MANCHESTER 1824
The University of Manchester

Privacy Preserving Billing in Local Energy Markets with Imperfect Bid-Offer Fulfillment

A report submitted to The University of Manchester for the degree of
Bachelor of Science in Computer Science
in the Faculty of Science and Engineering

Year of submission
2023

Author
Andrei Hutu

Supervisor
Dr. Mustafa A. Mustafa

Department of Computer Science

Contents

Word count: 12,827

List of Tables

List of Figures

List of Algorithms

Abbreviations

ACD	Aggregate consumption data
BillCalc	Bill calculation
CD	Consumption data
ECD	Encrypted consumption data
FiT	Feed-in tariff
GridOp	Grid operator
HomoDec	Homomorphic decryption
HomoEnc	Homomorphic encryption
KeyGen	Key generation
LEM	Local energy market
MPC	Multi-party computation
P2P	Peer-to-Peer
P2PM	Peer-to-Peer market
PPBSP	Privacy-preserving billing and settlements protocol
RES	Renewable energy source
RM	Retail market
RP	Retail price
SG	Smart grid
SM	Smart meter
SOTA	State of the art
TD	Total deviation
TDD	Total demand deviation
TP	Trading price
TrPlat	Trading platform
TSD	Total supply deviation

Notations

$\{X\}_{pub}$	Value 'X' encrypted using key 'pub'
pub_X, $priv\_X$	Public key of 'X', Private key of 'X'
U_n / N_u	Total no. of users
U^x	Individual user
U_{val}	Individual meter reading of user
U_{P2P}	Individual committed volume of user
$InDev_x$	Individual deviation of a participant
$InDev_i$, $InDev_j$	Individual deviation of a consumer / prosumer
C_n	Total no. of Non-P2P consumers
C_i	Individual consumer
$P2P_n^c$	Total no. of P2P consumers
$P2P_{n,k}^c$	Total no. of P2P consumers per supplier
$P2P_i^c$	Individual P2P consumer
C_{dem}^{P2P}	Individual committed demand of P2P consumer
P_n	Total no. of Non-P2P prosumers
P_j	Individual prosumer
$P2P_n^p$	Total no. of P2P prosumers
$P2P_{n,k}^p$	Total no. of P2P prosumers per supplier
$P2P_j^p$	Individual P2P prosumer
P_{sup}^{P2P}	Individual committed supply of P2P prosumer
T_{over}^c	Total volume over-consumed
T_{under}^c	Total volume under-consumed
T_{over}^p	Total volume over-supplied
T_{under}^p	Total volume under-supplied
T_up	Total volume under-consumed or over-supplied
T_down	Total volume over-consumed or under-supplied
S_n / N_s	Total suppliers
$N_{u,s}$	Total no. of users per supplier
S_k	Individual supplier
S_k^{inc}	Individual supplier income
S_k^{exp}	Individual supplier expenditure
S_k^{bal}	Individual supplier balance
S_k^{P2P}	Individual supplier P2P residue
V^{RM}	Total volume traded at the retail market

Abstract

Smart grids are being increasingly deployed worldwide, as they constitute the electrical grid of the future, providing bidirectional communication between households. One of their main potential applications is the peer-to-peer (P2P) energy trading market, which promises users better electricity prices and higher incentives to produce renewable energy, while also increasing energy efficiency by reducing the electricity waste that arises from transportation across long distances. However, most P2P markets require users to submit energy bids/offers well in advance of their corresponding time slot, which cannot account for unexpected surpluses of energy consumption/production. Moreover, the fine-grained metering information used in calculating and settling bills/rewards is inherently sensitive and must be protected in conformity with existing privacy regulations.

To address these issues, this report proposes a novel privacy-preserving billing and settlements protocol, PPBSP, for use in local energy markets with imperfect bid-offer fulfillment, which only uses homomorphically encrypted versions of the users' half-hourly consumption data. In addition, PPBSP also supports various cost-sharing mechanisms among market participants, including two new and improved methods of proportionally redistributing the cost of maintaining the balance of the electrical grid in a fair and intuitive manner.

An informal privacy analysis is performed in order to highlight the privacy-enhancing characteristics of the protocol, which include metering data secrecy and bill confidentiality. The performance-related properties of PPBSP are also evaluated in terms of both computation cost and communication overhead, demonstrating its efficiency and feasibility for markets ranging from the size of small local communities to large urban centres, thanks to the highly parallelizable nature of the billing algorithm and the low computational load placed on the users' smart meters.

Declaration of Originality

I hereby confirm that this report is my own original work unless referenced clearly to the contrary, and that no portion of the work referred to in the report has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Intellectual Property Statement

i The author of this thesis (including any appendices and/or schedules to this thesis) owns certain copyright or related rights in it (the "Copyright") and s/he has given The University of Manchester certain rights to use such Copyright, including for administrative purposes.

ii Copies of this thesis, either in full or in extracts and whether in hard or electronic copy, may be made *only* in accordance with the Copyright, Designs and Patents Act 1988 (as amended) and regulations issued under it or, where appropriate, in accordance with licensing agreements which the University has from time to time. This page must form part of any such copies made.

iii The ownership of certain Copyright, patents, designs, trademarks and other intellectual property (the "Intellectual Property") and any reproductions of copyright works in the thesis, for example graphs and tables ("Reproductions"), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property and/or Reproductions.

iv Further information on the conditions under which disclosure, publication and commercialisation of this thesis, the Copyright and any Intellectual Property and/or Reproductions described in it may take place is available in the University IP Policy (see `http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=24420`), in any relevant Dissertation restriction declarations deposited in the University Library, and The University Library's regulations (see `http://www.library.manchester.ac.uk/about/regulations`).

Acknowledgements

I would like to thank my supervisor, Dr. Mustafa A. Mustafa, who provided continuous counsel and guidance during the entirety of my project's timeline, and whose consistent weekly availability meant my burning questions never went unanswered for long.

I wish to also thank my family for their unconditional support throughout my three years of university and especially during the writing of this report. Without their reassuring presence and words of encouragement, I doubt this project and, consequently, my degree would have turned out the same.

Finally, I thank my friends and, in particular, my flatmate Codrin for putting up with my sporadic kitchen rants and for playing a pivotal part in the rubber duck debugging technique that I have mastered while discussing my progress.

1 Introduction

1.1 Motivation

Many different researchers and stakeholders hold the vision that smart grid (SG) will be the next-generation electrical grid for providing electricity to millions of households around the world in a distributed manner [1]. In essence, a smart grid is an advanced version of the traditional electrical grid system which also incorporates two-way electricity and communication flow capabilities between different devices that work together to collect, transmit, and analyze data in real time [2]. A general smart grid architecture is illustrated in Figure 1. Among its various components, smart meters (SMs) are the ones to enable fine-grained, immediate monitoring of energy consumption and production, supporting the integration of renewable energy sources and, most importantly, enabling the communication of such data for use by innovative SG applications [3]. With 29.5 million SMs already installed in UK households, representing 52% of all electrical energy meters [4], it is planned that the automatic sending of such half-hourly meter readings from every single house and small business will become the default option by 2025 [5].

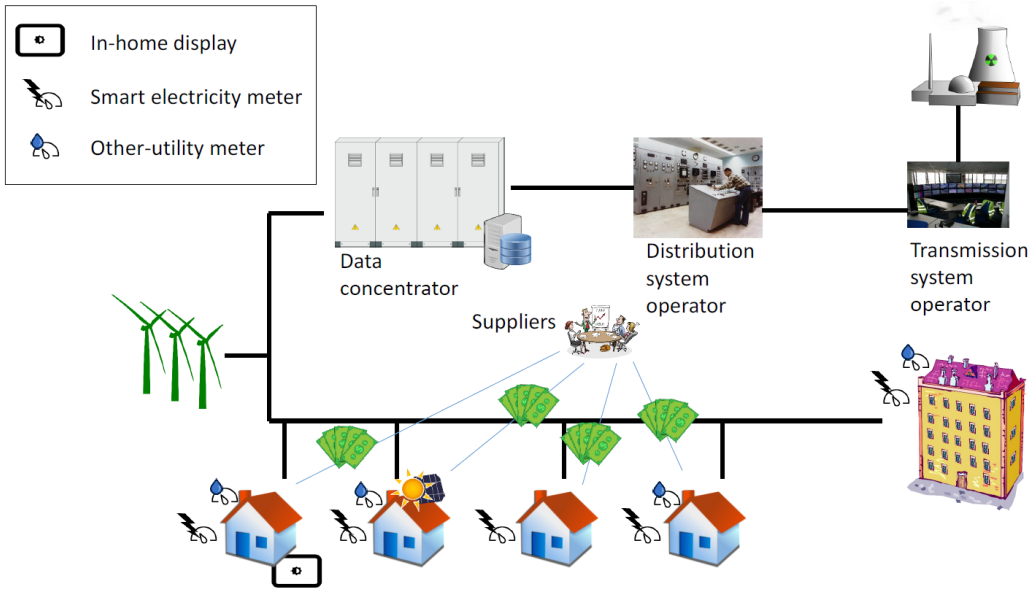


Fig. 1. Illustration of a smart grid architecture [6].

The potential benefits of smart grids have attracted diverse stakeholders, including policymakers, energy providers, and also consumers. Governments and regulatory bodies recognise the importance of SGs for energy security, reducing greenhouse gas emissions, and increasing energy efficiency by reducing the waste of energy from transportation across long distances [7]. Meanwhile, energy suppliers and distributors view SGs as an opportunity to optimise their operations, reduce costs, and provide better customer service [8]. A recent SG application that strongly benefits energy customers [9] and on which this report will focus is the peer-to-peer (P2P) electricity trading market [10], as the

preferred implementation of the local energy market (LEM) model [11]. The P2P market enables individuals or organizations to buy and sell electricity directly from each other, without the need for a centralized intermediary such as energy suppliers, leading to a more efficient and flexible energy market [12]. Not only does it lead to better prices for consumers, but it also gives users a higher incentive to produce and sell their renewable energy, as the P2P trading price of electricity is highly advantageous to the fixed Feed-In Tariff (FiT) imposed by suppliers in traditional energy systems. Moreover, as the trading price at the P2P market is decided based on current supply and demand needs, the adoption of such a system has been shown to be capable of improving the local balance of energy generation and consumption [13]. An example LEM is illustrated in Figure 2.

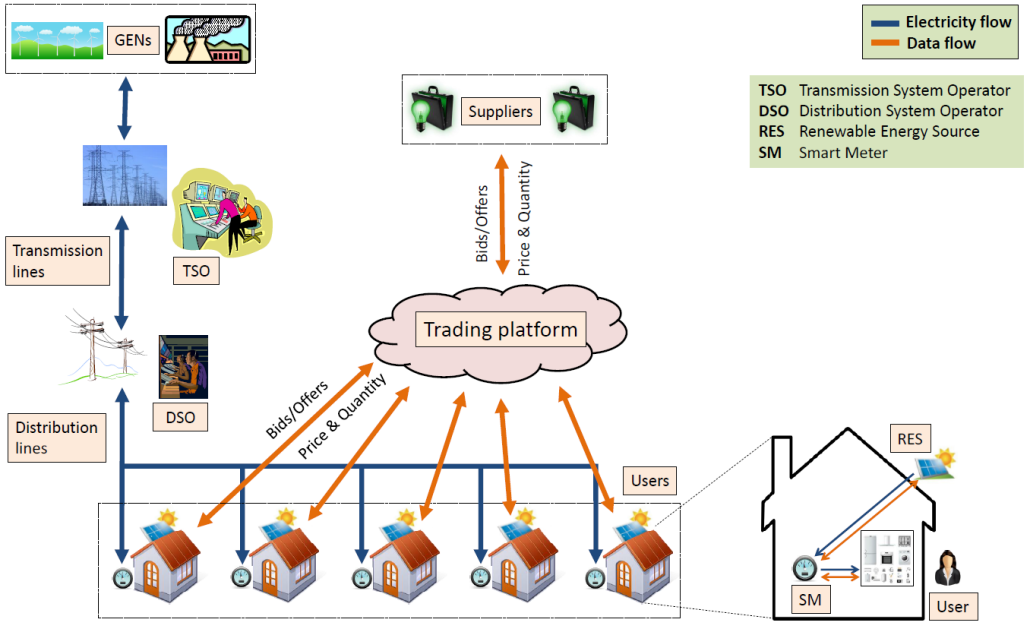


Fig. 2. A proposed local energy trading market architecture [6].

1.2 Problem Statement

In most P2P markets, users are required to submit bids/offers regarding their predicted energy consumption/production during a specific period (e.g. 30 minutes, one hour, etc.) ahead of time, using historical data of the household's load profile [14], weather forecasts [15], etc. Although accurate, it is impossible for any algorithm to predict the exact demand/supply of a household without fail, as unexpected surpluses of energy consumption/production are inevitable. This additional demand/supply represents the deviation between the user's commitments at the P2P market (their bid/offer) and their actual volume of energy consumed/produced during that period (measured by the SM). Together, these deviations can affect the efficient operation of the grid and increase the cost of keeping it balanced [16].

