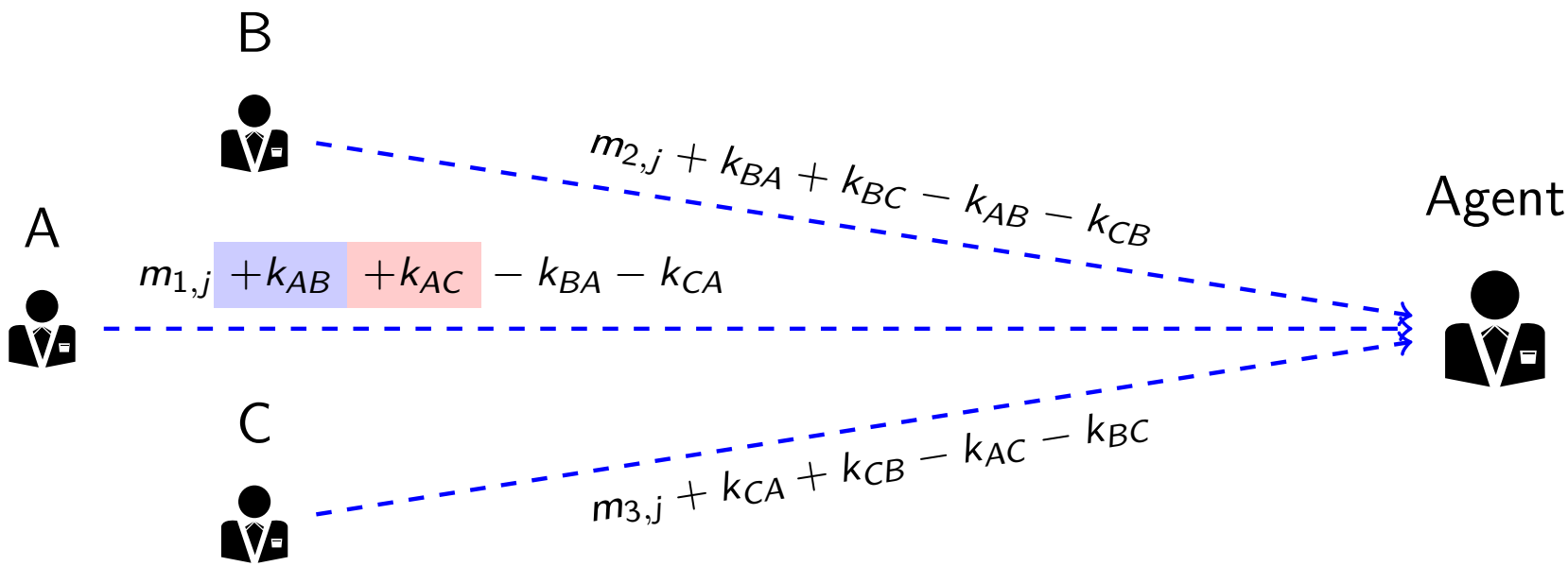
SDC-Nets

Unconditional Secure [Cha88]



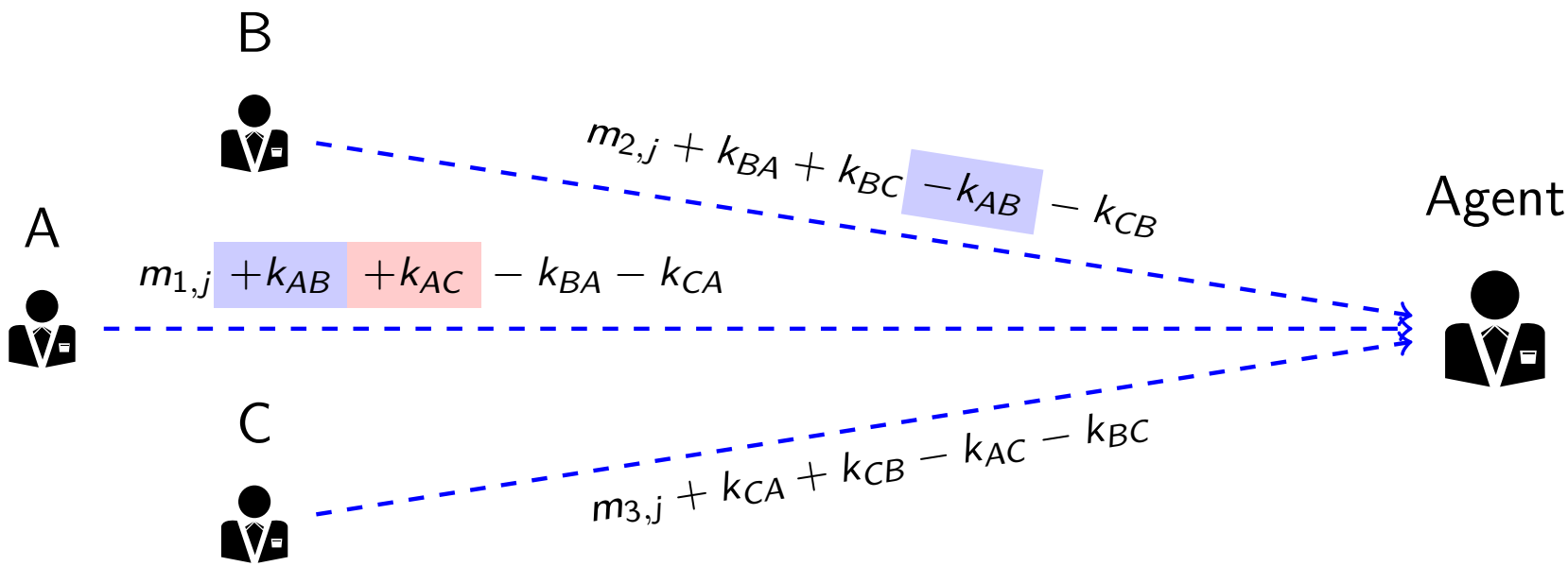
SDC-Nets

Unconditional Secure [Cha88]



