**Master's Thesis**

# Privacy-preserving Smart Metering Using DC-Nets

Gregor Garten

December 26, 2021

TU Dresden
Faculty of Computer Science
Institute of Systems Architecture
Chair of Privacy and Data Security

Supervisors: Dr. Stefan Köpsell
Dr. Elke Franz
Betreuender Mitarbeiter: Dipl.-Inf. Tim Lackorzynski

# Lorem Ipsum

## Selbständigkeitserklärung

Hiermit erkläre ich, dass ich diese Arbeit selbstständig erstellt und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Dresden, den **?today?**

Gregor Garten

**Abstract**

. . . abstract . . .

write abstract

# Contents

# Todo list

# List of Figures

# List of Tables

# 1 Introduction

adopt title page

adopt disclaimer

write introduction

## 1.1 A Section

Referencing other chapters: 2 3 4 5 6 7

| Name | Y | Z |
|---|---|---|
| *Foo* | 20,614 | 23 % |
| *Bar* | 9,914 | 11 % |
| *Foo + Bar* | 30,528 | 34 % |
| *total* | 88,215 | 100 % |

Table 1.1: Various very important looking numbers and sums.

More text referencing Table 1.1.

## 1.2 Another Section

Citing [**bellard2005qfa**] other documents [**bellard2005qfa**; **boileau06**] and Figure 1.1. Something with umlauts and a year/month date: [**becher04:˙feurig˙hacken˙mit˙firew**]. And some online resources: [**green04**], [**patent:4819234**]

## 1.3 Yet Another Section

add content

## 1.4 Test commands

DROPS L$^4$LinuxNOVA QEMU `memcpy` A sentence about BASIC. And a correctly formatted one about ECC.

Figure 1.1: A long description of this squirrel figure. Image taken from `http://commons.wikimedia.org/wiki/File:Sciurus-vulgaris_hernandeangelis_stockholm_2008-06-04.jpg`

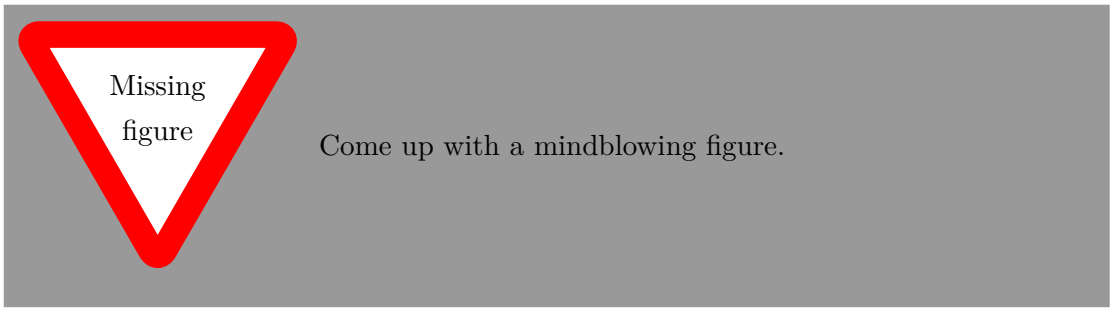


Figure 1.2: A mindblowing figure

# 2 Technical Background

This section introduces an overview of the basic concepts for this work. Therefore, the key components of the smart grid are explained, what structural changes and what challenges the smart grid will bring. In addition, this chapter discusses the current state of research.

## 2.1 Smart Grid

The original energy network was mainly considered as a transmission system to send electricity from the generators via a elongated network of cables and transformers to the consumers.Instead of a few electricity producers (e.g. nuclear power plants, coal-fired power plants), which were responsible for a large part of the electricity generation, there are now many smaller producers (e.g. wind turbines). However, renewable power generation is often dependent on external environmental factors. In order for the smart grid to be stable despite fluctuations in power generation, smart meters have been introduced. This enables the electricity provider to receive the electricity consumption of a household every 15 minutes. It offers the possibility to get more easily the current electricity demand from the consumers. Previously, the current electricity demand was simulated from load forecasting models. If the demand should increase spontaneously, peaker plants, mainly consisting of coal-fired power plants, would be turned on to quickly meet this demand. This is costly and environmentally unfriendly. Since then, structural changes have been made to optimize the energy grid and make it more intelligent by exchanging information in near-real-time. This allows the demand to be matched to the available supply. The fundamental component of the smart grid are the smart meters, which were already mentioned. They which will be discussed in more detail in the next section.(Quelle:Smart Grid Communications)(Privacy Survey2013)

## 2.2 Smart Meter

Smart meters are the key component in a smart grid. A smart meter is an electricity meter that has an interface to the Internet. It enables two-way communication between the control center and the meter. This is also called Advanced Metering Infrastructure (AMI). Two-way communication improves the quality of the power grid and makes it possible to offer services that would not be feasible without a smart meter. For example it's now practicable to detect power outages.As a result, the power grid operator can detect power failures on its own. Previously, the operator was dependent on customer calls to detect power outages. Another new feature is detailed monitoring of power

flows at the smart meter. Before, power flows could only be measured up to substations. This new function enables electricity network operators to quickly detect changes in consumption behavior and react to them without having to use peaker plants, which are costly and environmentally unfriendly. Depending on the setting, smart meters can send electricity consumption to the electricity provider at least every 15 minutes. In combination with the consumption of all users and the current electricity supply, a better price can be achieved. This is also called real-time pricing. So not only can the customer be offered a better electricity contract, in addition the meters no longer have to be read at home by a technician from the electricity provider. This makes billing easier for customers and electricity providers. Furthermore, customers can also check their current electricity consumption via the interfaces provided by the smart meter in order to analyze their own behavior and to reduce their consumption. (Privacy-Aware Smart Metering)

## 2.3 Smart Meter Privacy

The main advantage of the smart grid is the communication between the consumers and the energy suppliers. It is precisely this communication that solves a lot of structural problems in today's energy system. However, sending user information every 15 minutes allows for new methods that can be used to create accurate behavioral analyses in one's own home. Sending private electricity consumption data is therefore very sensitive information and must to be protected. This is not an easy task, because on the one hand the electricity consumption must be protected and anonymized, and on the other hand the billing and costs must be clearly assignable to a person. In the following paragraphs, we will describe how simple behavioral analyses are generated by electricity consumption. Subsequently, solutions to Metering for Billing and Metering for Operations will be presented, which have been discussed in the scientific community so far.(Privacy-Aware Smart Metering)

### 2.3.1 Non-intrusive load monitoring

Interpreting power consumption with the intent of identifying devices in the home is called non-intrusive load monitoring (NILM). George Hart and Fred Schweppe were the first to develop non-intrusive load monitors in 1985 and connect them to electricity meters. They were able to record the current power consumption up to every 5 seconds. Then they did the following steps to identify appliances in a household:

1. Edge Detection:
   Look for sharply rising or steeply falling edges in the stored electricity consumption. These edges indicate that a device may have been switched on or off at that moment.