Moreover, to enable the calculation and settlement of bills and rewards for users participating in the P2P electricity trading market, their fine-grained meter readings would need to be communicated to

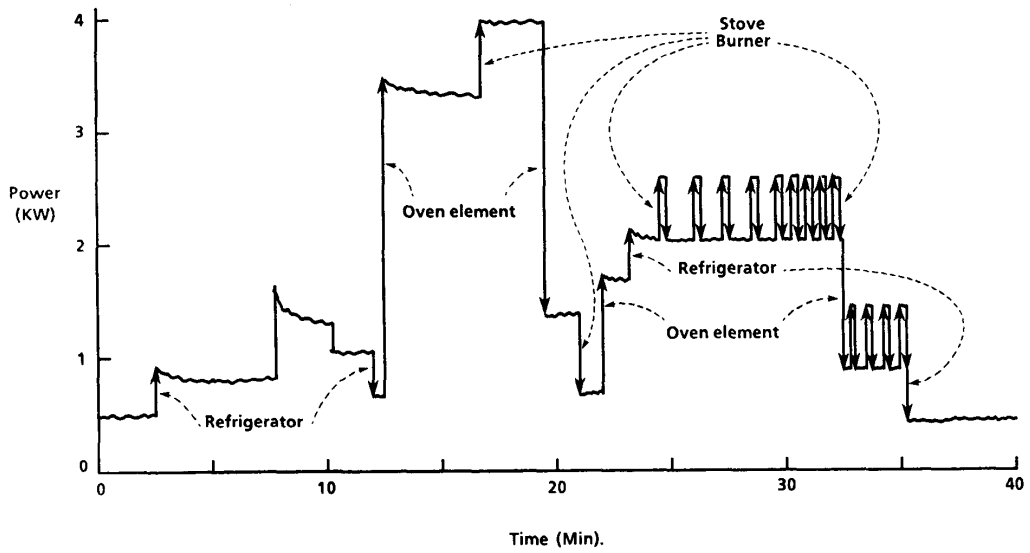


Fig. 3. Non-intrusive appliance load monitoring example [17].

the trading platform, grid operators, suppliers, or even other participants in the market. Since this type of data inevitably contains sensitive information concerning the residents of a household [18], [19], and thus undoubtedly infringes both the European General Data Protection Regulation (GDPR) and the British Data Protection Act (DPA) [20], particular attention has been paid to the possible private information that a malicious agent could discover about the inhabiting individuals. Among others, risks include the use of non-intrusive load monitoring (NILM) techniques [21] to infer the electrical consumption patterns of individual users, which could lead to the disclosure of privacy-invasive insights about specific medical conditions [22], religious beliefs, home appliance usage habits [23], etc. Such, NILM is also one of the primary methods for performing consumer behaviour analysis [24] and has the potential to lead to targeted advertising [25]–[27], insurance adjustment, or discrimination and profiling [28]. Figure 3 illustrates what type of information can be gathered from a household's electric power load profile. Therefore, the need arises for a privacy-upholding solution capable of working on a protected version of the user's sensitive data, including both the energy volume committed to the P2P market and the corresponding individual deviation, which would reveal only aggregated consumption data statistics to other curious market entities.

1.3 Aims and Objectives

To address these privacy concerns, the aim of this project is to design, implement and evaluate a novel privacy-preserving solution capable of calculating and resolving electrical energy bills and reward payments in local energy markets with imperfect bid-offer fulfillment, using only encrypted versions of the users' fine-grained consumption data. The solution should be also compatible with existing P2P trading markets from literature.

The objectives are outlined as follows:

- Perform a review of existing literature in order to identify research gaps.
- Design a protocol capable of settling energy bills in a privacy-friendly manner for use in local energy markets.
- Implement and evaluate the proposed algorithm to verify its efficiency and practicality.

For protocol evaluation, an analysis of its privacy-related characteristics, as well as performance-related properties, will be conducted. First, the privacy and security analysis will examine whether the appropriate requirements established in the design preliminaries are upheld. Afterwards, the performance evaluation will test the computational complexity and the communication overhead of the proposed protocol, simulating the costs of real-world scenarios by varying the number of participating households, therefore covering a broad range of possible sizes for LEMs (from small, isolated communities to large metropolitan centres).

1.4 Limitations of Current Solutions

A privacy-enhancing solution for billing using a symmetric homomorphic encryption scheme has already been proposed by Alabdulatif *et al.* [29], while another privacy-friendly implementation of a local energy trading market using multi-party computation [30], later improved by the same authors through the addition of a simple billing algorithm has also been presented [31]. However, neither of these protocols takes into account the possible differences between the final meter readings and the volume that each user previously committed to trade for at the P2P market.

Despite the energy deviations' importance to the balance of the electrical grid, this topic has been mostly neglected in prior research, especially in the context of privacy-conscious implementations. The first to propose a solution for LEMs with imperfect bid-offer fulfillment, capable of bill adjustments in line with the respective individual deviations, were Thandi *et al.* [32], whose protocol accomplishes the privacy-enhanced billing and settlements process using a partially homomorphic cryptosystem. However, the billing model presented only considers the individual deviations separately from each other, and thus inter-supplier aggregation of deviations is not supported, which would allow individual household deviations to compensate for each other, lowering energy costs for all P2P users.

While recent papers have proposed various billing models for P2P energy markets which take into account these half-hourly individual deviations, incentivising consumers/prosumers to minimise their own deviations by proposing different methods of distributing monetary rewards/punishments among the set of participants [33], they were not designed to be at all privacy-preserving by themselves, but rather theoretical algorithms to be implemented in novel privacy-friendly protocols.

1.5 Contributions of the Work

To address the aforementioned limitations, we propose a novel privacy-preserving billing and settlements protocol (PPBSP) for local energy markets with imperfect bid-offer fulfillment. More specifically, the novel contributions of this work are fourfold:

- Design a novel privacy-protecting protocol, PPBSP, by improving on the current state-of-the-art (SOTA) solutions [32], which uses the Paillier partial homomorphic encryption scheme to calculate and settle bills in P2P markets, taking into account each user's individual deviation from the committed volumes and supporting the social splitting of their accompanying costs among all consumers/prosumers.
- Implement and improve two SOTA billing models from literature [33] by adding a proportional redistribution of the costs incurred for maintaining the grid's balance in the presence of individual deviations, leading to a more fair and intuitive calculation of bills and compensations for P2P market participants.
- Perform privacy and security analysis of PPBSP in regard to internal system entities.
- Implement and evaluate the performance of PPBSP in terms of its computational and communication costs, both in theory (via analysis and extrapolation) and in practice (through simulations and measurements). The entire codebase is publicly hosted on my personal GitHub account.

The results of the work and research performed during this 3rd Year Project will later be summarised and subsequently submitted in the form of a conference paper to the 9th IEEE International Smart Cities Conference (ISC2 2023).

1.6 Report Structure

The rest of the report is organised as follows:

- Section 2 presents the necessary background knowledge and discusses related work.
- Section 3 outlines the design preliminaries involved in implementing PPBSP.
- Section 4 proposes and describes in detail the design properties of PPBSP.
- Section 5 analyses the privacy and security properties of the protocol and evaluates its performance in terms of computation and communication costs.
- Section 6 summarises my work and proposes future research avenues.

2 Background and Related Work

This section presents the necessary background information on smart grids and local energy markets, as well as the cryptographic building blocks used in the design of PPBSP. Afterwards, I also give an overview of the current research in privacy for smart grids, with an emphasis on settling bills in LEMs.

2.1 Local Energy Trading Concepts

2.1.1 Smart Grid

The smart grid (SG) represents an enhancement of the traditional electrical grid infrastructure through the implementation of a two-way communication network connecting its various entities and components [34]. One of its main components is the smart meter (SM), a device which replaces traditional electricity meter on the customer's premises, capable of the following crucial functions:

- It is capable of measuring the flow of electricity in both directions, from the grid to the household and vice versa.
- It facilitates bidirectional communication with other actors within the SG system.
- It has the ability to measure various parameters related to the flow of electricity, including voltage level and frequency.

This integration of automatic meter readings can lead to a more reliable and efficient grid through automatic grid management systems and to more accurate and efficient billing and energy trading. The latter constitutes the motivation for the development of local energy market models.

2.1.2 Local Energy Market

The status quo in most liberalised energy markets limits customers to only buying or selling electricity from their energy supplier, thus leaving them few options to optimise their prices and providing no incentive to adopt renewable energy sources (e.g. solar panels), as any excess production is automatically injected back into the grid for little to no remuneration.

Contrary to this, LEMs permit users to trade electricity with other users and suppliers [18]. This means that a household generating more electricity than needed to cover its own demand is able to sell that surplus to another local consumer at the peer-to-peer trading market. Therefore, the P2P market participants set their own common trading prices, allowing them to purchase electricity at a

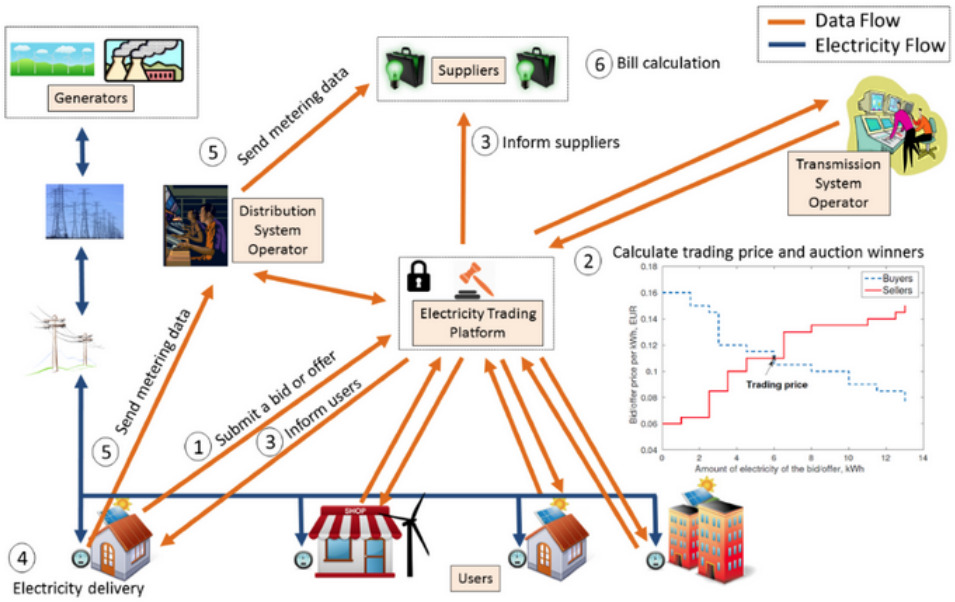


Fig. 4. A P2P local electricity trading process [6].

lower price and also sell it at a higher one than the suppliers' offer. This process is illustrated in Figure 4. The potential benefits of LEMs include the increased autonomy of microgrids, the decreased transmission-related electricity losses by encouraging the use of locally generated energy, and, most importantly, the additional incentives to install renewable energy sources. Naturally, for users who are unable to participate in the local electricity trading market, the supplier will remain an alternative source for both purchasing and selling electricity, thus serving as a secondary source for most households.

2.1.3 P2P Billing Model

Most P2P electricity trade markets determine the trading price through an auction mechanism in which the users participate by submitting their bids and offers in advance [35]. Therefore, an increased demand for electricity leads to a higher price, incentivising the prosumers to generate and sell more energy to compensate and the consumers to lower their consumption, whereas a larger supply than demand leads to a lower trading price, encouraging consumers to capitalise on and increase their consumption and prosumers to temporarily store away their electricity surplus. As this double auction mechanism takes place well in advance of the actual consumption/production time (ranging from 30 minutes to a day before), households are required to predict their future demand/supply values. As expected, such a process, however accurate, will lead to marginal, yet likely non-zero, differences between the volume that a user has committed to buy from/sell to the P2P market and their real meter readings, which are called individual deviations.

For a prosumer (a user that has sent an offer to sell electricity), a positive deviation means that the household supplied more energy than necessary, while a negative one denotes the under-production

of electricity. Similarly, for a consumer (a user that has submitted a bid to purchase electricity), a positive deviation suggests consuming more than the committed volume, whereas a negative value indicates the unfulfillment of the household's consumption commitments. Moreover, in some instances, it is possible for a prosumer to under-supply to the extent that they actually become a net buyer of electricity for that trading period. The billing models proposed in this report are designed to seamlessly accommodate this case, too.

A billing model with imperfect bill-offer fulfillment takes into account both the user's committed volume to the P2P market and its individual deviation in order to incrementally calculate the monthly electricity bills by splitting the cost of the aforementioned deviations fairly among household [33], using various methods that are further described in Section 4.3.1. From beginning to end, the process of producing the bill for a single trading period (e.g. 30 minutes, one hour) consists of the following four steps:

1. Each user predicts the future demand/supply of the household using historical data, alongside other parameters, and submits the bid/offer to the P2P electricity auction.
2. The trading price is decided by the relationship between current supply and demand, while users are informed whether their bid/offer has been accepted by the auction.
3. Meter readings are performed for the respective trading period and the discrepancies between them and the corresponding bid/offers are noted.
4. Each user's partial bill is calculated by the trading platform.

This work tackles the intricacies of the last two steps, from the moment real electricity consumption/production data is made available by the smart meter to the end of the bill settlement process.