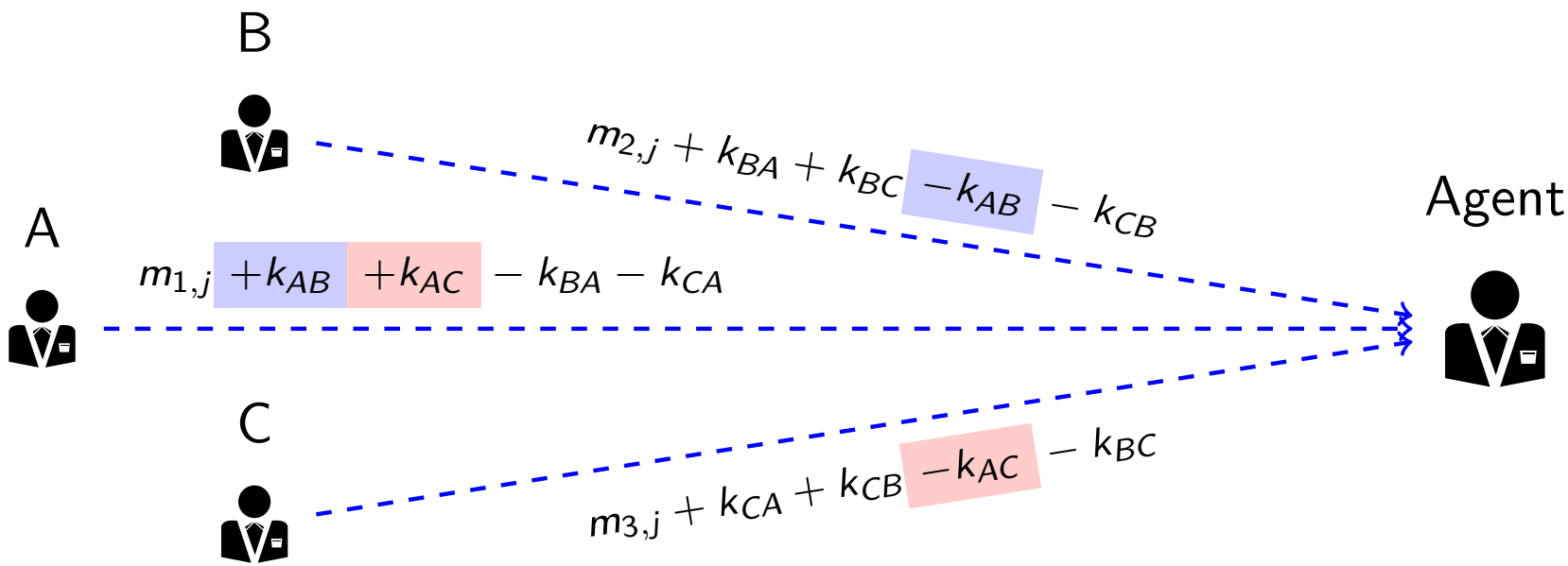
SDC-Nets

Unconditional Secure [Cha88]



SDC-Nets

Unconditional Secure [Cha88]

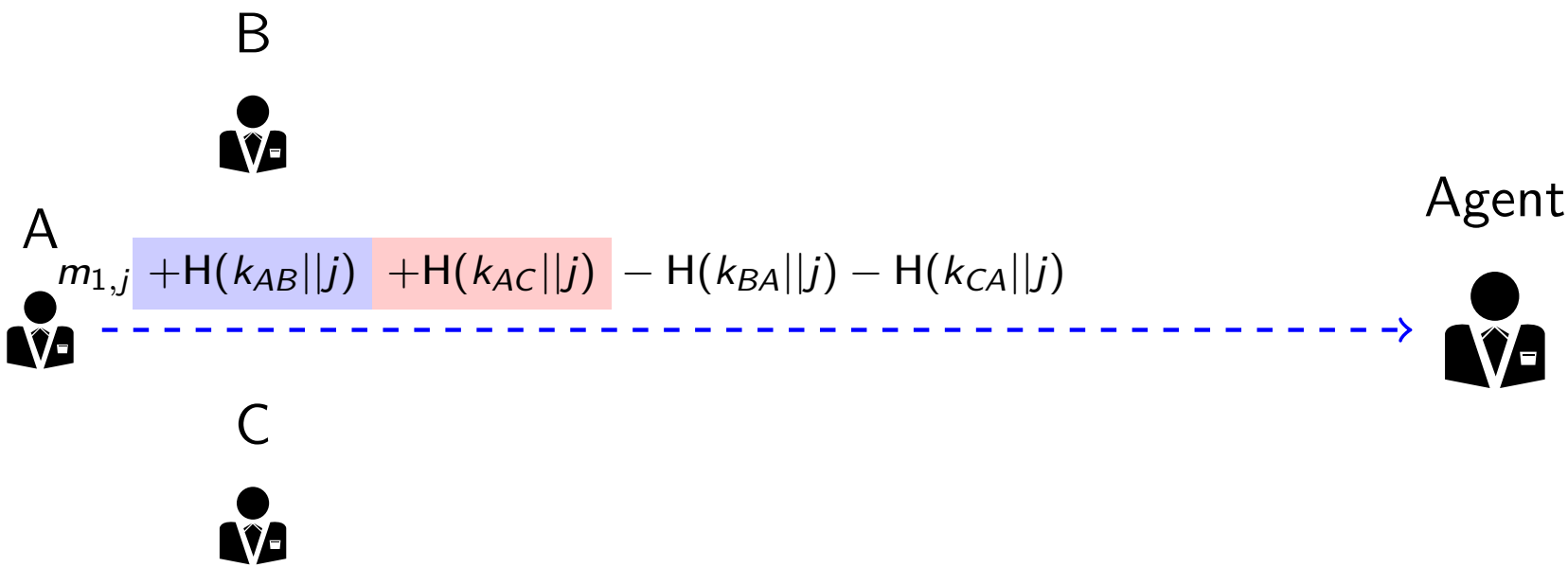


SDC-Nets

[GJ04]