2. Cluster Analysis:
   The events of steeply rising or steeply falling edges are saved. These events are then visualized in a graph with the following characteristics. Each event is ordered

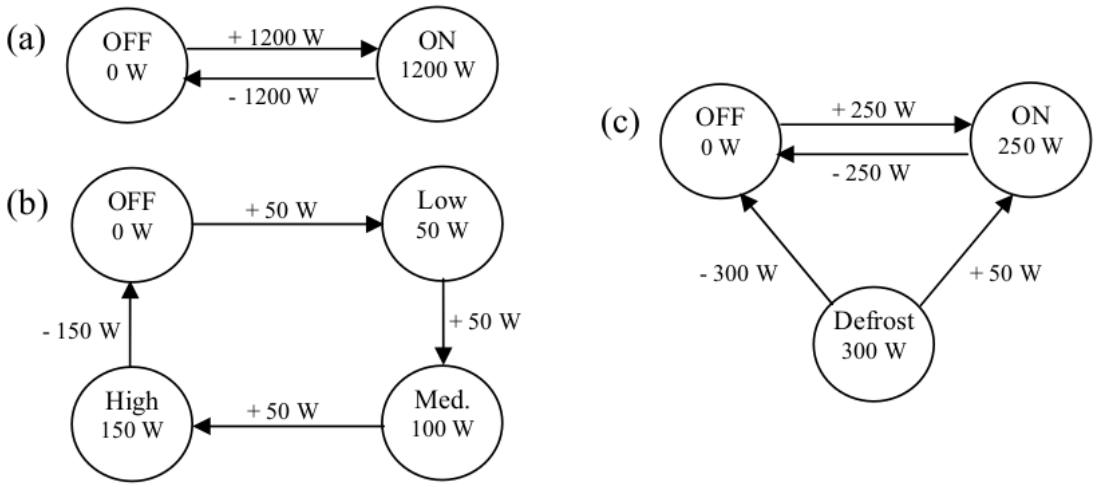


Figure 2.1: An example of a NILM analysis.

according to how much power was consumed or how much power was "released" from the device (e.g. when it was switched off). Essentially, a cluster analysis is then applied to the diagram and each cluster represents a household appliance.

3. Appliance Model Construction
   Since different household appliances have been determined by the clusters, appliance models can now be constructed. In this step, different states in which an appliance can be in, are found based on the different power consumption. An example of how the result of a appliance model looks like can be seen in Figure 2.1.

4. Behavior Analysis:
   Once the majority of the household appliances have been identified, the behaviors of people in the household can be analyzed. In real time, it is possible to track the use of devices, since individual signals can be identified as they occur and do not need to be reconstructed anymore. At this point, several approaches can be taken to provide behavioral analysis. A common approach is to track how long a device has been in use and create statistics on how each device has been used. A daily analysis can be viewed in Figure 2.2.

5. Appliance Saving:
   The last approach is to name the household appliances found(washing machine, etc.) and store them in a database. So that in the case of a further household analysis, it is possible to fall back on appliances that have already been found.

The founder of NILM G. W. Hart himself said in 1989: "Specifically, I recommend that legal restrictions be enacted or clarified so that electric power usage is considered as private as any phone conversation."(Residential Energy Monitoring) Hence, there is a need for a privacy-preserving solution for smart meters. Although the original NILM approach measured power consumption every 5 seconds, there are now methods to

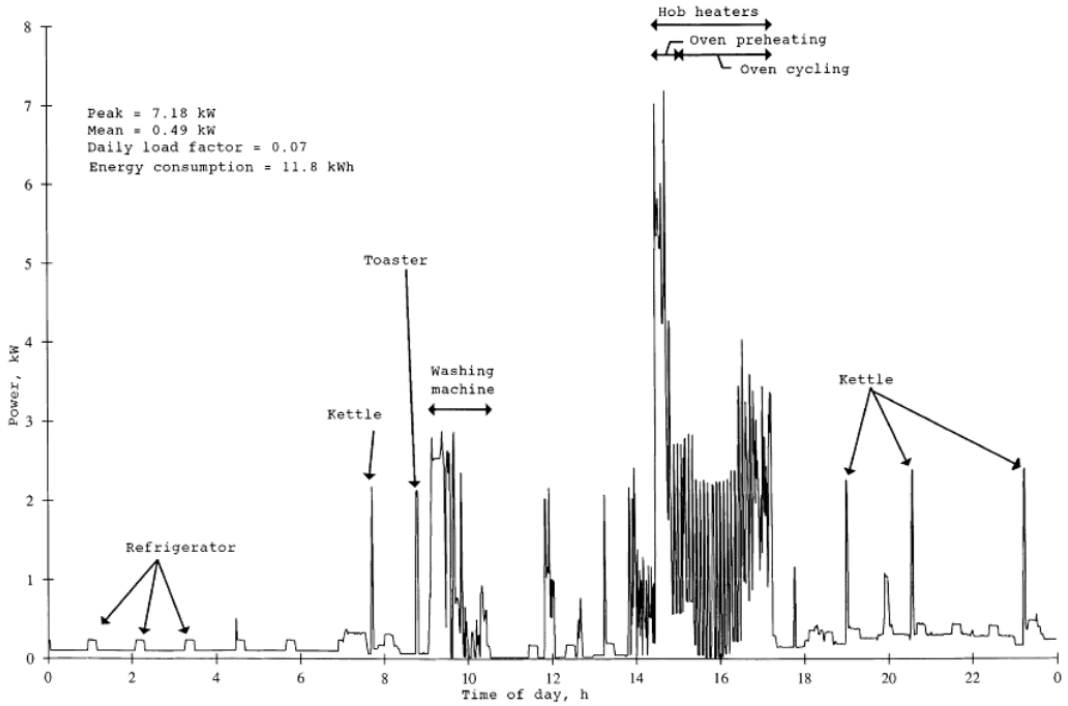


Figure 2.2: An example day of a NILM analysis.

identify household appliances when power consumption is measured every 15 minutes.(A Neuron Nets Based)

### 2.3.2 Metering for Operations

The paragraph deals with solutions for Metering for Operations, which has been previously discussed in other scientific works. At Metering for Operations, there is currently no established consensus on a solution. Various technical proposals have already been presented in scientific papers, but there is a lack of uniform criteria and often different conditions are set for the power grid. One reason for this could be that smart grids are realized differently in other countries. In the following, the different approaches are divided into categories and presented conceptually.