2.2 Privacy Issues and Cryptographic Building Blocks

2.2.1 Privacy Concerns of Smart Metering

Multiple studies have shown that personal information can be inferred by observing a household's fine-grained electricity consumption data [36]–[38]. For example, non-intrusive load monitoring can reveal information regarding religion by observing early morning activity during the month of Ramadan, or provide health-related information like sleeping habits and cooking tendencies. Because of the unique nature of each appliance's load signature, it is also possible to identify specific appliances in a detailed consumption pattern [17], as illustrated in Figure 5. This data can be used by various entities such as marketers, insurance companies, or criminals for reasons ranging from targeted advertisements and insurance adjustments to identifying the presence of valuable appliances and planning break-ins.

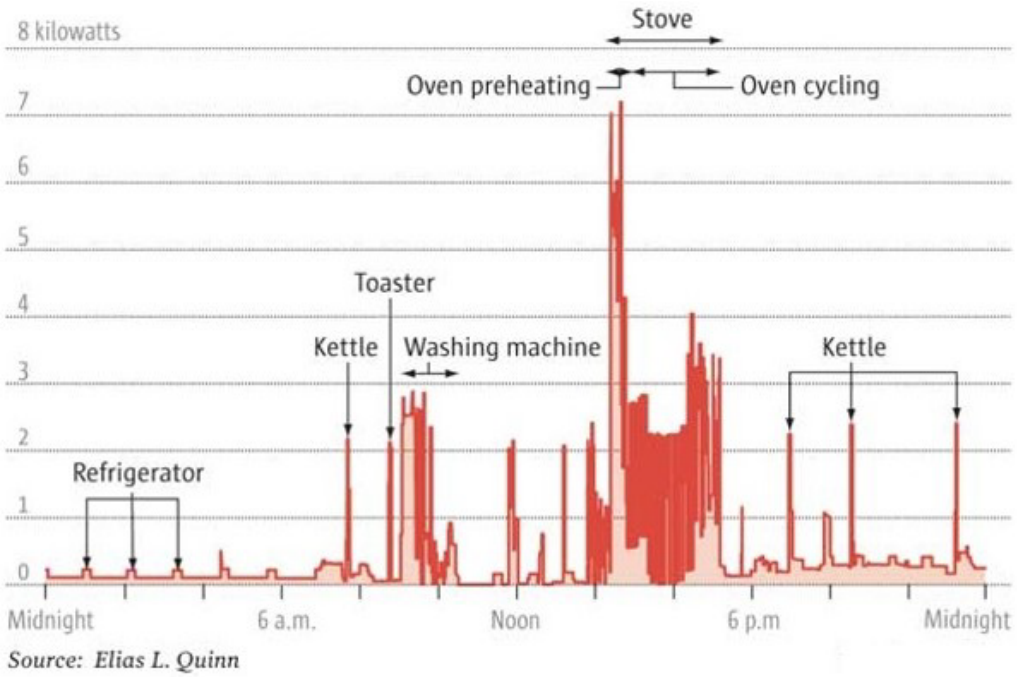


Fig. 5. Recognising appliances in a detailed consumption pattern [39].

2.2.2 Honest-but-Curious Model

This report extensively uses the honest-but-curious adversary model or semi-honest model [40]. This model assumes that parties follow the protocol accurately (i.e they are "honest"), but they also actively seek to infer knowledge about other entities from all the inputs they receive or any intermediate computation results (i.e. they are "curious"). Thus, honest-but-curious adversaries aim to maintain the proper functioning of the system in order to avoid being identified by monitoring mechanisms while also maximising their chance to infringe on others' privacy.

In the LEM case, honest-but-curious smart meters are trusted to only communicate accurate meter readings, the trading market will correctly calculate the users' bill, etc. However, suppliers, the market operator and other entities will also try to deduce individual load profiles by analysing values which have been submitted to them.

2.2.3 Cryptographic Schemes

Asymmetric Key Encryption. An asymmetric key cryptosystem involves the use of two distinct, but mathematically connected, keys by both the sender and the receiver in order to perform cryptographic operations, whose primary goals are message confidentiality, authenticity, etc. One of the keys, referred to as the public key, is made public, while the other key, known as the private key, must be kept confidential, accessible only by its owner [41]. An example of such a cryptosystem being used to provide message confidentiality is depicted in Figure 6.

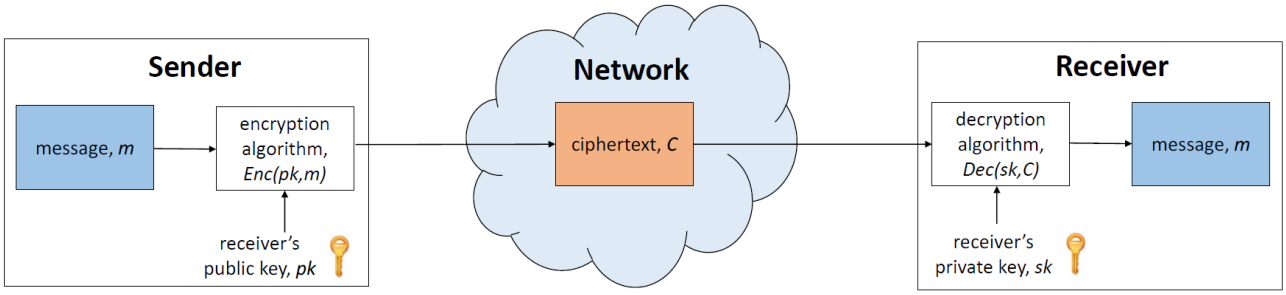


Fig. 6. Asymmetric key cryptosystem [42].

Homomorphic Encryption. Homomorphic encryption represents a set of encryption functions which provide semantic security and enable specific algebraic computations to be carried out directly on the ciphertext, without the need for decryption. When the resulting ciphertext is finally decrypted, the output obtained is the same as that achieved if the operations were instead performed on the unencrypted data [43]. These encryption schemes are mostly used in privacy-conscious solutions, in which mathematical operations must be carried out while keeping the inputs hidden. Homomorphic cryptosystems can be categorised into multiple types, the most important of which being:

- *Partially homomorphic encryption (PHE)*: allows one select operation (addition or multiplication) to be performed on ciphertext an unlimited number of times.
- *Somewhat homomorphic encryption (SHE)*: allows two types of operations (addition and multiplication) to be performed on ciphertext a set number of times.
- *Fully homomorphic encryption (FHE)*: supports arbitrary computation on ciphertexts, being the most powerful type of homomorphic encryption, but limited by its large computational overhead.

Paillier Cryptosystem. Out of the many homomorphic encryption schemes, the one that is of particular interest to this report is the Paillier cryptosystem [44]. It is an efficient and semantically secure partially homomorphic cryptosystem, and, most importantly, it has an additive homomorphism property, desirable for privacy-preserving data aggregation. This means that multiplying the ciphertexts of any number of messages results in a ciphertext of the sum of all the messages, as described in (1). Moreover, the cryptosystem is indeterministic, meaning that the same message will be encrypted in different resulting ciphertexts given distinct random values of the blinding factor r.

$$\begin{aligned} C(m_1) \cdot c(m_2) &= (g^{m_1} \cdot r_1^n) \cdot (g^{m_2} \cdot r_2^n) \mod n^2 \\ &= g^{(m_1+m_2)} \cdot (r_{12})^n \mod n^2 \\ &= C(m_1 + m_2) \end{aligned} \tag{1}$$

The Paillier cryptosystem works as follows:

- Key Generation:
  1. Select two large prime numbers (p, q).
  2. Calculate $n = p \cdot q$ and $\lambda = lcm(p-1, q-1)$, where lcm means the least common multiple.
  3. Define the function $L(u) = (u-1)/n$.
  4. Choose a generator $g \in \mathbb{Z}^*_{n^2}$.
  5. Calculate $\mu = \left(L(g^\lambda \mod n^2)\right)^{-1} \mod n$.
  6. (n, g) is the public key.
  7. (λ, μ) is the private key.
- Encryption:
  1. Given a message $m \in \mathbb{Z}_n$
  2. Select a random number $r \in \mathbb{Z}^*_n$.
  3. Compute ciphertext $C = Enc(m) = g^m \cdot r^n \mod n^2$.
- Decryption:
  1. Given a ciphertext $c \in \mathbb{Z}^*_n$
  2. Decrypt it with $m = Dec(c) = L(c^\lambda \mod n^2) \cdot \mu \mod n$.

2.3 Related Work

The preservation of users' privacy represents a topic of great importance to the feasibility of SG applications, which has been studied extensively by the research community [45]. McDaniel *et al.* [46] are the first to identify the privacy-related vulnerabilities in SG systems and call for a broad national effort from government, academia and industry to propose and evaluate new solutions, while Kalogridis *et al.* [47] present a unified framework that provides a methodological approach for integrating privacy into SGs. This report will focus only on a particular problem, which is the privacy of billing in local energy markets, instead of broadly covering the entire SG field.

A comprehensive security analysis of local energy trading markets was performed by Mustafa *et al.* [18], raising several privacy threats and outlining a corresponding set of requirements for such a

market. Various solutions partially addressing these concerns have been proposed. Uludag *et al.* [48] implemented a distributed bidding system that ensures the privacy of bidders, except for the winning bidder, whose identity is disclosed to the service provider, and later extended their design to accommodate a multi-winner auction mechanism [49]. Deng *et al.* [50] introduced an energy trading framework which does not expose the individual customer's bidding price and volume by using homomorphic encryption. Multi-party computation (MPC) [51] has also been used to avoid privacy leakage. An energy auction mechanism implemented by Aly *et al.* [52] allows generators and suppliers to trade electricity in an oblivious manner at the day-ahead market. However, none of these solutions describes in detail the billing and settlements process which would happen after the trades are confirmed.

Pillitteri *et al.* [53] also present a detailed explanation of privacy threats that may arise in the context of SG implementations, as well as suggestions on how to address them. One of the proposed techniques for achieving privacy-preserving metering data aggregation for billing purposes involves the use of homomorphic encryption schemes, but it does not provide an in-depth analysis of this approach. Traditionally, homomorphic encryption has been used in the private aggregation of metering data for operational purposes [54]–[56], but it has also recently been used for private billing by [29]. However, their implementation relies on a symmetric encryption scheme and thus requires a secure key exchange method to function. As for MPC, Abidin *et al.* [30] used it to design a privacy-friendly approach to local energy trading and later improved their protocol through the proposal of a simple privacy-preserving billing algorithm [31]. However, neither of these solutions takes into account the possible deviations between the final meter readings and the volume that each user committed to trade for at the P2P market.

Despite the significance of energy deviations in P2P markets, this issue has been largely overlooked in existing literature, with most prior research either assuming perfect fulfillment of the committed volumes [31], neglecting to include these deviations into their billing models [57], or introducing mechanisms which penalise market participants regardless of their personal contribution to the grid's energy imbalance [58]. Thandi *et al.* [32] were the first to propose a homomorphic billing and settlements scheme which supports bill adjustments according to the individual differences in real electricity consumption/production compared to each user's initial trade commitments. However, the billing mechanism implemented only takes account of the individual deviations independently of each other and does not support any type of social splitting of the deviations' associated costs among P2P market participants, as proposed by Madhusudan *et al.* [33].

Unlike the aforementioned solutions, this report proposes a homomorphic privacy-preserving billing and settlements protocol for local energy markets with imperfect bid-offer fulfillment, which splits the incurred cost from the users' deviations fairly.

3 Preliminaries

This section outlines the system and threat model, assumptions and functional and privacy requirements used in the design of PPBSP.

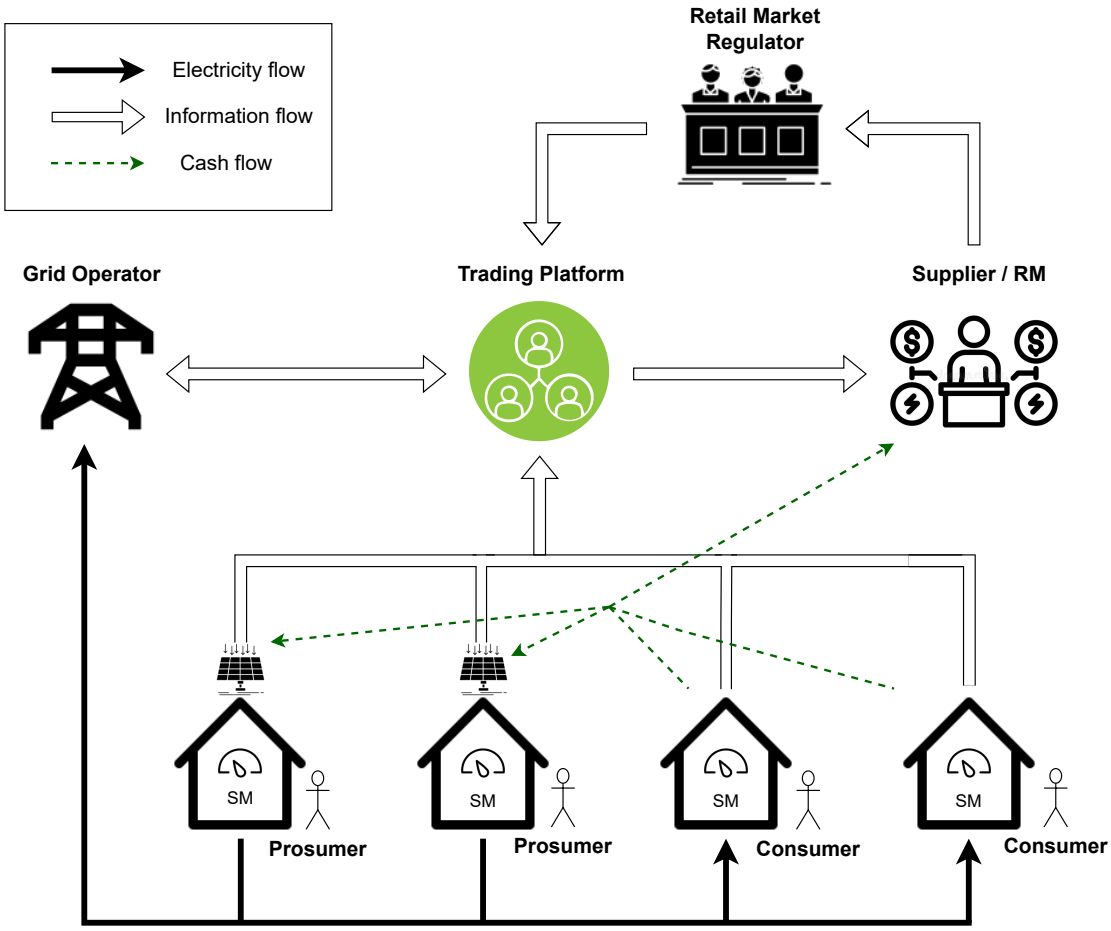


Fig. 7. System model.