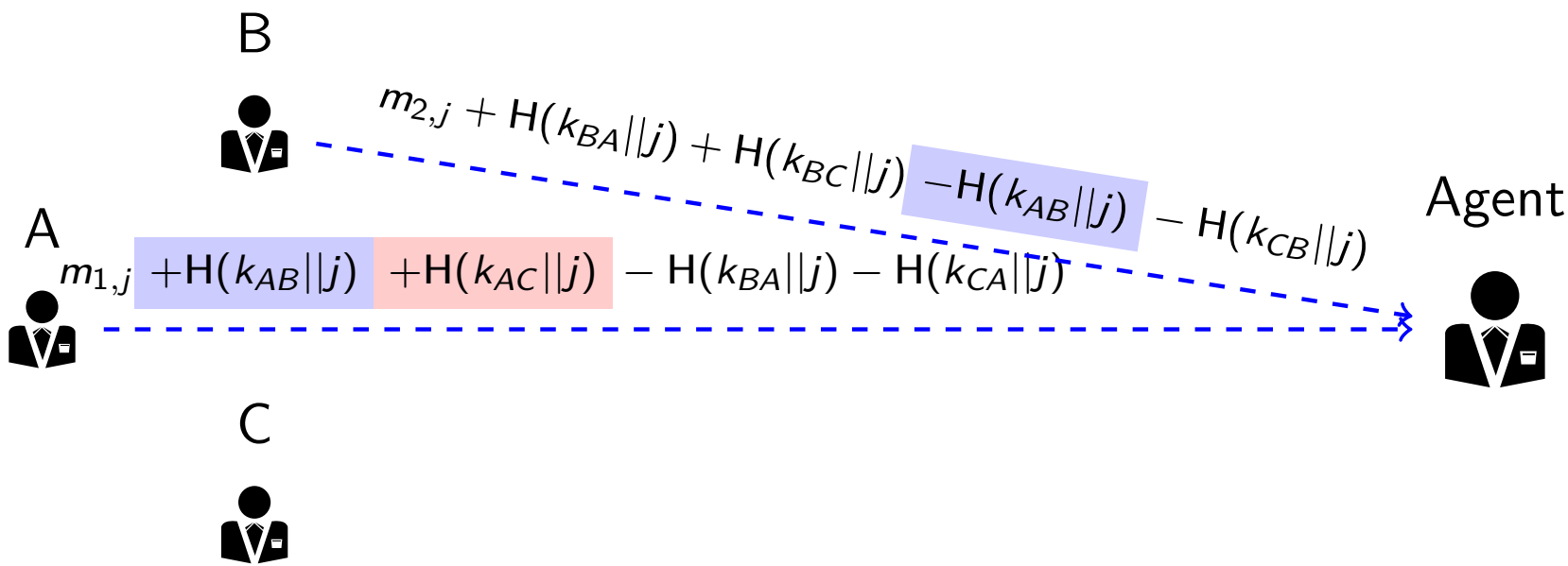
SDC-Nets

[GJ04]