#### Anonymization or Pseudonymization Without Aggregation

This approach describes the removal of smart information that allows identification. Identifiable information can also be replaced by pseudonyms. Solutions with trusted third parties are often used in this case. A trusted third party usually acts as an intermediary between the customer and the power grid provider. The trusted third party must be acknowledged by all participants and take a neutral position. In practice, however, this is difficult to achieve because the trusted third party is often hired as a service provider by the electricity supplier and is therefore also paid by the supplier.

In the paper "A privacy-preserving Concept for Smart Grids" by Petrlic[quelle], a trusted third party is used as an intermediary. In the proposal, a smart meter communicates with a trusted third party. Certificates formed with a public key infrastructure can be used to verify and validate information flows from smart meters at the TTP. As soon as the Trusted Third Party has checked the correctness of the smart meter information, it can pseudonomize/anonymize all the necessary information. Only then is the further processed anonymized information forwarded to the electricity provider by the TTP in encrypted form. This means that the electricity provider cannot assign individual electricity consumption to its customers. With this procedure, smart meters can be anonymized. However, if it is possible for an attacker to record the data traffic between the smart meter and the TTP, then the attacker could forward the time stamps and smart meter identification to the electricity provider. Using these two pieces of information, the electricity provider could at least gain some insight, since it would be possible to match when information is sent to the TTP and when it is received by electricity provider.(Privacy-Aware Smart Metering)

**Aggregation with Trusted Third Parties**

In the attack just described, the electricity provider tries to link two events. One is the arrival of the message at the TTP and the other is the arrival of the message at the provider itself. One way to prevent this attack is aggregation. In this case, the smart meter sends its electricity consumption to the TTP. Certificates are also sent from the smart meter so that the TTP can check the information for correctness and authenticity. Instead of forwarding the information to the electricity provider, the TTP waits until all smart meters have sent their data for which the TTP is responsible. This data is all added up and a message is sent from the TTP to the electricity provider with the total electricity consumption of all smart meters. From the aggregated value, it is not possible to extract an individual smart meter's electricity consumption, which is why the electricity provider cannot filter out information about individual customers.(A Privacy Model for Smart Metering)
Homomorphic encryption approaches also fall into this category. Homomorphic encryption algorithms allow simple operations such as addition and multiplication to be performed on the encrypted messages. In some homomorphic encryption schemes, only addition OR multiplication are supported. These are then called partial homomorphic encryption. There are also bihomorphic encryption approaches. Here not only the operations on the ciphertexts are homomorphic, but also the operations on the keys. This means that if a plaintext a is encrypted with the key x and a plaintext b is encrypted with the key z, that one can decrypt the ciphertexts enc(a+b) with the keys x+z. A bihomomorphic encryption approach with TTP has been proposed by Vetter et al.[quelle] In this case, the TTP acts as the key authority. This means that it creates all cryptographic keys and forwards them to the smart meter, which is then used for further communication with a central store. The smart meter encrypts its data and sends it to the central storage. The central storage also stores the incoming data in encrypted form, so that no unencrypted data can be found on the storage. In addition, the central

storage has no access to the keys and thus has no way to decrypt the information or access meaningful data. Therefore, the central repository has to be trusted only in terms of functionality. If an electricity provider wants to know the electricity consumption of its customers, it makes a request to the central repository, which sends the aggregated encrypted data to the electricity provider. In order for the electricity provider to decrypt the data, the key authority has to release the correct keys. It is impossible for the electricity provider to query the value of just one smart meter. This is because the key authority can only issue keys that can decrypt aggregated totals. It is guaranteed by the homomorphic encryption method which is used. The advantage of using this approach is that the different functionalities, namely storage of data and key acquisition for confidentiality and authenticity is realised from different participants.(Privacy-Aware Smart Metering)

**Aggregation Without a Trusted Third Party**

The solution proposed in this thesis is also one of the methods that aggregate without a trusted third party. The advantage of this approach is that no one has to trust a trusted third party. In general, one has to ask the questions who aggregates the data and who generates/uses the keys. In addition, a common problem to consider is how the procedure deals with a few participants/customers.
In the solution of Mármol et al. again a bihomomorphic encryption method is proposed. The approach of Mármol has already been discussed and implemented in a master thesis at this chair.[quelle biselli] As a reminder, bihomorphic encryption algorithms can perform simple operations such as addition on both the ciphertext and the keys. This property is exploited in the presented method of Mármol. Since it aggregates the keys and not the power consumptions as before. Furthermore, it does not matter which bihomomorphic encryption method is used, as long as all smart meters agree on one method. A key is generated from every smart meter in the power grid. Afterwards, the key is used to encrypt the power consumption. The key is then used to encrypt the electricity consumption and the encrypted data is sent to the network operator. The transmission channel to the network operator is chosen in such a way that the identity of the smart meter remains secret. This prevents the smart meter from exposing itself during communication with the operator. Groups are formed among smart meters and a smater meter aggregator is selected in each group. The aggregator is selected randomly and all smart meters send their keys to this aggregator. Subsequently, the keys are summed up at the aggregator and sent to the network operator. The network operator receives a single key and with this key it can only decrypt the messages from one smart meter group. additionally, the operator has to add up all the messages and only then it will be possible to decrypt the messages. There is a possibility that aggregator cooperates with the network operator. The aggregator would then be able to send individual keys from smart meters to the operator. While the operator would not be able to match the key to any message, by brute force it could decrypt all messages with that key and see which decrypted message has meaningful content. To prevent this attack, an additional measure is taken. All smart meters in a group organize themselves topologically in a ring structure. In this ring structure, all smart meters cooperate with each other


Figure 2.3: The power consumption of a household in a day with battery.

and change their keys every round in such a way that the individual key of a smart meter changes, but not the summed key of all smart meters. Even if the aggregator forwards the keys to the network operator, they would no longer be valid in the next round.(nochmal nachlesen, warum nicht eine individuelle Nachricht entschlüsselt werden kann) A disadvantage of this procedure is that if a smart meter leaves the group, then a new aggregated key must be formed.(Privacy-enhanced architecture for smart metering)

### Battery Solutions

The battery approach describes a household with a connected battery that is charged, e.g. by grid purchase or photovoltaic panels. The goal of the approach is that the battery feeds energy into the household in such a way that the grid operator can no longer detect private information based on the electricity consumption.