3.1 System Model

Figure 7 illustrates the system model used in this report. Its consisting entities are the following:

1. *Users (Consumers / Prosumers)* who:

    - must pay monthly bills for the total energy consumption corresponding to their household;
    - are compensated for their sold production of electricity from renewable energy sources (RES);

- can be either a net importer or net exporter of electricity in any given time slot;
- submit bids/offers for electrical energy using their smart meter (SM) based on predictions by their Home Energy Management Systems (HEMS);
- are temporarily classified as either consumers C_i (buyers) or prosumers P_j (sellers) for each time slot, based on their type of bid/offer submitted at the energy auction; and
- send actual half-hourly consumption/production data through their SM at the end of each trading period to calculate payments.

2. *Peer-to-peer Market Operator / Trading Platform*:

- handles the energy double auction by accepting/rejecting bids and offers to clear the market;
- sets the electricity trading price (TP) based on current supply and demand values;
- keeps track of each user's monthly net balance, updating after every trading period;
- aggregates market-wide electricity usage statistics for each trading slot, to communicate to the grid operator;
- sends each supplier's net balance change for each trading period; and
- sends the final monthly bills of each user to its corresponding supplier.

3. *Suppliers*:

- sell electrical energy to consumers at a retail buy price (RP);
- buy electrical energy from prosumers at a fixed Feed-in Tariff (FiT);
- receive customer bills, including both the capital they traded at the P2P market (with other users) and the backup retail market (directly with the supplier); and
- keep the respective supplier's profit and send the rest to the other suppliers, distributed in accordance with the market regulator's guidance.

4. *Grid Operator*:

- decrypts the aggregated energy usage statistics for each trading slot;
- communicates the decrypted values back to the P2P trading platform for their use in bill calculation; and
- serves as an independent entity capable of periodically (or on-request) checking the sincerity of the suppliers.

5. *Retail Market Regulator*:

    - coordinates the fair redistribution between suppliers of capital acquired by the supplier base in its role as an intermediary of the customer balances traded at the P2P market.

3.2 Threat Model

The threat model of the proposed solution is as follows.

- All entities presented in the system model are considered honest-but-curious entities, meaning that they will only follow the protocol and ruleset provided to them, but will also try to learn as much as possible from the information they have available [59]. Therefore, the peer-to-peer market operator can be trusted to accurately compute the monthly bills and rewards, but cannot be allowed to have access to the raw smart meter data due to privacy concerns. Similarly, the grid operator is expected to provide correct decrypted values of the market deviation statistics, yet it must not be presented with non-aggregated user consumption data.

  The energy suppliers represent a special case of semi-honest agents, as even if they were to behave as malicious entities capable of communicating erroneous, beneficial information about their customers' bills, the existence of an overseeing power makes getting caught and subsequently punished an inevitability, leaving the suppliers no rational motive for acting in a self-serving manner. Therefore, by circumstance, energy suppliers can also be modelled as honest-but-curious entities, trusted to authentically settle bills and payments as long as their truthfulness can be verified by another supervisor agent.

- All external entities operating on the network are malicious. They will try to intercept, read and modify communications between the aforementioned agents.

3.3 Assumptions

We use the following assumtions in our design.

- The distributed system is supported by an underlying network that follows secure communication protocols, such as a robust public-key cryptosystem and digital signatures. Therefore, all communication is assumed to be safe from interception, reading, or modification by malicious entities. Thus, this report is only concerned with protecting sensitive information from its intended recipients.

- A user's household, comprising of a smart meter (SM) and a Home Energy Management System (HEMS), is considered a single, temper-proof entity. The data it collects and sends is assumed to be correct.
- Every consumer/prosumer is assumed to pay their respective bill at the end of the billing period. In the event that they do not, the suppliers would shoulder the debt and deal with the situation accordingly.
- Each participant in the protocol has access to everyone's homomorphic public keys and their own private key.
- There exists a double auction mechanism that sets a single unique trading price for both selling and buying electricity at the P2P market in line with the current supply and demand values.
- The TP is always valued between the FiT and the RP.
- The user is informed of the acceptance status of their bid/offer at the energy auction before the end of each trading period.
- The volume bought at the P2P market is equal to the volume sold at that same P2P market.

3.4 Privacy and Security Requirements

Our designed solution should satisfy the following security and privacy requirements.

- *Metering data confidentiality*: The fine-grained (half-hourly) energy meter readings must only be known by the respective users. For all other uses, such as aggregation or bill calculation, the data must only be available in an encrypted format.
- *Partial bill confidentiality*: The partial bill will be stored by the peer-to-peer market operator only in an encrypted format, which it is unable to decrypt by itself, until the end of the month in order to calculate the final monthly bill. That final bill can be shown to suppliers in order to settle bills as it no longer contains any privacy-sensitive information.
- *Supplier accountability*: An authorised enquiring entity should be able to verify the veracity of each supplier's reported leftover capital after settling bills with its customers.

4 Protocol Design

This section details the novel privacy-preserving billing and settlement protocol PPBSP, which improves upon the SOTA solution for bill settlements in LEMs with imperfect bid-offer fulfillment [32]. Before an intricate explanation of each entity's role and function, a general overview of the protocol is outlined first, explaining the separate phases of the algorithm, from system initialisation, to partial bill calculation, and finally bill settlement. Figure 8 illustrates the general information flow of PPBSP.

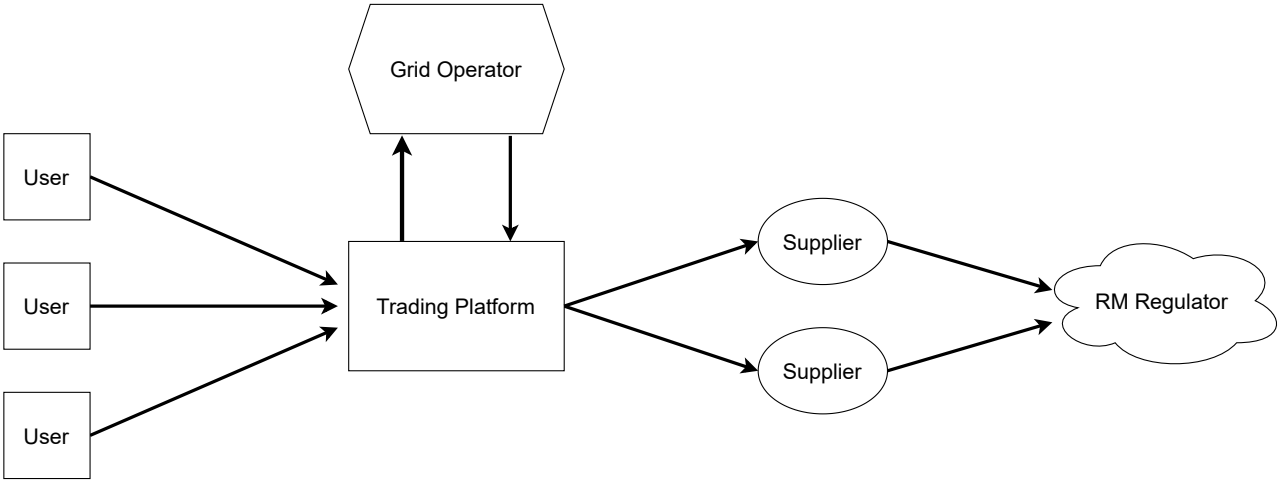


Fig. 8. PPBSP overview.

4.1 Overview of PPBSP

PPBSP comprises three distinct phases: system initialisation, partial bill calculation, and final bill settlement. A Python implementation is also publicly available on my personal GitHub account.

Phase 1 is equivalent to the *system initialisation*. In this phase, the energy suppliers, as well as the grid operator, generate a public-private homomorphic key pair, making the former available to any authorised enquiring entity, while keeping the latter only to themselves. Parallel to this, the P2P trading platform is initialised with a single corresponding grid operator, a list of users, identified using unique IDs, a list of energy suppliers, and a many-to-one relationship mapping each user to its respective supplier.

Phase 2 occurs at the end of each *trading period*, e.g. every 30 minutes in the case of half-hourly meter readings, and represents the partial bill calculation, performed using the following steps. Each user's SM measures the current meter reading for the specific trading slot, separating the electricity consumption/production into committed energy amount and individual deviation, based on its prior bid/offer at the energy auction. Using this metering data along with the knowledge of its latest auction bid and access to a network of public keys, the SM constructs a final payload including ho-

momorphically encrypted versions of the sensitive metering data and additional non-sensitive metadata, which is then sent to the trading platform. Using the received payloads, the trading platform calculates each user's partial bills for the corresponding trading period in accordance with one of the four implemented billing models, with the grid operator acting as a crucial part in market-wide data aggregation in two of the algorithms. After the partial bill calculation is complete, suppliers are sent aggregated data about their customers for that trading period, particularly the respective supplier's net balance change over that slot after transactions with its customers at the retail market.

Phase 3 is repeated after each *billing period*, e.g. every month, and represents the final bill settlement, when the following steps take place. The trading platform aggregates each user's partial bills over the billing period and sends the final number to its corresponding energy supplier. Therefore, each supplier receives a list of final bills of their associated customers. At the same time, each supplier sums up their own net balance changes incurred in each trading period to arrive at a final net balance change value for that billing period. Acting as an intermediary of payments to the P2P market and the RM, after collecting payments or paying out rewards to its customers according to the final bills, each supplier subtracts its own earnings at the retail market (the final net balance) to keep to itself, with what remains being the residue of user transactions at the P2P market. These leftover differences (some positive, in the case where a supplier's customers bought more energy at the P2PM, and some negative, where a supplier's customers sold more energy at the P2PM) are communicated to the retail market regulator, which coordinates their fair redistribution such that the final aggregated residues from all suppliers equal 0, signifying a correct bill settlement process.

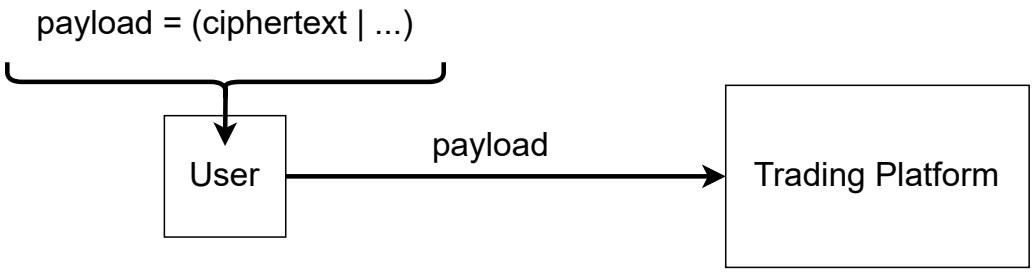


Fig. 9. User protocol.

4.2 User Protocol

At the end of every trading period, each user's SM is entrusted with the encryption and communication of the fine-grained metering data representing the electrical energy consumed/produced by that household over that slot (e.g. 30 minutes, one hour, etc.), in conformity with an accepted convention, in the form of a single payload containing all the necessary information for the trading platform to process and calculate the respective partial bills. This process is outlined in Figure 9. Moreover, PPBSP does not rely on the P2P trading platform having any pre-existing knowledge of the

Algorithm 1 User Protocol

procedure PAYLOAD($is\_bid\_accepted, bid\_type, U^x_{P2P}, U^x_{val}$)
  $net\_consumption\_time$ = $sign(U^x_{val})$
  $InDev_x$ = $(bid\_type \times U^x_{val}) - U^x_{P2P}$
  $\{U^x_{P2P}\}_{pub\_S_k}$ = $Enc(U^x_{P2P}, pub\_S_k)$
  $\{U^x_{P2P}\}_{pub\_GridOp}$ = $Enc(U^x_{P2P}, pub\_GridOp)$
  $\{InDev_x\}_{pub\_S_k}$ = $Enc(InDev_x, pub\_S_k)$
  $\{InDev_x\}_{pub\_GridOp}$ = $Enc(InDev_x, pub\_GridOp)$
return $payload = (is\_bid\_accepted \| bid\_type \| net\_consumption\_type \| sign(InDev) \| \{U^x_{P2P}\}_{pub\_S_k} \| \{InDev_x\}_{pub\_S_k} \| \{U^x_{P2P}\}_{pub\_GridOp} \| \{InDev_x\}_{pub\_GridOp})$

results of the energy auction. This design choice ensures a more distributed delegation of responsibilities across the system's entities and facilitates the protocol's integration with already existing double auction mechanisms from the literature [30], being an inherently modular approach. However, this means that all information regarding the acceptance status of user bids, their type (i.e. whether they were for buying or selling energy), as well as the energy amount which the respective user committed to trading at the P2P market must be communicated individually to the platform to allow for the calculation of the partial bills.