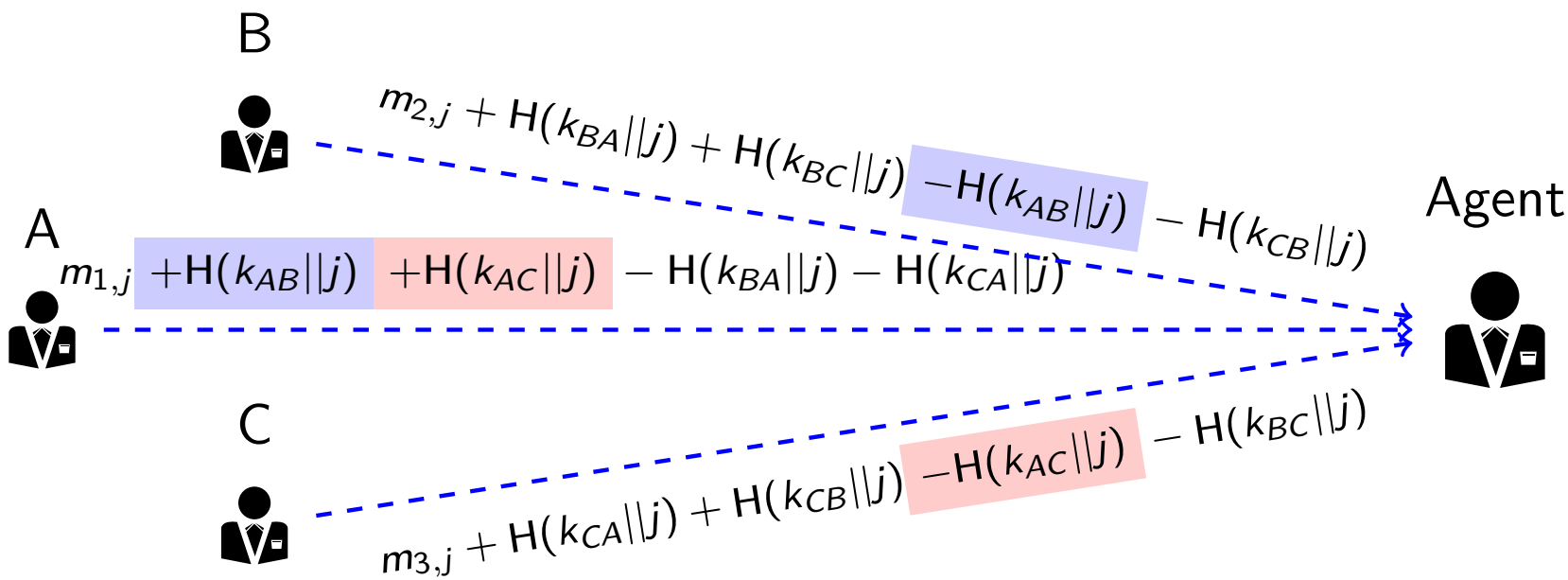
SDC-Nets

[GJ04]



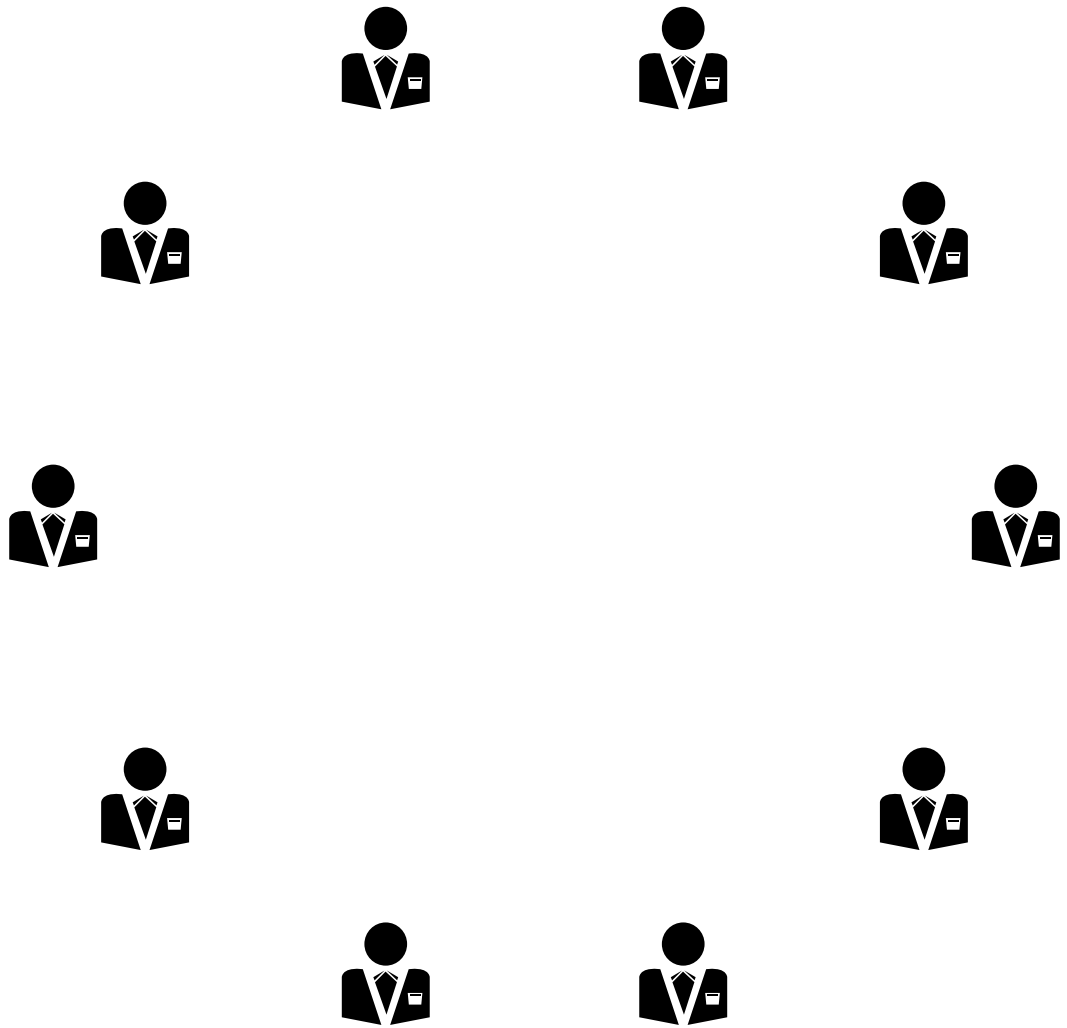
SDC-Nets

[GJ04]