The figure shows the electricity consumption of a private household with a connected battery that is charged via solar panels. It can be seen 3 lines. The red line shows the electricity consumption of the household. The green line shows when the battery is discharged(when the battery is feeding power to the household). The blue line is the power consumption that the grid operator can see.In the figure you can see that when the battery brings electricity to the household, then grid operator sees that a household does not consume electricity. In other cases, the grid operator sees that electricity is

being consumed, but it is much less than the house actually consumes because the battery offsets some of the electricity consumption. In other words, if a household is connected to a battery, the grid operator cannot make correct statements about the behavior of the people in the household.
An algorithm for batteries was proposed in(Protecting consumer privacy from electric load monitoring). This method uses an algorithm that can control the battery to produce a constant characteristic curve in consumption. The algorithm targets a static and fixed current consumption. The target consumption is calculated differently by the algorithm depending on the house consumption and battery capacity. If the power consumption is below the consumption set by the algorithm, then the battery is charged with the difference from the target consumption. If the power consumption is above the target consumption set by the algorithm, the battery is discharged with the difference from the target consumption. If the consumption is significantly higher, so that the battery can no longer absorb the additional consumption, then it is switched to recovery mode. In recovery mode, the target consumption is temporarily increased, so that the battery can charge on the side, even though the house is currently consuming a lot of power. If the recovery mode can be switched off, then a new target consumption is calculated based on the new data. It is important to remember that this method does not anonymize power consumption, so it is even more important to measure how much information can still be extracted from power consumption. There are the following metrics to calculate how much privacy is gained by the algorithm.

1. Relative Entropy:
   Relative entropy is used to compare two sources of information. In this case it would be the power consumption with the algorithm and the power consumption without the algorithm. These two loads form a stochastic process and can then be compared with the relative entropy. (Affordable privacy for home smart meters)

2. Cluster Classification:
   The cluster classification has already been explained for the NILM method and described in this paper at [ref]. The cluster classification has already been explained for the NILM method and described in this paper at [ref]. It can also be used as a metric to evaluate privacy. Here one would perform a cluster analysis with the battery method and once without. Then one looks at the number of clusters in both measurements and if fewer clusters are found with the battery method, then this is considered a privacy gain.

3. Regression Analysis:
   In the regression analysis, first a cross-correlation and afterwards a simple linear regression is performed. More precisely, both power consumptions are ”superimposed” at the point of their maximum cross-correlation. Subsequently, a linear regression is performed and the privacy is evaluated on the basis of the quality of the predictor.

### 2.3.3 Metering for Billing

In order to fully protect the privacy of a household, metering for billing procedures must also be applied. Otherwise, conclusions about electricity consumption can be drawn from the billing. A simple solution would be to increase the frequency of the billing period. But at the same time it is also in the interest of the customer to buy electricity as cheaply as possible. The customer can be offered better electricity contracts if the billing period is shorter. In addition, it cannot be guaranteed that the customer's privacy is not violated in more complex electricity contracts by other features, even if a higher billing period is used. In the following paragraph, different methods are explained that solve the problem for metering for billing.

#### Billing with a Trusted Third Party

The advantages and disadvantages of a TTP have already been explained in the upper section. The principle is similar to metering for operations. The smart meter sends its measurements to the TTP and the TTP calculates the bill over the time period specified in the electricity contract. The billing is then sent to the electricity provider. On paper, this approach is simple, but important practical questions often remain unanswered. For example, who pays the trusted third party? In this case, the trusted third party provides a service to the electricity provider. However, if the electricity provider pays for the service, then the trusted third party is no longer independent.

#### Billing with a Trusted Platform Module

Billing can also be implemented on the smart meter with a Trusted Platform Module. A TPM is a chip that is installed within the smart meter and thus additional security features can be used on the smart meter. The TPM contains a cryptographic processor that can generate random numbers, generate RSA keys, generate SHA-1 hashes and it has an encryption-decryption-signature engine. In addition, the TPM can be used to prove that nothing has been tampered with the smart meter afterwards. A secured smart meter can therefore perform correct billings at the customers side and the electricity provider can trust the smart meter. However, the TPM is installed by the electricity provider and it only guarantees the validity of the billing. If the electricity provider decides to send additional sensitive information within the calculations in the TPM, the TPM has no advantage for the end user.(Privacy-Aware Smart Metering)

#### Billing Secured via Cryptography

Lastly, there is the cryptographic commitment method. With this approach, no other participant needs to be trusted. A smart meter can use a cryptographic commitment to prove that each bill was calculated correctly. So with cryptographic commitments, billing can be done on the customer side.
Lastly, there is the cryptographic commitment method. With this approach, no other participant needs to be trusted. A smart meter can use a cryptographic commitment

to prove that each bill was calculated correctly. So with cryptographic commitments, billing can be done on the customer side. A commitment is a cryptographic application and works as follows. Both sides agree on the same commitment procedure. Then it is possible that one side can generate a c=(x,r) as an obligation. Here x would be the calculation and r would be a random number. If one wants to check the commitment for correctness, then there is an Open(c,x,r) function that returns True(if correct) or False(if incorrect). Cryptographic commitments are mathematically constructed so that it is easy to compute a c=(x,r), but hard to find an x /= x' with an r' such that open(c,x',r') returns True. In this use case, the following procedure is often used. [pedersen]
Commit(x, r) · Commit(y, s) = Commit(x+y, r+s)
$Commit(x, r)k$ = Commit(x · k, r · k)
The special feature of the method of [pedersen] is that at the same time non-homomorphic properties are satisfied. Without going into exact technical details, cryptographic commitments work as follows in a smart grid. The smart meter generates a cryptographic commitment for each measurement. Via a public key infrastructure, the smart meter and the electricity provider receive cryptographic keys. With these keys, the smart meter can sign its commitments and then send them to the electricity provider. The electricity provider checks the commitments for correctness and if all data is correct, the electricity provider sends back a list with electricity prices and the corresponding time stamps. The meter now knows at each point in time how much electricity was consumed and what the price was. By exploiting the homomorphic properties of the procedure, the smart meter can now calculate the electricity prices. The electricity price in this case would be the variable k.So the smart meter creates new cryptographic obligations with the electricity price calculated on the consumption and sends these new obligations to the electricity provider. The electricity provider can verify the correctness by performing the same calculations as the smart meter. If the results with the Open(c,x,r) method return true, then the calculations were performed correctly by the smart meter. This method is suitable for simple electricity tariffs when only a factor on the electricity consumption needs to be calculated. If an electricity contract is more complex with different conditions such as a higher electricity price if a certain electricity consumption is exceeded, then this approach can no longer be implemented.

write state

# 3 Design

This chapter outlines the conceptual solution of this thesis to achieve privacy-preserving smart meters. The proposed protocol can be categorized as aggregation without a trusted third party. Before discussing the conceptual solution, the technical guideline from the BSI will be explained. The BSI is the cyber-security authority of the German government and is responsible for critical infrastructures such as smart grids in Germany. The technical guideline TR-03109 resolves all security standards and security concepts that must be met by all power grid providers in Germany. Therefore, the technical guideline gives a good overview of the actual structure of the German power grid. After getting an overview of the power grid and its participants, an attacker model will be designed. The attacker model will introduce all necessary participants, what their motives are and what malicious motives they might pursue. Finally, the security protocol will be presented. It will be shown how the protocol can be integrated into the technical policy and how different potentially malicious participants are handled.