The step-by-step process of payload generation by the SM is presented in Algorithm 1 and described below:

1. It reads the real energy consumption data for the specific trading period U^x_{val}, which then needs to be expressed in terms of:

   - whether or not the user's bid at the P2P market has been accepted $is\_bid\_accepted$:

$$is\_bid\_accepted = \begin{cases} 1 & \text{if bid accepted,} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

   - whether the user offered to buy or sell energy during the auction (consumer/prosumer) bid_type:

$$bid\_type = \begin{cases} 1 & \text{if buying P2P energy,} \\ -1 & \text{otherwise} \end{cases} \tag{3}$$

   - whether the user ended up being a net buyer or a net seller of electricity over the trading slot $net\_consumption\_type$, equivalent to the sign of U^x_{val}:

$$net\_consumption\_type = \begin{cases} 1 & \text{if net buyer of energy,} \\ -1 & \text{otherwise} \end{cases} \tag{4}$$

$$\equiv$$

$$net\_consumption\_type = sign(U^x_{val}) \tag{5}$$

- the energy volume amount committed to the P2P market U^x_{P2P}:

$$U^x_{P2P} \in \mathbb{R}_+, \text{ according to the submitted bid} \tag{6}$$

  The committed value is always a positive number $U^x_{P2P} \geq 0$. Whether the volume was bought or sold at the P2P market is indicated by bid_type.

- the individual deviation $InDev_x$, as a measure of the difference between the real meter reading and the volume committed to trading at the P2P market:

$$InDev_x = bid\_type \times U^x_{val} - U^x_{P2P} \tag{7}$$

because

$$U^x_{val} = bid\_type \times (U^x_{P2P} + InDev_x), \text{ where } bid\_type \in \{\pm 1\} \tag{8}$$

- the sign of the individual deviation $sign(InDev_x) \in \{\pm 1\}$.
  Paillier's cryptosystem does not natively support comparing ciphertext with a constant, as the encryption function is only additively homomorphic. Although there are methods of achieving this operation by subtracting the comparison constant c from the encrypted number $enc(X)$, then multiplying the difference with a randomly generated positive number r, sending the final value $(enc(X) - c) \times r$ to be decrypted using the appropriate private key, and seeing whether the result is a positive or negative number, the added complexity and communication cost make this implementation undesirable for PPBSP. Since the trading platform will only ever need to compare the individual deviations with 0, checking if they are positive or negative, the SM can perform this quick operation itself, as it already knows the comparison constant. Therefore, a simple binary value sent by the user's SM inside the payload is enough.

2. It encrypts the privacy-sensitive data using partially homomorphic encryption:

   - U^x_{P2P} is encrypted once using the supplier's homomorphic public key pub_S_k, and once using the grid operator's analogous public key pub_GridOp, generating two separate ciphertexts: $\{U^x_{P2P}\}_{pub\_S_k}$ and $\{U^x_{P2P}\}_{pub\_GridOp}$

   - $InDev_x$ is similarly encrypted once using the supplier's homomorphic public key pub_S_k, and once using the grid operator's key pub_GridOp, generating another two separate ciphertexts: $\{InDev_x\}_{pub\_S_k}$ and $\{InDev_x\}_{pub\_GridOp}$

- Since $is\_bid\_accepted$, bid_type, $net\_consumption\_type$, and $sign(InDev_x)$ contain less detailed private user information, their privacy-invasiveness must be weighed up against their necessity in the billing algorithm. Therefore, they are not homomorphically encrypted in order to support the comparison operation performed by the trading platform, which is not natively supported by the Paillier cryptosystem, despite the small, but non-zero, information leak.

If PPBSP were to perform homomorphic encryption only using the user's corresponding supplier's public key pub_S_k, bill settlements would still be possible for the first two billing models (see Sections 4.3.2 and 4.3.3), but market-wide energy consumption deviation data across multiple suppliers' customer bases could no longer be aggregated, rendering the last two billing algorithms unusable (see Sections 4.3.4 and 4.3.5). Moreover, by not rerunning the calculations with an independent trusted third-party (TTP) homomorphic public key, we would not be able to fulfil one of this project's proposed requirements, leaving no entity capable of holding the suppliers accountable by potentially verifying their bill settlement results.

Alternatively, the user's consumption data could only be encrypted using the grid operator's key pub_GridOp, which still allows for any of the four possible partial bill calculation algorithms to be used by the trading platform. However, in this case, the computation and communication load placed on the GridOp would be disproportionately large, and it would also introduce an unnecessary single point of failure (SPOF) into the system, leaving the GridOp as the only entity capable of decrypting and reporting each user's bills and each supplier's profits.

Therefore, the payload includes multiple encrypted versions of the consumption data, once with the corresponding supplier's public key pub_S_k, and once with the grid operator's public key pub_GridOp, increasing the redundancy of the system by effectively doubling the encryption computation load on the SM and the partial bill calculation time on the trading platform, neither of which are too high anyway, but crucially eliminating the SPOF, thus improving the system's availability and reliability, and also minimising any risk of a supplier deviating from the protocol, because of the implicit auditing ability of the grid operator.

3. It appends the aforementioned data values together to construct the payload and send it to the trading platform:

$$\begin{aligned} payload = (&is\_bid\_accepted \| bid\_type \| net\_consumption\_type \| sign(InDev_x) \| \\ &\{U^x_{P2P}\}_{pub\_S_k} \| \{InDev_x\}_{pub\_S_k} \| \{U^x_{P2P}\}_{pub\_GridOp} \| \{InDev_x\}_{pub\_GridOp}) \end{aligned} \tag{9}$$

Naturally, the entire payload is further encrypted in line with the public-key cryptosystem used to implement the underlying distributed network of computers. The communication protocol between the network's devices is assumed to be secure, protected against tempering by external entities, and thus has been abstracted from this and all upcoming steps of the bill settlement process.

4.3 Trading Platform Protocol

The responsibility of the trading platform (TrPlat) is two-fold:

1. Calculate the partial bills of the market's users.
2. Communicate the final bills to the corresponding suppliers.

Firstly, every trading period (e.g. 30 minutes, one hour, etc.), the trading platform receives the payloads from its users (e.g. households, small businesses, etc.) which include homomorphically encrypted versions of their fine-grained energy consumption data, along with information regarding their bid/offer at the latest electricity auction. These payloads are individually stored by the TrPlat, while the individual deviation data which is encrypted using the grid operator's homomorphic public key pub_GridOp is aggregated into market-wide statistics that represent the deviations of energy supply and demand from their predicted values, described in detail in Section 4.4. The encrypted aggregate data is then sent to the GridOp for decryption. Depending on the selected billing model implemented by the trading platform, the TrPlat could continue with the partial bill calculation immediately after receiving an acknowledgement message from the GridOp (see Sections 4.3.2 and 4.3.3), or it might have to wait for the plaintext version of the aggregated statistics to arrive back from the GridOp before being able to pursue its algorithm any further, as the decrypted values are vital parts of the bill calculation algorithm (see Sections 4.3.4 and 4.3.5). After the trading slot's partial bills are computed, the TrPlat sends each supplier its own respective net balance change for that period, representing the sum of all buying/selling energy transactions with its users at the retail market (positive for making a profit, negative for making a loss), in order to help them better understand the direction the market is leaning towards (demand or supply), leading to more accurate predictions of future customer behaviour trends and making them better prepared to meet their customers' demands in the following trading periods.

Secondly, every billing period (e.g. one month), the trading platform needs to inform the suppliers of their respective customers' individual final energy bills, homomorphically encrypted using the specific supplier's public key pub_S_k, which are more likely to be negative (owing money to their supplier), than positive (being owed money by their supplier). In most of the billing models presented in this report (see Sections 4.3.3, 4.3.4, and 4.3.5), these final bills include both the bills to/from the P2P market (from energy transactions with other users) and the bills to/from the RM (from transactions directly with the energy supplier), in a single numerical value which each user pays to/receives from their supplier. The details of bill settlement and supplier responsibilities are described in Section 4.5.

4.3.1 Overview of Billing Models

The following subsections outline different billing algorithms for P2P markets with imperfect bid-offer fulfillment which run after every trading period on the trading platform, whose inputs include each user's energy volume committed to the P2P market and their individual deviation from that value, and whose outputs consist of the users' partial bills and each supplier's balance change for the respective trading slot. Evidently, all input and output values are homomorphically encrypted ciphertext, in order to preserve the privacy of user bills and fine-grained energy measurements. Moreover, each billing algorithm is run twice every trading period, once using inputs encrypted with the corresponding supplier's public key pub_S_k and once using those encrypted with the grid operator's public key pub_GridOp. The rationale behind this requirement is comprehensively explained in step 2 of Section 4.2.

The four implemented billing models have been adapted from [33], with all of them being modified to allow for the use of Paillier homomorphic encryption. Furthermore, the Status Quo algorithm (see Section 4.3.2) has been adapted to fit the type of payload described in Section 4.2, and the Social Cost Split (see Section 4.3.4) and Universal Cost Split (see Section 4.3.5) billing models have also been improved by adding a weighted redistribution of the total volume of energy over-consumed (under-produced) or under-consumed (over-produced) by reselling it at the trading price (TP) to each user whose $InDev_x$ negatively influenced the balance of the electricity grid (pushed the corresponding aggregated deviation value away from 0), according to each respective user's proportional contribution to the total deviation TD, total supply deviation TSD, and total demand deviation TDD, instead of the equal redistribution implemented and analysed by [33]. Notations are listed in the Notations section.

4.3.2 Billing Model for Retail Markets – the Status Quo

The status quo in most of the liberalised energy retail markets (RM) around the world allows consumers and consumers to trade electrical energy only directly with their contracted supplier at the RM. This exclusivity deal forbids any energy trading between local consumers and prosumers, their only option being buying to/selling from one of the accredited energy providers. Any excess of energy produced by prosumers that is fed into the power grid is regulated and bought by suppliers at a unique tariff, called the Feed-In Tariff (FiT), which is standardised at the country level by the respective market regulator. Therefore, users have little to no incentive to adopt renewable energy sources or change their load profiles. Moreover, in the presence of an imperfect bill-offer fulfillment assumption, whereby the users' actual consumption data is expected to deviate slightly from the predicted values, neither consumers nor prosumers have any reason to reduce their individual deviations, which would help minimise the grid-balancing cost.

The billing model that illustrates the status quo has been described in detail in Algorithm 2. The

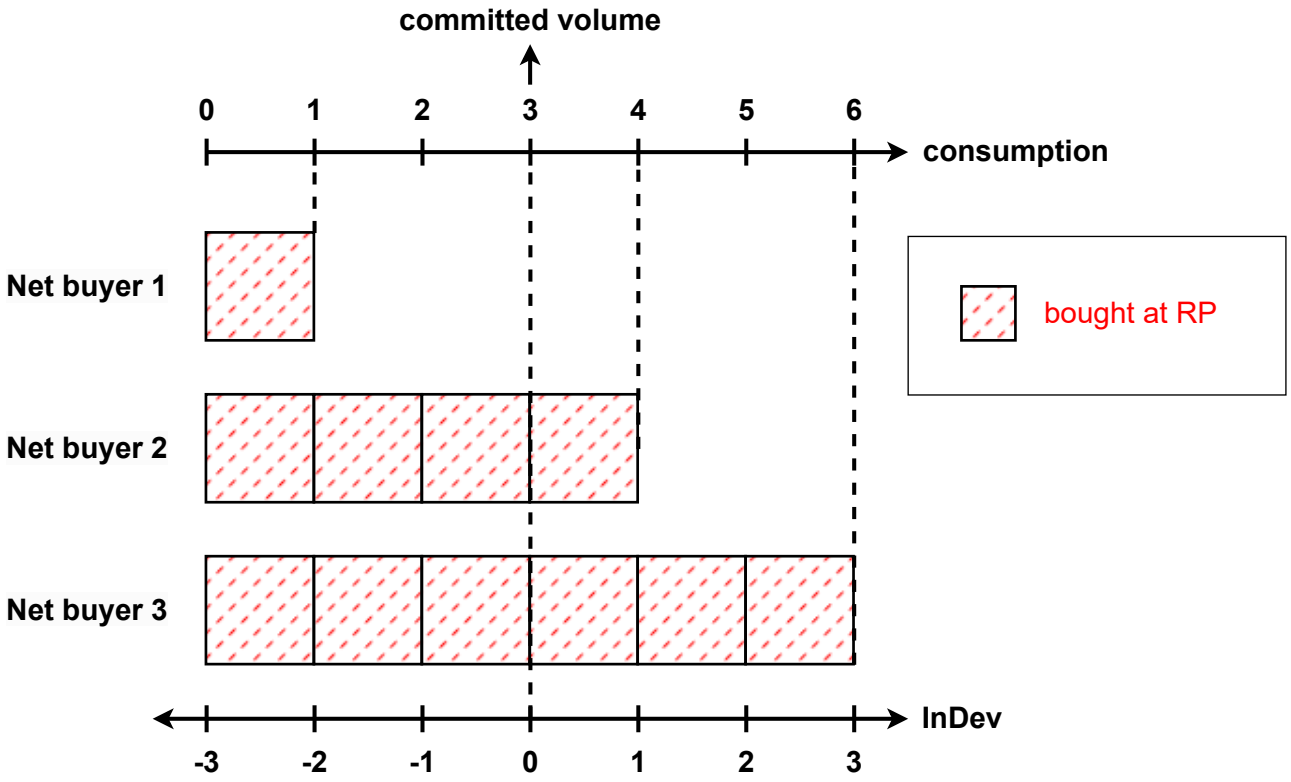


Fig. 10. Status quo billing example.

version of the algorithm presented in this report has been designed to function for both Non-P2P and P2P users, using the payload format outlined in Section 4.2. In the case of Non-P2P users, it is just a privacy-preserving version of the worldwide status quo, while for P2P users, it represents the fall-back option for bids that were not accepted at the P2P market, which still need to be settled somehow. However, the desire is for as many bids as possible to be accepted at the energy auction, such that fewer partial bills are calculated using this billing model.