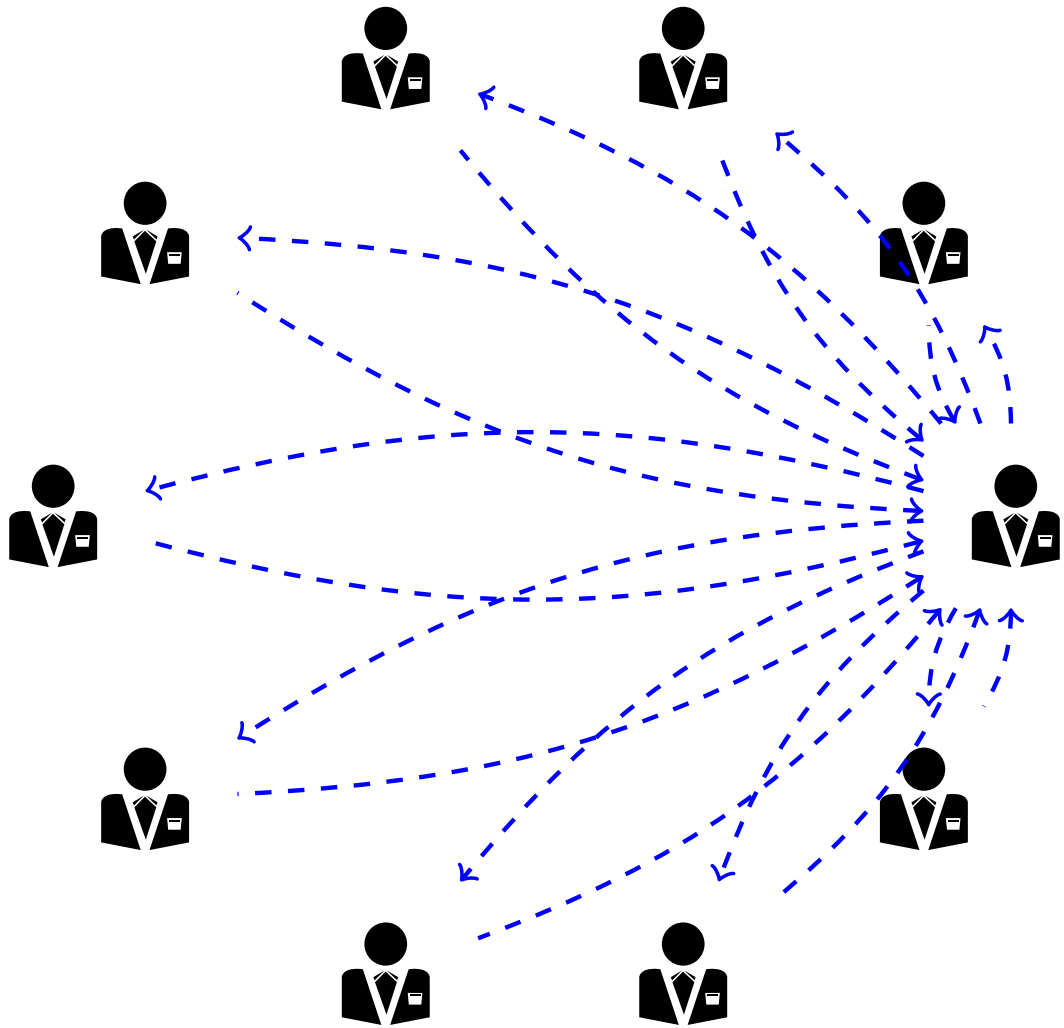
SDC-Net

Keys for 10 users



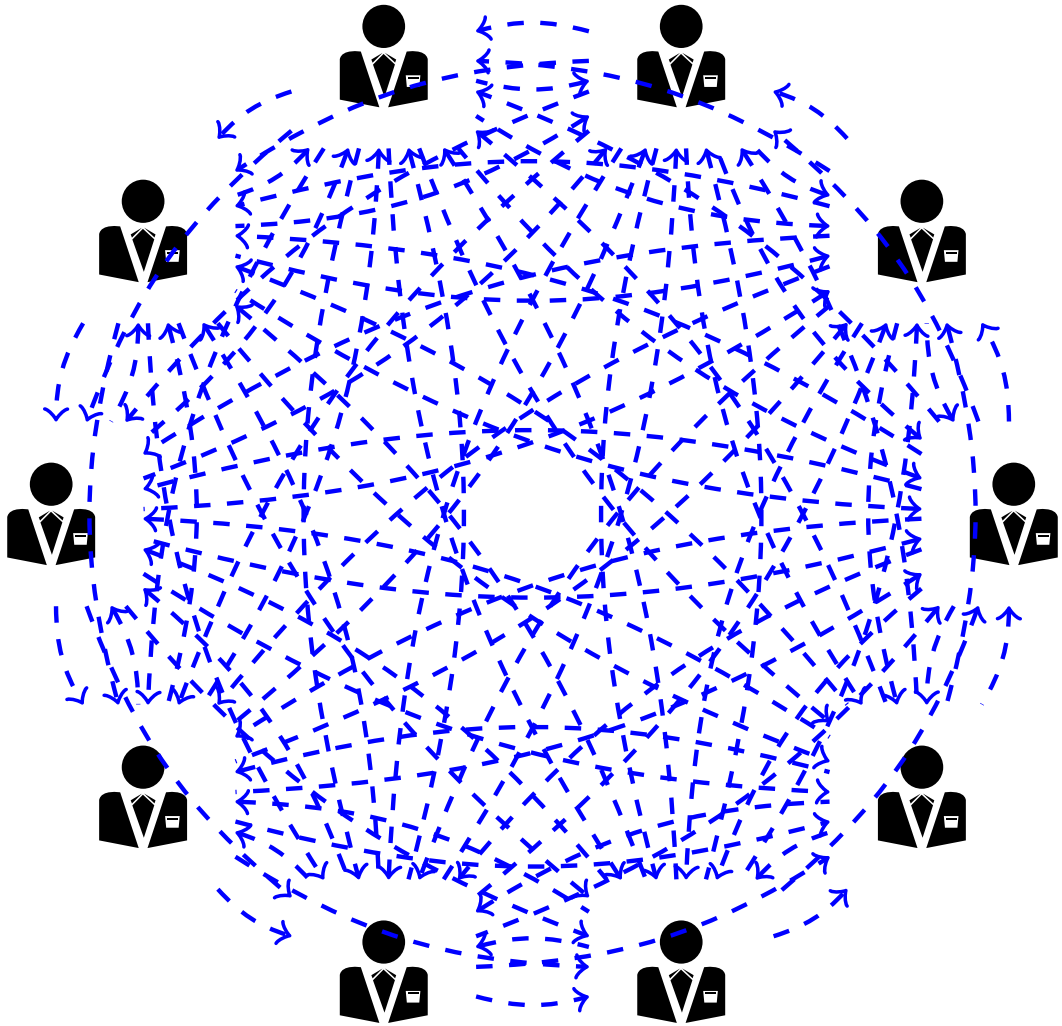
SDC-Net

Keys for 10 users



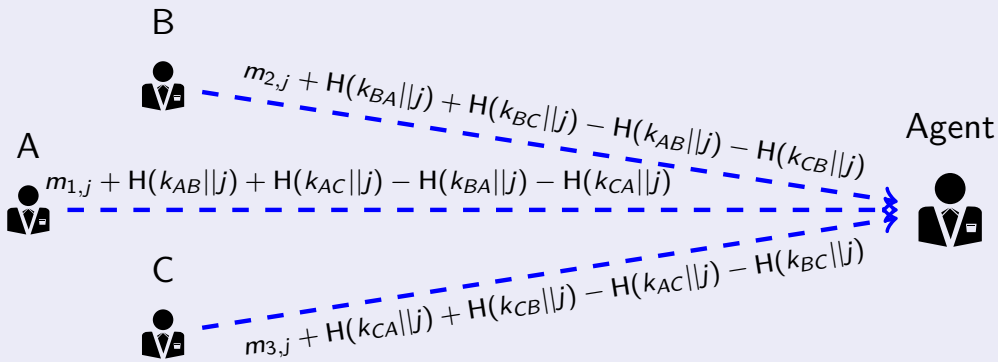
SDC-Net

Keys for 10 users

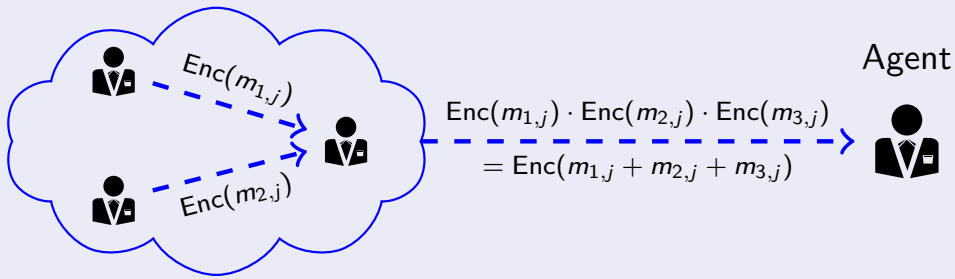


SDC-Nets versus AHEPs

Symmetric DC-Nets (SDC-Nets)



Additive homomorphic encryption primitives (AHEPs)



ADC-Net

Required Properties [BBM14; BM14b; BVM15]

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	✗	✗	

ADC-Net

Required Properties [BBM14; BM14b; BVM15]

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	✗	✗	✓

Interesting Results

Beyond the State of the Art

Result:

Asymmetric DC-Nets are abstractions of Symmetric DC-Nets

[BBM14]

Interesting Results

Beyond the State of the Art

Result:

Asymmetric DC-Nets are abstractions of Symmetric DC-Nets

[BBM14]

Result:

AHEPs are particular cases of ADC-Nets

Interesting Results

Beyond the State of the Art

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

CSR
LNCC

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security

Introduction to PPP

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

Dataset

Raw Dataset ✗

The raw dataset has inconsistencies

Dataset

Raw Dataset ✗

The raw dataset has inconsistencies

Sanitized Dataset ✓

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

Dataset

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

Comparison of requirements

between Privacy-Preserving Protocol (PPP)