## 3.1 Technical guideline TR-03109

This paragraph will discuss the technical guideline published by the BSI (Federal Office for Information Security). The BSI is the entity of the German federal government that deals with digital security issues and issues recommendations as well as mandatory security guidelines for critical infrastructures. Among other things, technical guidelines are published in which security standards are defined for different IT systems. The technical guideline BSI-TR-03109 defines minimum requirements for the functionality, security and interoperability of smart meters in Germany. The technical guideline BSI-TR-03109 defines minimum requirements for functionality, security and interoperability that individual components of smart meters in Germany must fulfill. The guideline as a whole consists of 6 different documents, which are shown in Figure 3.1. Based on the guidelines, it is possible to have devices certified by test centers. Unless otherwise described, all information are derived from the technical guideline.

**Actors on the SMGW**

1. Consumer:
   The consumer is the person who uses electrical energy, gas, water or heat. In addition, the consumer is the owner of the measurements processed and stored in the SMGW. In order to interact with the SMGW, the consumer uses a

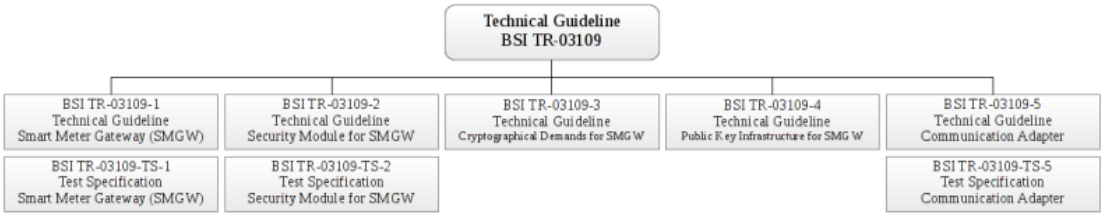


Figure 3.1: An example of a NILM analysis.

communication device. All necessary data can be retrieved and displayed through it.

2. SMGW administrator:
   A Smart Meter Gateway Administrator (GWA) a trusted entity and each SMGW is assigned a GWA. The GWA handles the configuration, monitoring and control of SMGWs and it is even possible to perform updates of SMGWs via the GWA.

3. Authorized external entities:
   External market participants (EMT) are all other authorized participants in the energy network that can establish a communication connection with the SMGW.These include power grid providers and electricity suppliers. The SMGW ignores all other communication requests that do not come from the GWA or EMTs in order to prevent attacks.

There are several other actors such as Controllable Local Systems, service technicians and meters. However, these actors do not play a major role in the protocol that is proposed here.

**Interfaces and functions of the Smart Meter Gateway**

A smart meter or as described in the technical guideline a smart meter gateway(SMGW) must provide 3 different physical interfaces.

1. Local Metrological Network (LMN):
   The LMN is the communication interface in which communication takes place with the connected meters for energy and material quantities (electricity, gas). An SMGW can communicate with one meter from one end user or with several meters from different end users. In practice, however, one SMGW is often responsible for one meter. The measured values are sent from the meters via the LMN to the SMGW and stored there.

2. Wide Area Network (WAN):
   The WAN is the only communication interface with which the SMGW can communicate with EMTs or GWAs over the Internet. If a request is made to the SMGW

that was not sent by these authorized participants, then the request is discarded and ignored.

3. Home Area Network (HAN):
   In HAN, an SMGW interacts with Controllable Local Systems (e.g., photovoltaic systems). In addition, users and service technicians can use the HAN interface to display information about power consumption through functions offered by the SMGW.

**Functionality of the smart meter gateway**

First, the task of SMGW is to store the measurements sent by meters from the LMN. Then, the readings are processed in the SMGW and sent to the authorized EMTs in the WAN after processing. An SMGW must also perform the tasks of a firewall and separate the 3 interfaces. It is therefore impossible for an EMT or GWA to make requests to devices located in the HAN or LMN, even if it is allowed to interact with the SMGW over the WAN. Since the WAN interface is the most important interface for this work, it will be discussed in more detail.

**Functions of the SMGW in the WAN**

The tasks performed by the WAN have already been explained in the paragraph above. Now the functions and security mechanisms offered by the SMGW to guarantee secure interaction on the WAN will be described.

1. Transmission of measured values based on evaluation and WAN communication profiles:
   Communication profiles of GWAs are stored in SMGW. The communication profiles determine how the data is processed in the SMGW and forwarded to EMTs.

2. Pseudonymization:
   Data that is not relevant for billing must be pseudonomized for data protection reasons. For this purpose, the unique identification number that each SMGW has is replaced by a pseudonym. Subsequently, the information is not sent directly to an EMT, but is forwarded to the EMT via the GWA. This additionally protects the identity of the sending SMGW.Even if peusodonymization does not allow an SMGW to be directly assigned, the described attack in [ref] and the resulting behavioral analysis is still possible. Since no other security mechanisms are available from the SMGW, the question must be asked whether pseudonymization as proposed in the technical guideline is sufficient.

3. Time synchronization:
   In order for the cost electricity consumption to be calculated correctly, it is essential that the SMGW have an accurate time. For this purpose, the system time of the SMGW is synchronized with the time server of the GWA at regular intervals.