The appropriate naming convention for the two types of users in the RM billing model is net buyers and net sellers, with the former consuming more energy than they produce, and the latter doing the opposite. This is a departure from the usual nomenclature used throughout this report, which otherwise splits users into consumers and prosumers, because these terms only refer to a user's type of bid/offer at the energy auction, rather than their actual meter readings with which the Status Quo algorithm is concerned. Figure 10 showcases an example market with three net buyers, whose entire need for electricity is fulfilled at the RM.

A summary of the privacy-enhancing status quo algorithm is given below:

- The payloads of P2P users, which separate the half-hourly consumption data into the volume committed to the P2P market $\{U^x_{P2P}\}_{pub\_S_k}$ and the household's deviation from that volume $\{InDev_x\}_{pub\_S_k}$, are converted back into a single value for the actual meter reading $\{U^x_{val}\}_{pub\_S_k}$. The encrypted consumption data in Non-P2P payloads is already formatted in the appropriate style and does not require any alterations.

Algorithm 2 Billing Model for Retail Markets

procedure NET BUYER BILLS, NET SELLER REWARDS, SUPPLIER BALANCE
for each timeslot **do**
  for each x, k in U_n, S_n **do**
    if user is P2P **then**
      $\{U^x_{val}\}_{pub\_S_k}$ = $\{U^x_{P2P}\}_{pub\_S_k}$ + $\{InDev_x\}_{pub\_S_k}$
    end if
    if $net\_consumption\_type \neq bid\_type$ **then**
      $\{U^x_{val}\}_{pub\_S_k}$ = $-\{U^x_{val}\}_{pub\_S_k}$
    end if
    if user is net buyer **then**
      $\{U^x$ bill$\}_{pub_S_k}$ = $\{U^x_{val}\}_{pub\_S_k} \times$ RP
      $\{S^{inc}_k\}_{pub\_S_k}$ += $\{U^x$ bill$\}_{pub_S_k}$
    end if
    if user is net seller **then**
      $\{U^x$ reward$\}_{pub_S_k}$ = $\{U^x_{val}\}_{pub\_S_k} \times$ FiT
      $\{S^{exp}_k\}_{pub\_S_k}$ += $\{U^x$ reward$\}_{pub_S_k}$
    end if
    $\{S^{bal}_k\}_{pub\_S_k}$ += $\{S^{inc}_k\}_{pub\_S_k} - \{S^{exp}_k\}_{pub\_S_k}$
  end for
end for

- Net buyers can purchase electricity solely from their suppliers at a retail price (RP). The suppliers set the RP, and typically present consumers with multiple tariffs to choose from, ensuring that their prices remain competitive with those of other energy suppliers.
- Net sellers are limited to selling their surplus of electrical energy to suppliers at a fixed rate, commonly referred to as FiT. Depending on the country, the FiT may vary based on the type and size of the renewable energy source used by the user to generate electricity.
- Energy suppliers are responsible for selling electricity to the customers with whom they have signed exclusive contracts, while also buying back any excess electricity that these users return to the grid.

With all electricity transactions involving the suppliers, the volume traded at the RM for the status quo is equal to the sum of all measured consumption volumes:

$$V^{RM}_{SQ} = \sum_{x=1}^{U_n} |U^x_{val}| \tag{10}$$

It must be noted that suppliers are very likely to profit from transactions at the RM, especially when generalising to the level of their entire customer base, since the price they sell energy at, the RP, is much higher than the price at which they buy energy back from the users, the FiT. For example, even in a case where the energy consumption of the user base is equal to its surplus energy production, and thus the volume sold is equal to the volume bought at the RM, the supplier, being the only allowed trading partner for any individual customer, will always accrue a sizeable profit. Therefore, the

status quo greatly favours the suppliers, giving little-to-no incentive for net sellers to ever produce more electrical energy than they themselves require, as the excess volume sold at the RM will only grant them a marginal capital gain.

With this in mind, the need for billing models for P2P markets that allow users to trade energy among themselves becomes apparent. Three such models for P2P markets with the RM as back-up are described in the following subsections.

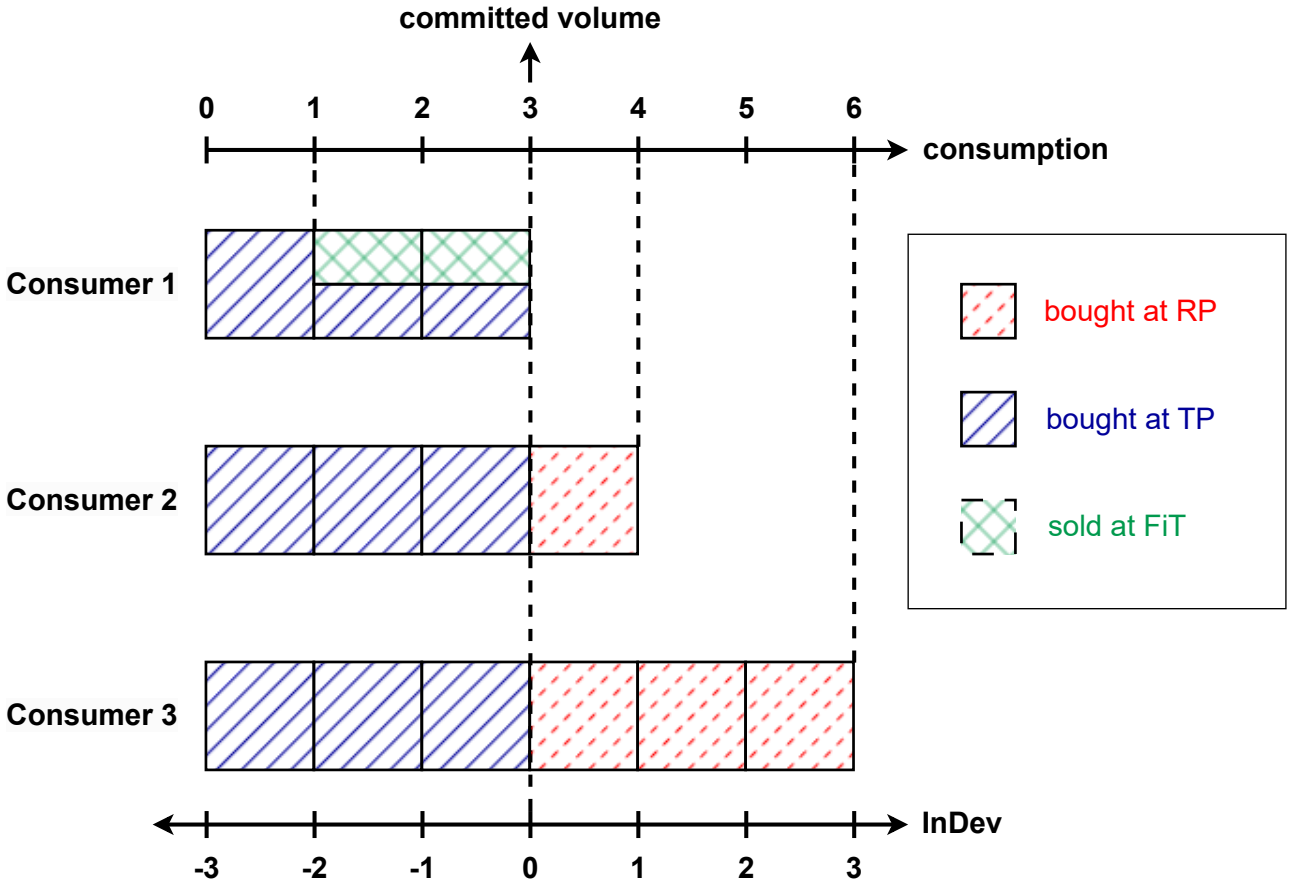


Fig. 11. Individual cost split billing example.

4.3.3 Billing Model with Individual Cost Split

This billing algorithm makes each P2P user independently responsible for trading away/compensating for their individual deviations from the committed bids/offers, by buying/selling the electricity deficit/surplus at the retail market (RM), while the committed volumes are traded at trading price (TP). Negative deviations must be compensated for at the RM in order for the P2P trade commitments to be fulfilled, while positive deviations of both consumers and prosumers are also traded directly at this back-up market. Figure 11 illustrates an example market with three individual consumers whose committed volumes are all 3 kWh, highlighting the use of the RM to either sell their negative deviation (Consumer 1) or purchase their positive deviations (Consumer 2 and Consumer 3).

Algorithm 3 Billing Model with Individual Cost Split

procedure CUSTOMER BILLS, PROSUMER REWARDS, SUPPLIER BALANCE
for each timeslot **do**
  if bid accepted **then**
    for each i, j and k in $P2P_n^c$, $P2P_n^p$ and S_n **do**
      if $sign(InDev_x) = 0$ **then**
        $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $\{C_{dem}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $\{P_{sup}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{S_k^{inc}\}_{pub\_S_k}$ += 0; $\{S_k^{exp}\}_{pub\_S_k}$ += 0
      end if
      if $sign(InDev_x) < 0$ **then**
        $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $\{C_{dem}^{P2P}\}_{pub\_S_k} \times$ TP + $\{InDev_i\}_{pub\_S_k} \times$ FiT
        $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $\{P_{sup}^{P2P}\}_{pub\_S_k} \times$ TP + $\{InDev_j\}_{pub\_S_k} \times$ RP
        $\{S_k^{inc}\}_{pub\_S_k}$ -= $\{InDev_j\}_{pub\_S_k} \times$ RP
        $\{S_k^{exp}\}_{pub\_S_k}$ -= $\{InDev_i\}_{pub\_S_k} \times$ FiT
      end if
      if $sign(InDev_x) > 0$ **then**
        $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $\{C_{dem}^{P2P}\}_{pub\_S_k} \times$ TP + $\{InDev_i\}_{pub\_S_k} \times$ RP
        $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $\{P_{sup}^{P2P}\}_{pub\_S_k} \times$ TP + $\{InDev_j\}_{pub\_S_k} \times$ FiT
        $\{S_k^{inc}\}_{pub\_S_k}$ += $\{InDev_i\}_{pub\_S_k} \times$ RP
        $\{S_k^{exp}\}_{pub\_S_k}$ += $\{InDev_j\}_{pub\_S_k} \times$ FiT
      end if
      $\{S_k^{bal}\}_{pub\_S_k}$ = $\{S_k^{inc}\}_{pub\_S_k} - \{S_k^{exp}\}_{pub\_S_k}$
    end for
  end if
  if bid not accepted **then**
    for each i, j and k in C_n, P_n and S_n **do**
      goto Algorithm 2
    end for
  end if
end for

The specifics of the privacy-preserving Individual Cost Split billing model are shown in Algorithm 5 and are outlined below:

- Positive deviations of consumers (i.e when a consumer consumes more energy than their committed volume) are bought at RP from their contracted energy supplier.
- Negative deviations of consumers (i.e. when a consumer consumes less energy than they committed in their bid) are also compensated at the RM. The committed energy volume must still be purchased in its entirety from the P2P market at TP as the bid dictates, despite not being consumed completely, and is then sold at a fixed FiT to their corresponding energy supplier.
- Positive deviations of prosumers (i.e when a prosumer produces more electricity than their committed volume) are sold directly to their supplier at the FiT.
- Negative deviations of prosumers (i.e. when a prosumer produces less electricity than they

committed in their offer) are also compensated at the RM. Since the prosumer must nevertheless offer to the P2P market the volume of energy they committed, the difference is bought from their contracted supplier at RP and immediately sold at TP to the P2P market.