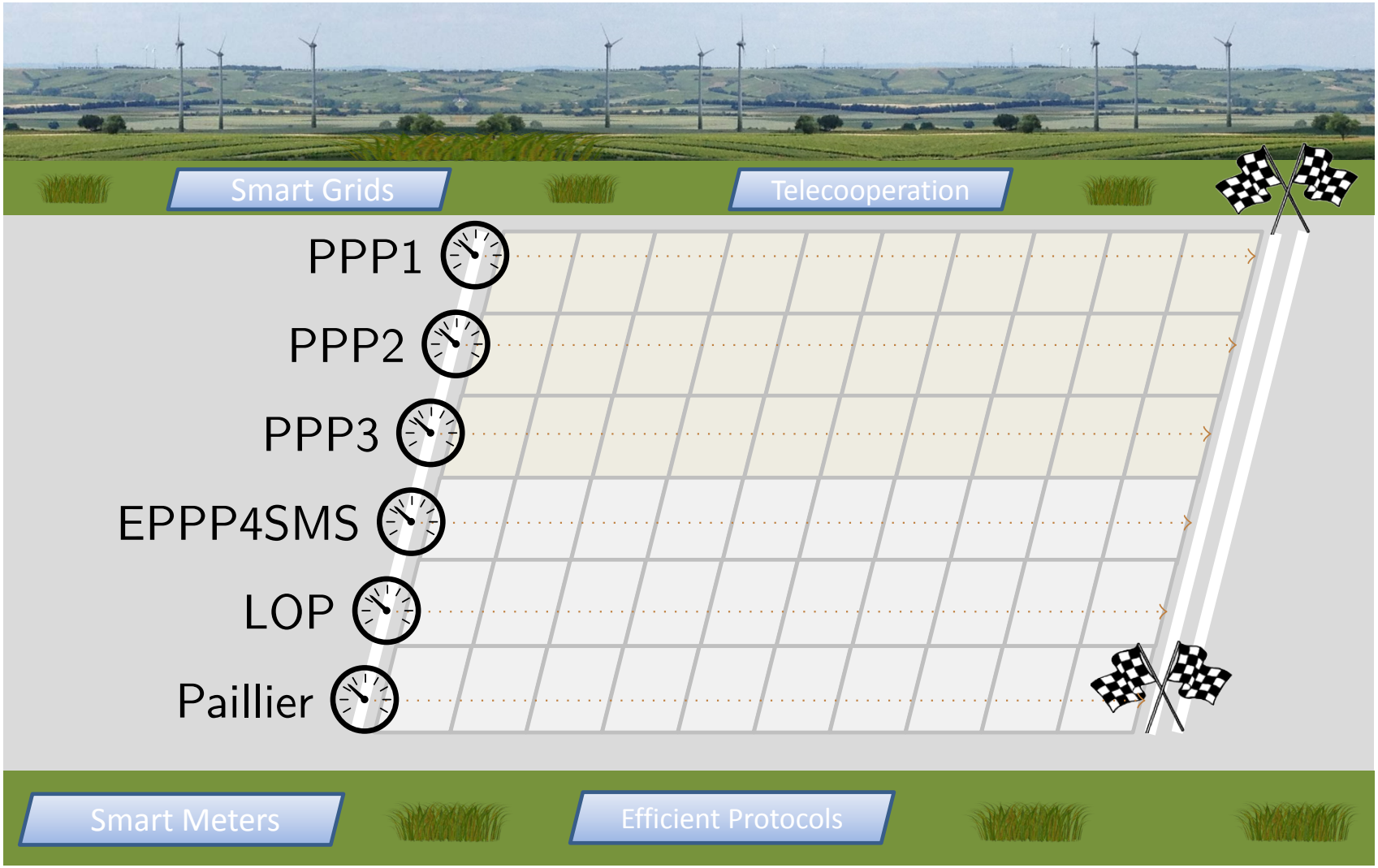
Protocol				Efficiency		
				Enc	Agg	Dec
PPP1	✓	✗	✗	$O(1)$	$O(\tilde{i})$	$O(\tilde{i})$
PPP2	✗	✓	✓	$O(\log(k))$	$O(\tilde{i})$	$O(k)$
PPP3	✓	✓	✓	$O(\log(k))$	$O(\tilde{i})$	$O(\log(k))$
EPPP4SMS	✓	✓	✓	$2O(\log(k))$	$O(\tilde{i})$	$O(\log(n))$
LOP - SDC-Net	✓	✗	✗	$O(\tilde{i})$	NA	$O(\tilde{i})$
Paillier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