4. Wake-Up Service:
   A GWA is able to force a communication link with the SMGW. This is done

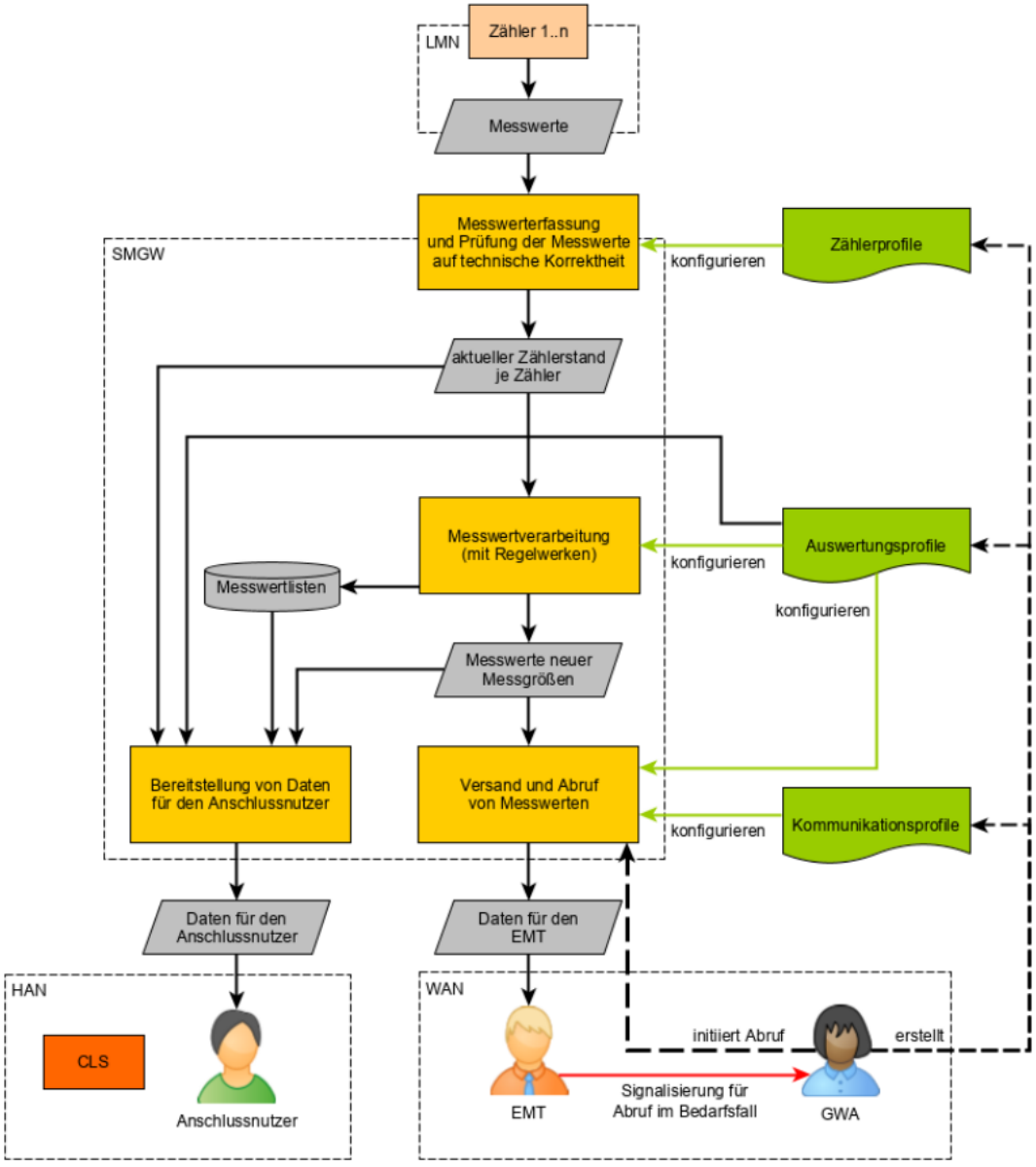


Figure 3.2: An example of a NILM analysis.

via a data packet signed by the GWA. The SMGW then establishes a fixed preconfigured communication connection to the GWA. This enables the GWA to execute administration commands on the SGMW.

## 3.2 Adversary Model

It has already been explained in this chapter which participants in the power grid interact with each other. Now in particular it will be discussed which motives the different participants have and which malicious motives can be pursued by the participants or by attackers.

The smart meter attempts to achieve the 3 security objectives of confidentiality, integrity and availability. The 3 security goals are often summarized as CIA. Another important security goal for this work is anonymity. The 4 definitions are essential for the understanding of this work. Therefore, the terms are explained below.

1. Confidentiality:
   It is not possible for an unauthorized party to gain information about the content of the data sent.

2. Integrity:
   It is not possible for an unauthorized party to modify the content of data without data without this being noticed.

3. Availability:
   It is not possible for an unauthorized party to interfere with the functionality of a service.

4. Anonymity:
   Verbergen der Identität vor dem Kommunikationspartner??? Vllt wer hat die Daten gesendet, wer hat den Stromverbrauch gesendet?

All available attacks will aim at bypassing these security targets to get information about the customer.

### 3.2.1 Customer's Motives

For the costumer, all the security goals defined above are important. But by far the most important is the security goal of anonymity through the smart meter. Possible attacks on the electricity consumption penetrate deeply into the private sphere of each customer. Therefore, no conclusions may be drawn from the electricity consumption of a customer. On the other hand, unethical customers may try to steal electricity to save energy costs. The smart meter is located in or on the customer's house. An unethical customer could attempt to tamper directly with the smart meter's hardware or software. The attempts could look like this, a Costumer could try to reduce the recorded electricity consumption at the Smart meter or the Smart meter could be manipulated to measure less electricity when electricity prices are high and more electricity when electricity prices are low.

### 3.2.2 Electricity Provider's Motives

For the electricity provider, the authenticity of the billing is the most important security objective because From the electricity provider's point of view, the customer is not trustworthy in the calculation of the bill. In addition, the customer has access to the smart meter at almost any time in an environment trusted by the customer. Unlike analog meters, smart meters cannot be mechanically attacked. But if a customer manages to change the software of the smart meter, the billing can be manipulated at the same time. On the other hand, the electricity provider can also be an overly intrusive electricity provider. In the paragraph [Ref NILM] it was explained how a behavioral analysis can be created from the electricity consumption. This sensitive information could be used to gain an additional source of income. In [SSRN] it was listed which questions could be answered by a Nilm analysis. Quote: "On what days and during what times do you watch TV? How much home time do you spend in front of your computer?" or "Are any of the appliances in your household failing or operating below optimal efficiency? Do you own (and so presumably like) lots of gadgets?". Advertising companies would certainly pay money for this kind of information in order to be able to advertise more accurately.