- Consumers/prosumers with no individual deviation only trade their energy volumes at TP.
- Energy suppliers are responsible for selling electricity at RP to under-supplying prosumers ($InDev_j < 0$) and over-consuming consumers ($InDev_i > 0$). They also purchase electricity at FiT from over-supplying prosumers ($InDev_j > 0$) and under-consuming consumers ($InDev_i < 0$).
- Consumers/prosumers whose bids/offers were not accepted at the auction trade their entire consumption/production with the respective supplier at RP and FiT, according to Algorithm 2.

With all individual deviations being independently traded at the RM, whether bought or sold, the total volume of energy traded with the suppliers is equal to the sum of the absolute values of every consumer's/prosumer's deviation:

$$V_{Ind}^{RM} = \sum_{i=1}^{P2P_n^c} |InDev_i| + \sum_{j=1}^{P2P_n^p} |InDev_j| \tag{11}$$

However, it is not ideal for individual deviations to be traded independently of each other. For example, assuming a system with 2 consumers, the first having a deviation $InDev_1 = 2$, and the other $InDev_2 = -2$, there is effectively no need for each of them to resolve their deviations with their supplier independently, as they would both benefit from compensating for one another, since an under-consumer balances out an equivalent over-consumer on the power grid. Intuitively, the under-consumer sells the unused electricity they bought at TP from the P2P market to the over-consumer at the same TP. The former benefits from selling their excess energy at TP instead of the lower FiT, while the latter benefits from buying their electricity deficit at TP instead of the higher RP. Therefore, in order to minimise the volume traded at the RM, reduce consumer bills and increase prosumer rewards, it is possible for the consumers (over-consuming and under-consuming) to compensate for each other, with the prosumers (over-supplying and under-supplying) also doing the same. Such a billing model is introduced in the next subsection.

4.3.4 Billing Model with Weighted Social Cost Split

This billing model uses the aggregated individual deviations of consumers to socially split the cost among them proportionally to each consumer household's effect on the total demand deviation. Similarly, the prosumers' deviations are aggregated into a single value which is split among prosumers according to their contribution to the total supply deviation. Because this model makes use of aggregated values of encrypted meter readings in calculating the partial bills, the trading platform must wait for the decrypted statistics to arrive from the grid operator before continuing its algorithm.

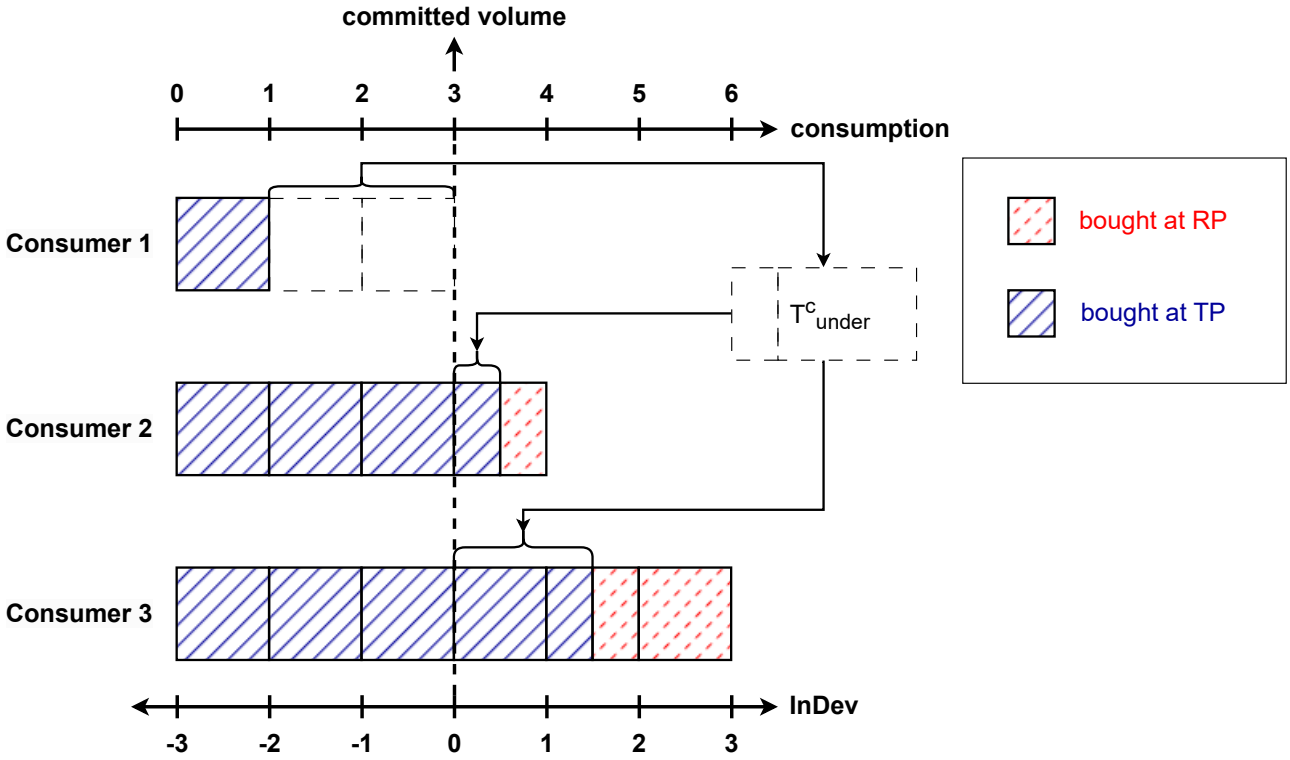


Fig. 12. Weighted social cost split billing example.

Figure 12 illustrates an over-consuming market with three individual consumers whose committed volumes are all 3 kWh, highlighting the weighted redistribution of electricity bought at TP from the one under-consumer (Consumer 1) to the two over-consumers (Consumer 2 and Consumer 3), before using the RM as a fall-back.

The characteristics of the privacy-preserving Weighted Social Cost Split billing model are shown in Algorithm 4 and described below:

- The total demand deviation (TDD) is calculated as the sum of all consumer individual deviations. The total supply deviation (TSD) represents the aggregate of all prosumer individual deviations.
- If the TDD is equal to zero, then all consumers buy their entire consumed energy volume at TP, regardless of their individual deviations. This benefits both under-consumers, since they do not need to sell their excess electricity at FiT to the RM, and the over-consumers, as they are not forced to buy their electricity deficit at RP from their supplier. The case where the TSD is zero is analogous.
- A positive TDD indicates that the consumers, as a whole, over-consumed in relation to the total volume bought at the P2P market. Therefore, the under-consumers only partially compensate for the over-consumers. Effectively, the under-consumers buy their committed energy volumes at TP and then sell on the unused electricity to the over-consumers also at TP. Such, the total volume under-consumed T^c_{under} disappears from the under-consumers' bills and is proportion-

Algorithm 4 Billing Model with Weighted Social Cost Split

for each timeslot **do**
  if bid accepted **then**
    procedure CUSTOMER BILLS, SUPPLIER INCOME/EXPENDITURE
    for each i and k in $P2P_n^c$ and S_n **do**
      if TDD = 0 **then**
        $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $\{C_{dem}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{S_k^{inc}\}_{pub\_S_k}$ += 0
      end if
      if TDD < 0 **then**
        if $sign(InDev_i) \geq 0$ **then**
          $\{P2P_c^i \text{ bill }\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k}) \times$ TP
          $\{S_k^{inc}\}_{pub\_S_k}$ += 0
        end if
        if $sign(InDev_i) < 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k} \times \frac{T_{over}^c}{T_{under}^c}) \times$ TP $+ \{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{over}^c}{T_{under}^c}) \times$ FiT
          $\{S_k^{exp}\}_{pub\_S_k}$ -= $\{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{over}^c}{T_{under}^c}) \times$ FiT
        end if
      end if
      if TDD > 0 **then**
        if $sign(InDev_i) \leq 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k}) \times$ TP
          $\{S_k^{inc}\}_{pub\_S_k}$ += 0
        end if
        if $sign(InDev_i) > 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k} \times \frac{T_{under}^c}{T_{over}^c}) \times$ TP $+ \{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{under}^c}{T_{over}^c}) \times$ RP
          $\{S_k^{inc}\}_{pub\_S_k}$ += $\{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{under}^c}{T_{over}^c}) \times$ RP
        end if
      end if
      $\{S_k^{bal}\}_{pub\_S_k}$ = $\{S_k^{inc}\}_{pub\_S_k} - \{S_k^{exp}\}_{pub\_S_k}$
    end for
    end procedure
    procedure PROSUMER REWARDS, SUPPLIER INCOME/EXPENDITURE
    for each j and k in $P2P_n^p$ and S_n **do**
      if TSD = 0 **then**
        $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $\{P_{sup}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{S_k^{exp}\}_{pub\_S_k}$ += 0
      end if
      if TSD < 0 **then**
        if $sign(InDev_j) \geq 0$ **then**
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k}) \times$ TP
          $\{S_k^{exp}\}_{pub\_S_k}$ += 0
        end if
        if $sign(InDev_j) < 0$ **then**
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k} \times \frac{T_{over}^p}{T_{under}^p}) \times$ TP $+ \{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{over}^p}{T_{under}^p}) \times$ RP
          $\{S_k^{inc}\}_{pub\_S_k}$ -= $\{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{over}^p}{T_{under}^p}) \times$ RP
        end if
      end if
      if TSD > 0 **then**
        if $sign(InDev_j) \leq 0$ **then**
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k}) \times$ TP
          $\{S_k^{exp}\}_{pub\_S_k}$ += 0
        end if
        if $sign(InDev_j) > 0$ **then**
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k} \times \frac{T_{under}^p}{T_{over}^p}) \times$ TP $+ \{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{under}^p}{T_{over}^p}) \times$ FiT
          $\{S_k^{exp}\}_{pub\_S_k}$ += $\{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{under}^p}{T_{over}^p}) \times$ FiT
        end if
      end if
      $\{S_k^{bal}\}_{pub\_S_k}$ = $\{S_k^{inc}\}_{pub\_S_k} - \{S_k^{exp}\}_{pub\_S_k}$
    end for
  end if

  if bid not accepted **then**
    for each i, j and k in C_n, P_n and S_n **do**
      goto Algorithm 2
    end for
  end if
end for=0

ately redistributed to the over-consumers' bills, based on each over-consumer's contribution to the total volume over-consumed T^c_{over}. In practice, consumers that under-consumed buy their actual energy consumption volume at TP, regardless of their individual deviation, while the consumers who over-consumed buy their committed volume at TP, an additional proportion of the compensated energy at TP, and the rest of their consumption at RP from the RM. As a result, under-consumers benefit from buying their exact energy consumption at TP, rather than buying the larger committed volume at TP and selling the deviation at FiT, while the over-consumers gain by buying part of their individual deviation at TP and the rest at RP, instead of purchasing it all at RP.

- A negative TDD indicates that the consumers, as a whole, under-consumed, leaving excess energy on the grid, and the over-consumers can only partly compensate for the under-consumers. In essence, the under-consumers again buy their committed energy volumes at TP and then sell on proportions of their individual deviations to the over-consumers also at TP. The proportions resold at TP are based on each under-consumer's contribution to the total volume under-consumed T^c_{under} and add up to the value of the total volume over-consumed T^c_{over}. Therefore, the over-consumers purchase their entire actual energy consumption volume at TP, whereas the under-consumers, after reselling an appropriate part of their individual deviation at TP, sell the rest at FiT to the supplier. As a result, the over-consumers benefit by buying their total energy consumption at TP, instead of buying the committed volume at TP and their deviation at RP, and the under-consumers gain by selling part of their individual deviation at TP and the rest at FiT, rather than selling it all at FiT.

- Similarly, the cases for prosumers are analogous. If the TSD is positive (negative), then the aggregate deviation of prosumers who under-supplied (over-supplied) partially compensates for the prosumers who over-supplied (under-supplied). Under-suppliers (over-suppliers) sell all their produced electricity at the TP regardless of their individual deviation, while the prosumers who over-supplied (under-supplied) reduce their individual deviation with a proportional share of the total deviation of consumers who under-supplied T^p_{under} (over-supplied T^p_{over}), determined by their contribution to the total volume over-supplied T^p_{over} (under-supplied T^p_{under}). Therefore, prosumers benefit either by selling their entire production at TP or by reducing the revenue loss incurred by their individual deviations, which must be compensated for at the RM.

- Energy suppliers only trade electricity with those consumers/prosumers whose individual deviation sign is the same as the sign of the TDD/TSD respectively.

- Users whose bids/offers were not accepted at the auction must trade their entire consumption/production at the retail market at RP and FiT, according to Algorithm 2.

By dealing with consumer bills separately from prosumer rewards, the total volume of electricity traded with the energy suppliers is equal to the sum of the absolute values of TDD and TSD, with the

former representing the sum of all consumer deviations, and the latter constituting the sum of all prosumer deviations:

$$V_{Soc}^{RM} = |\sum_{i=1}^{P2P_n^c} InDev_i| + |\sum_{j=1}^{P2P_n^p} InDev_j| \tag{12}$$

Clearly, the billing model is still not optimal because of this separation between the consumers' and prosumers' effect on the balance of the grid. For instance, assuming a total supply deviation TSD $= 2$ and a total demand deviation TDD $= 2$, both consumers and prosumers would benefit from compensating for one another. Intuitively, the users which increase the total deviation of the grid (TD) by producing a surplus of electricity (over-suppliers) or by not fulfilling their consumption commitments (under-consumers) sell their individual deviations at the TP to the households which decrease the TD by producing less energy than they committed to (under-suppliers) or by consuming more electricity than they bid for (over-consumers). It is also important to note that a positive value of TSD has the same effect on the load on the power grid as an opposite-valued negative TDD, with the former indicating an over-consumption trend, and the latter an under-production tendency, both leading to a deficit of electricity. The opposite also holds. A billing algorithm that implements this idea is presented next.