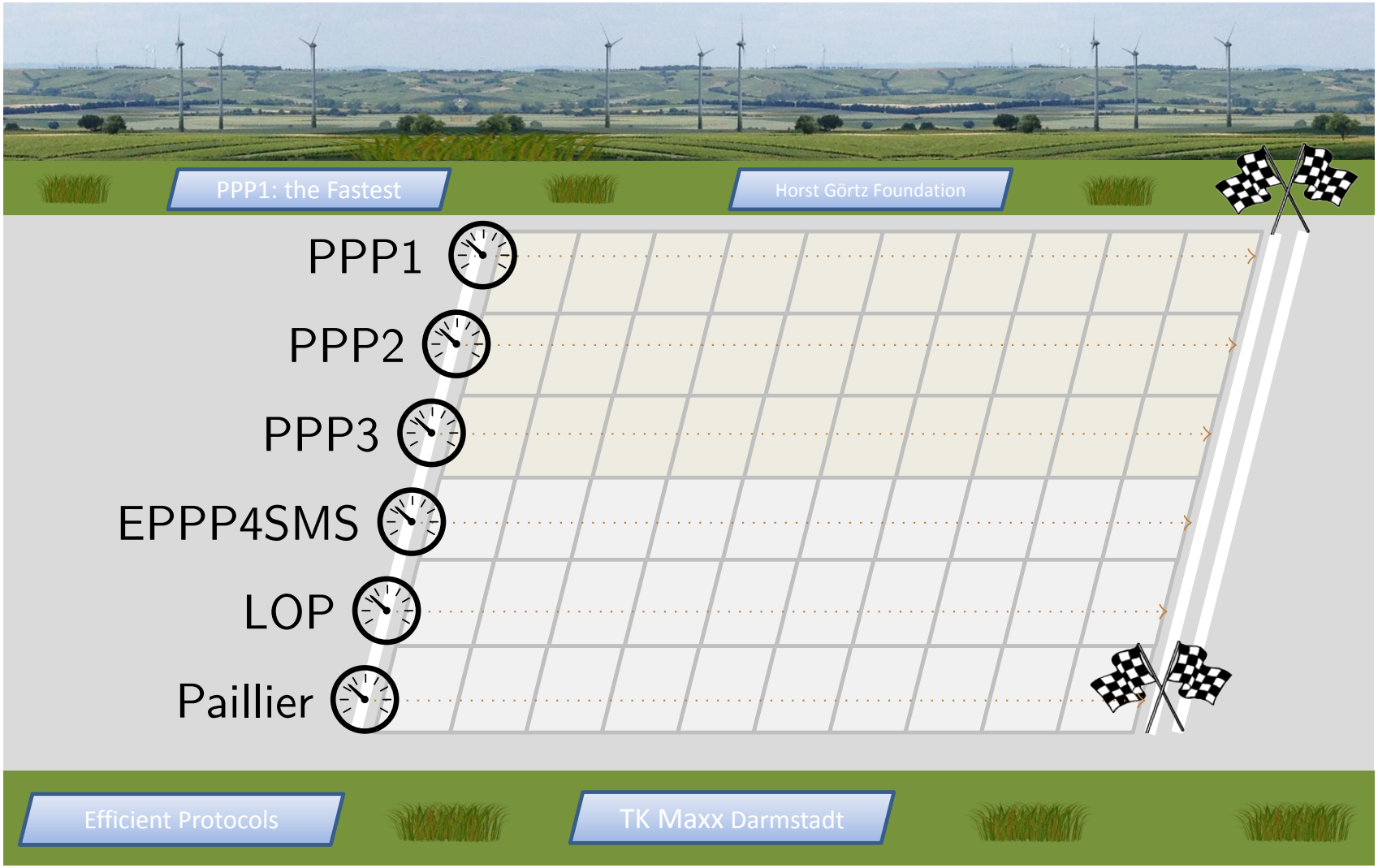
Overall Performance

Race protocols



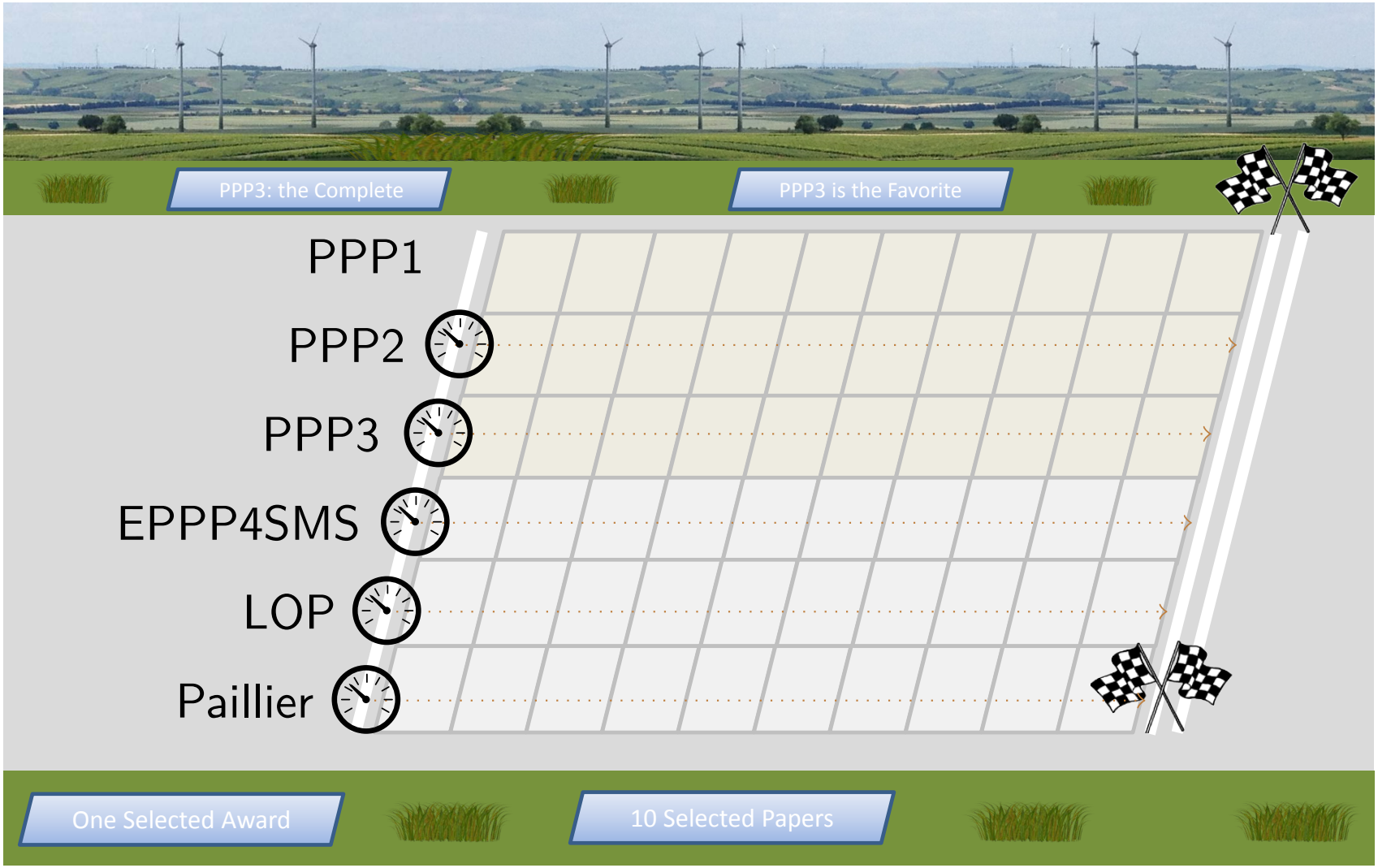
Overall Performance

Race protocols



Overall Performance

Race protocols



CSR
LNCC

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security

Introduction to PPP

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

Conclusion

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

Conclusion

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

Conclusion

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

Conclusion

- 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

Conclusion

- 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

Selected Publications

Journal Papers

[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

Selected Publications

Award

[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

Selected Publications

Conference Papers

[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 - congrasso 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

Outlook

ADC-Nets can be used in applications that require:

- SDC-Nets

Outlook

ADC-Nets can be used in applications that require:

- SDC-Nets
- AHEPs

Outlook

ADC-Nets can be used in applications that require:

- SDC-Nets
- AHEPs
  - electronic voting

Outlook

ADC-Nets can be used in applications that require:

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

Outlook

ADC-Nets can be used in applications that require:

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

Outlook

ADC-Nets can be used in applications that require:

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

Outlook

ADC-Nets can be used in applications that require:

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

Outlook

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

Outlook

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

CSR
LNCC

Thank You!

TECHNISCHE UNIVERSITÄT DARMSTADT

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

Contributions

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

CSR LNCC

Bibliography I

TECHNISCHE UNIVERSITÄT DARMSTADT

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.

Bibliography II

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.

Bibliography III

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.

Bibliography IV

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.