### 3.2.3 Eavesdropping

Eavesdropping may be the weakest type of attack, but successful eavesdropping on the communications of the smart meter could be useful to e.g. intruders. However, curious neighbors might also have an interest in the behavior inside the house. Turning on/off lights implies that someone is at home or leaving the house. Therefore, eavesdropping on electricity consumption could provide information about when is a suitable time to break in. To prevent eavesdropping, smart meter communication is encrypted to maintain confidentiality. Cryptographic algorithms such as AES are widely used today and have been analyzed for weaknesses over the years by a number of researchers. Hence, a successful attack on encrypted data to extract information is extremely unlikely.

### 3.2.4 Active Attackers

In Germany, the smart grid is one of the critical infrastructures. This means that the failure of the smart grid could lead to a significant compromise of public safety or other serious consequences. Such systems are threatened by active attackers. The objective of active attackers may not necessarily be to analyze a user's electricity consumption. They may want to disable availability through e.g. denial of service attacks. These attacks could leave major damage to the power grid and are definitely a realistic threat [quelle]. But this thesis focuses on smart meters and the anonymization of electricity consumption. That's why it is assumed that the active attacker does not carry out system-wide attacks on the power grid. Rather, it is assumed that the attacker attempts to take control in the proposed DC network. Among other things, it is assumed that the attacker has the theoretical ability to take over one or more SMGW and send messages through the SMGW. In addition, if the attacker has taken over an SMGW, it can perform all operations that are possible through the proposed DC network. In the next section, the conceptual solution of the DC-Net is proposed and how the DC-Net could

be implemented in the technical guideline of the BSI. It also describes which attacks on the DC-Net are possible with the defined attacker model.

## 3.3 A Privacy-Preserving Aggregation Scheme Using DC-Nets

In [Cha3-85, Cha8-85, Chau-88], David Chaum proposes a protocol which he calls DC network. The DC network offers the possibility to achieve both sender anonymity and receiver anonymity in communication networks. The operation of the DC network is explained in the following.

### 3.3.1 DC Networks

The DC network uses the property that any finite alphabet can be numerated( e.g a=0, b=1 etc). If an numerated alphabet from 0 is given, then this alphabet forms an abelian group (modulo alphabet size). Because of the abelian group, simple mathematical operations like addition can be performed on the numerated letters in the alphabet. In addition, a DC network assumes that messages are always sent that are of equal length. A participant in a DC network uses one or more keys with which it superposes the messages and one generated key is then communicated to exactly one participant. More precisely, each participant adds locally all key characters it generates. Then, the received keys from other participants are locally subtracted and finally, all meaningful characters (the message) that should be sent are added (modulo alphabet size). The result of the operation is distributed in the communication network and is called local superposition. The distributed superpositions are added together globally and the result is transmitted back to all participants. Thereby only the meaningful messages remain. If a participant does not want to send a meaningful message, the participant sends an empty message. The message consists only of zeros and is superposed with the key. The empty message reflects the neutral element in this structure. If all participants have sent only empty messages, the global result is a message only containing 0. If one of all participants have sent a meaningful message, the global superposition is the message. If more than one participant sent a meaningful message, then the result is the overlay of all sent messages and a single message from the overlay cannot be recovered. In the last case one speaks also of a collision. In order to solve this problem, the collision resolution algorithm with averaging can be used in a DC network. Exchanging keys to calculate the local sum can be very tedious. In addition, a different key must be exchanged for each message round. Otherwise it would be very easy to calculate the key from previously sent empty messages. Therefore, so-called pseudo-random number generators are commonly used. The participants share the initial values of the pseudo-random number generators with each other when they join the DC network. This can be done in the same way as the exchange of keys (e.g. a cryptographic key exchange procedure). Due to the deterministic property of PRNGs, the same sequence of numbers is always generated from an initial value. This in turn means that the initial value must remain secret and must not be revealed to any other participant, since otherwise the secret keys can be found out from the initial value. The consequence would be the loss of anonymity. The security of the DC network depends largely on how secure the PRNGs are. Therefore,

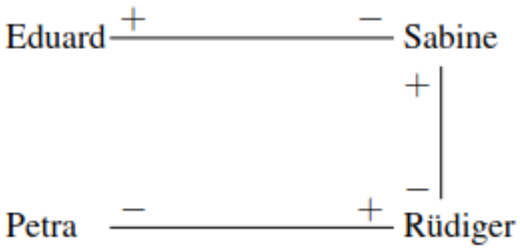


Figure 3.3: An example of a NILM analysis.

the PRNGs that are used must be cryptographically secure.

The principle of the DC network is illustrated graphically in figure 3.3 using a simple example. Figure 3.3 is also called the key graph of a DC network and shows 4 participants in a DC network that are connected to each other along a communication link. The outer participants have only one partner, the inner participants are connected to 2 partners. Each participant now exchanges keys with its direct partners. The outer partners need to exchange only one key and the inner ones exchange keys with two direct partners. The mathematical operation indicates whether the participant adds or subtracts the exchanged key with the partner. In the example given in the figure, the user Petra would subtract the exchanged key with Rüdiger from the message and would have formed her local superposition. Rudiger would have to add the exchanged key with Petra to his message. He would also have to subtract the key he exchanged with Sabine from the result to calculate his local superposition.

### 3.3.2 DC Network Protocol in a German Smart Grid

The DC network is a scheme that can be used to achieve sender anonymity and receiver anonymity. Considering the use case of the thesis, the receiver anonymity does not have to be implemented. The aim is to anonymize the electricity consumption and send it to the electricity provider. In this case, the electricity provider is a public recipient and known to all participants. Therefore, the identity of the electricity provider does not need to be protected. Unlike in a normal DC network, the participants do not want to communicate with each other, they only want to send their electricity consumption to the electricity provider. The only exception is when joining the DC network, there the customers have to perform a key exchange once to configure the initial value for the PRNG as explained in 3.3.2.

#### Protocol Header

Each frame in the DC network protocol has the following structure. As first field there is a Protocol Identifier field. The purpose of the Protocol Identifier field is to ensure that the application of the DC net protocol is recognized by all participants and that the SMGWs as well as the electricity provider can react correctly to the frames. This is followed by the DC Network Identifier field. The DC network identifier field offers the


Figure 3.4: An example of a NILM analysis.

electricity provider the possibility to operate several DC networks in different regions and to distinguish DC networks. In addition, each SMGW is given a unique identifier so that the SMGWs can be distinguished. If the network needs to perform error correction, SMGWs can be notified by the identification number from the power supplier. Although the SMGWs can be identified by the field, the electricity provider still cannot draw any conclusions about electricity consumption from the local superposition. The transmission bit indicates that an SMGW has sent a message and it is used for error correction procedures. The timestamp field indicates when a message was sent. This allows the electricity provider to classify messages by round and not charge for messages from different rounds. The second to last field is the notification field. The field is used for error codes. The electricity provider can thus send notifications to the SMGWs to start error correction procedures. In the last field, the Data field, only the local superpositions are sent.

**Protocol Initialization**

For the Protocol Initialization it is assumed that the electricity provider wants to create a completely new DC network. First, a unique and unchangeable DC Net Identifier is assigned from the electricity provider to the empty DC Net. At least 2 SMGWs have to enter the DC Net. A DC Net with only one participant is not operational and cannot offer anonymity. According to the Technical guideline TR-03109 from BSI, SMGWs are only allowed to communicate with authorized participants in the smart grid and all foreign requests are ignored. These are EMTs, GWAs and the electricity provider. In order for the DC grid to become operational, two SMGW must exchange an initial value to configure the PRNGs. A start value is exchanged once with which both PRNGs of the clients are initialized. As a result, the same random number sequences are generated independently of each other by the PRNG on both clients. But there is a communication barrier that does not allow SMGWs to communicate with other SMGWs. With the limited communication capabilities, the SMGWs rely on the electricity provider. The SMGWs can use a key exchange protocol like Diffie-Helman to transmit the initial value. Diffie-Hellman is a known key exchange protocol, where 2 users can publicly exchange a secret without a third person being able to figure out the secret.

SMGWs can generate cryptographically secure keys because they have a hardware security module built in. Therefore Key exchange procedures such as Diffie-Hellman can be implemented for the SMGW without any problems. Diffie-Hellman was also only mentioned as an example. There are various attacks on the Diffie-Hellman variant presented.The forwarding of SMGW messages by the electricity provider enables the implementation of other substantially secure key exchange procedures. The advantage

of this approach is that SMGWs are anonymous to other SMGWs. When the keys are exchanged, only the partners with whom the key is currently exchanged are aware of it. Uninvolved SMGWs do not receive any information about the entry of new users in a DC network. In addition, the participants share their client identifiers during the key exchange. Due to the exchanged communication details, each participant in the DC network knows the identification number of its neighbor. This is later helpful for error correction measures.
The use of a key exchange method also has disadvantages. By forwarding messages, the electricity provider knows which SMGW have exchanged keys with each other. Exchanging keys is equivalent to creating an edge in the key graph.Therefore, the electricity provider can easily replicate the key graph of the DC network. The knowledge about the structure of the key graph alone does not give the electricity provider any further knowledge, but a malicious electricity provider could use the knowledge to launch active attacks on individual SMGW. An example would be that a electricity provider wants to get information about the power consumption of an SMGW. The electricity provider could connect one or more SMGWs it controls to the victim SMGW through a key exchange that the attacker SMGW launches. The electricity provider could now hope that in the future the victim SMGW will only have keys with the attacker SMGW. Since the electricity provider controls the attacker SMGW and knows the keys of the attacker SMGW, it can reconstruct the electricity consumption of the victim SMGW from the local superposition.

**SGMW Registration in a DC Network**

An SMGW that wants to register in the DC network sends a special defined request to its power provider. For this purpose the notification field in the header is used and notification 1 is sent. Notification 1 represents a request from the SMGW to register in a DC network. The electricity provider assigns the requesting DC client to a suitable geographical region and suggests a suitable client (SMGW) which is already registered in the DC network. The electricity provider now establishes a tunnel and sends the tunnel information to the DC client and the registering client. Via this tunnel it is possible for the two SGMW to establish a communication link via the electricity provider. If an SMGW sends to the tunnel, the message is forwarded to the future neighbor. The DC client which is already present in the DC network is only informed by the electricity provider that it receives a new neighbor and has to exchange contact information. The requesting SMGW needs to send the seeds over the tunnel. To prevent the electricity provider from reading the seeds, the clients exchange Diffie Helmann keys via the tunnels provided.Once the seeds have been exchanged, the power provider is informed by the requesting client that it has successfully entered the DC network by notification 3. Subsequently, all participants in the DC network can send their local superpositions to the power provider. Here, the number sequences are used as keys, which are generated from the synchronized PRNGs. Subsequently, the local superpositions are sent to the electricity provider. The provider forms the global superposition and receives the aggregated power consumption of all SMGWs in the DC network. The local The electricity provider is responsible for ensuring that messages can be exchanged between

the registered clients via the tunnel already in use, if required. The already registered clients can therefore not choose which new communication partners they get. In addition it is assumed that the electricity provider has already been authorized by the SWA. Otherwise, the SMGW would not be able to establish a connection to the supplier.

### SGMW Normal Operation

wie sieht eine normale Operation aus? wie häufig wird gesendet? wofür wird das transmisson bit verwendet? und der timestampt

### SGMW Exit from the DC Network

An exit can be caused, for example, when the customer changes the electricity provider. Then a defined message is sent to the electricity provider when an exit occurs. The electricity provider informs the neighbors of the exiting client with a notification message 4. In addition, the DC Client Identifier of the exiting SMGW is sent with the notification message 4. This notification signals to the neighbors of the exiting SMGW that they must discard their PRNG configurations to client X and that they must not be used in the calculation of the local superposition in the next round. In order to avoid a synchronization error in the DC network, the "neighbors" must confirm to the power provider that all seeds have been discarded. Otherwise the case may occur that a SMGW continues to add the old key to its message. This would result in a useless global sum. Furthermore, the key graph must be considered. It could be the case that the underlying key graph splits into two DC networks. If this is the case, two separated DC networks are sending to the same DC network identifier. In the example of Figure 3.3, this could happen if Sabine and Rüdiger throw away their shared key. The result is different depending on the position where a DC net splits. But at least one DC network experiences a significant loss of anonymity due to the smaller number of participants that can be aggregated. In the case of particularly serious splits, it can even lead to a participant being completely disconnected from the DC network. If a disconnected client notices that it no longer has any neighbors, it sends a special emergency message to the power provider. Then a new registration process is initiated before the next round starts.
To avoid splitting into two DC networks, the exiting SMGW informs its neighbors with which direct partners it was connected. These then initiate a registration process and exchange keys with each other. The fact that all neighbors have exchanged keys with each other guarantees that a DC network does not split when an SMGW leaves.

### SGMW Connection loss

SMGWs have an Internet connection with which they can communicate in the WAN. If the Internet connection is interrupted, this can lead to an SMGW not being able to send its local superposition in time. write design

# 4 Implementation

. . . implementation . . .

write implementation

# 5 Evaluation

. . . evaluation . . .

write evaluation

# 6 Future Work

. . . future work . . .

write future work

# 7 Conclusion And Outlook

. . . conclusion . . .

write conclusion