4.3.5 Billing Model with Weighted Universal Cost Split

The final billing model is concerned with the total deviation of the P2P market, an aggregate value of all individual deviations of both consumers and prosumers, which is split among those users whose deviations are in the same direction as the TD, in proportion to their contribution to the aggregate value. Similarly to the Weighted Social Cost Split (see Section 4), the trading platform is forced to wait for the communication of the decrypted aggregate P2P market statistics before starting the partial bill calculation phase. Figure 13 showcases an example market with three individual consumers and three individual prosumers whose committed volumes are all 3 kWh, highlighting the weighted redistribution of electricity at TP from the one under-consumer (Consumer 1) and one over-supplier (Prosumer 2) to the two over-consumers (Consumer 2 and Consumer 3), before using the RM as a fall-back.

For the rest of this section, users who push the TD up by under-consuming or over-supplying will also be referred to as uptrenders, while those who pull the TD down by over-consuming or under-supplying will also be called downtrenders. The exact implementation of the privacy-preserving Weighted Universal Cost Split billing model is illustrated in Algorithm 5 and explained below:

- The total deviation (TD) is calculated as the sum of all prosumer deviations minus the sum of all consumer deviations, equivalent to the difference between the total supply deviation (TSD) and the total demand deviation (TDD).

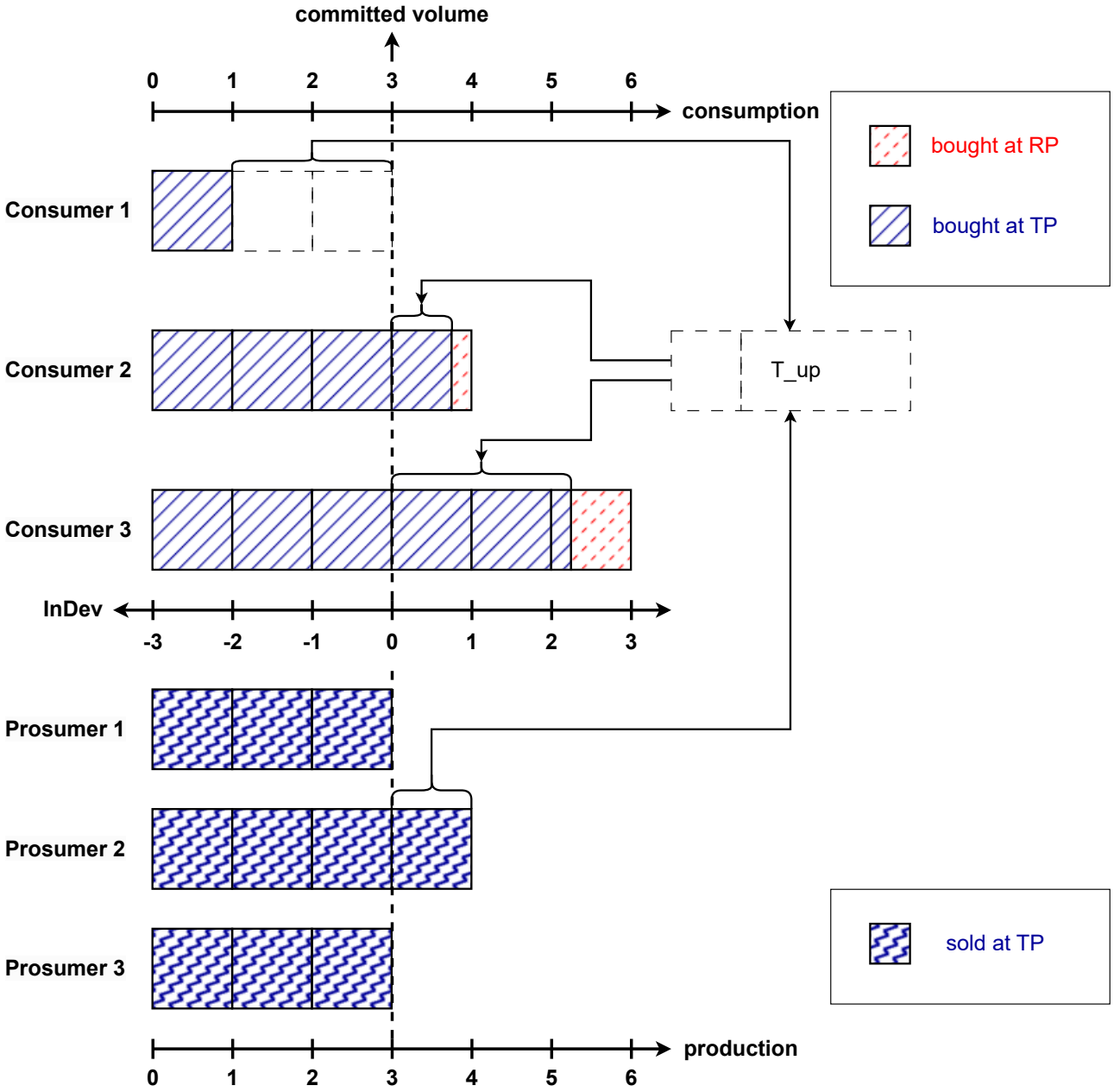


Fig. 13. Weighted universal cost split billing example.

- If the TD is zero, then all users participating in the P2P market buy/sell their actual energy readings at TP, disregarding the specific committed volumes or the individual deviations.

- A positive TD indicates that the total volume under-consumed or over-supplied $T\_up = T^c_{under} + T^p_{over}$ is greater than the total volume over-consumed or under-supplied $T\_down = T^c_{over} + T^p_{under}$, total supply being greater than the total demand for electricity. In this case, all downtrenders (over-consumers/under-suppliers) trade their exact energy meter readings entirely at TP, while the uptrenders (under-consumers/over-suppliers) partly compensate for their individual deviations. More specifically, under-consumers buy their committed volumes at TP, sell a proportion of their individual deviation to downtrenders also at TP, and the rest at FiT to suppliers, instead of selling the entire individual deviation at FiT. The over-suppliers sell their committed volumes at TP as usual, but also a share of their respective deviation at TP, before

Algorithm 5 Billing Model with Weighted Universal Cost Split

procedure CUSTOMER BILLS, PROSUMER REWARDS, SUPPLIER BALANCE
for each timeslot **do**
  if bid Accepted **then**
    for each i, j and k in $P2P_n^c$, $P2P_n^p$ and S_n **do**
      if TD = 0 **then**
        $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $\{C_{dem}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $\{P_{sup}^{P2P}\}_{pub\_S_k} \times$ TP
        $\{S_k^{inc}\}_{pub\_S_k}$ += 0; $\{S_k^{exp}\}_{pub\_S_k}$ += 0
      end if
      if TD < 0 **then**
        $\{S_k^{exp}\}_{pub\_S_k}$ += 0
        if $sign(InDev_x) \leq 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k}) \times$ TP
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k} \times \frac{T_{up}}{T_{down}}) \times$ TP $+ \{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{up}}{T_{down}}) \times$ RP
          $\{S_k^{inc}\}_{pub\_S_k}$ -= $\{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{up}}{T_{down}}) \times$ RP
        end if
        if $sign(InDev_x) > 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k} \times \frac{T_{up}}{T_{down}}) \times$ TP $+ \{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{up}}{T_{down}}) \times$ RP
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k}) \times$ TP
          $\{S_k^{inc}\}_{pub\_S_k}$ += $\{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{up}}{T_{down}}) \times$ RP
        end if
      end if
      if TD > 0 **then**
        $\{S_k^{inc}\}_{pub\_S_k}$ += 0
        if $sign(InDev_x) \leq 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k} \times \frac{T_{down}}{T_{up}}) \times$ TP $+ \{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{down}}{T_{up}}) \times$ FiT
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k}) \times$ TP
          $\{S_k^{exp}\}_{pub\_S_k}$ -= $\{InDev_i\}_{pub\_S_k} \times (1 - \frac{T_{down}}{T_{up}}) \times$ FiT
        end if
        if $sign(InDev_x) > 0$ **then**
          $\{P2P_c^i \text{ bill}\}_{pub\_S_k}$ = $(\{C_{dem}^{P2P}\}_{pub\_S_k} + \{InDev_i\}_{pub\_S_k}) \times$ TP
          $\{P2P_p^j \text{ reward}\}_{pub\_S_k}$ = $(\{P_{sup}^{P2P}\}_{pub\_S_k} + \{InDev_j\}_{pub\_S_k} \times \frac{T_{down}}{T_{up}}) \times$ TP $+ \{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{down}}{T_{up}}) \times$ FiT
          $\{S_k^{exp}\}_{pub\_S_k}$ += $\{InDev_j\}_{pub\_S_k} \times (1 - \frac{T_{down}}{T_{up}}) \times$ FiT
        end if
      end if
      $\{S_k^{bal}\}_{pub\_S_k}$ += $\{S_k^{inc}\}_{pub\_S_k} - \{S_k^{exp}\}_{pub\_S_k}$
    end for
  end if
  if bid not accepted **then**
    for each i, j and k in C_n, P_n and S_n **do**
      goto Algorithm 2
    end for
  end if
end for

trading the rest at FiT to the RM. These proportions of the sold at TP are based on each respective uptrender's contribution to the total volume under-consumed/over-supplied T_up, and sum up to the total volume over-consumed/under-supplied T_down.

- A negative TD suggests that the energy demand exceeds the energy supply, with the total volume over-consumed or under-supplied T_down being greater than the total volume under-consumed or over-supplied T_up. In this case, all uptrenders (under-consumers/over-suppliers) buy/sell their final meter readings at TP, regardless of their original committed volumes or deviations, while the downtrenders partially reduce the cost of their individual deviations. In particular, over-consumers purchase their committed volumes at TP as usual, but also a portion of their individual deviation at TP, before buying the rest at RP from the supplier, instead of trading for their entire deficit at RP. Likewise, under-suppliers sell their committed volumes at TP as always, then buy a share of their respective deviation from the uptrenders also at TP,

before purchasing the rest of the difference at RP from the RM, instead of making up for their whole individual deviation from trading with the suppliers.

- Energy suppliers only trade electricity with the users whose individual deviations point in the same direction as the TD.
- Unaccepted bids/offers are settled according to Algorithm 2.

Out of the four billing models presented, this algorithm is the one with the lowest energy volume traded at the RM, which favours the users as the electricity price at the P2P market is advantageous to the one offered by the suppliers. Specifically, the volume traded with the energy suppliers is equal to the absolute value of the sum of all individual deviations of consumers/prosumers:

$$V_{Univ}^{RM} = |\sum_{i=1}^{P2P_n^c} InDev_i + \sum_{j=1}^{P2P_n^p} InDev_j| = |\sum_{x=1}^{P2P_n} InDev_x| \tag{13}$$

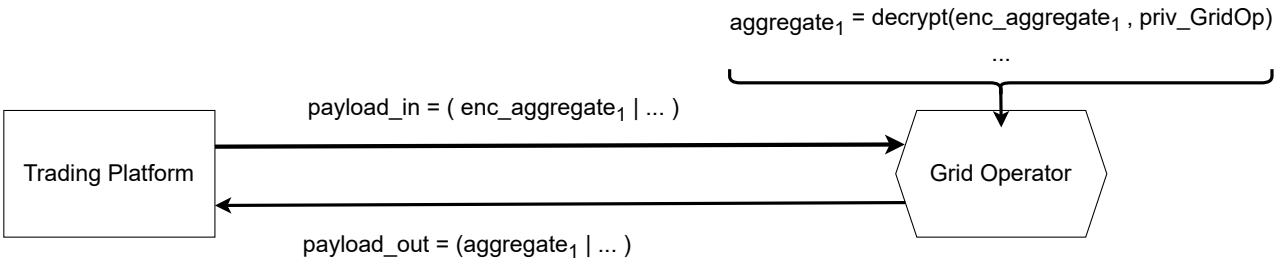


Fig. 14. Grid Operator protocol.

4.4 Grid Operator Protocol

The grid operator is a trusted third party (TTP) whose responsibility is to decrypt the incoming aggregated values describing the P2P market, to communicate their plaintext form back to the trading platform, and to act as a supervisor of supplier honesty, having the ability to check the final reported bills using the backup values calculated and stored by the trading platform during the billing period. Its protocol is illustrated in Figure 14. For each trading period, the grid operator's instructions are separated into the following steps, also illustrated in Algorithm 6:

1. Receive a list of encrypted aggregate values in the form of an incoming payload comprising of the total volume under-consumed, over-consumed, under-supplied, and over-supplied by the P2P users:

$$payload\_in = (\{T_{under}^c\}_{pub\_GridOp} \| \{T_{over}^c\}_{pub\_GridOp} \| \{T_{under}^p\}_{pub\_GridOp} \| \{T_{over}^p\}_{pub\_GridOp}) \tag{14}$$

Algorithm 6 Grid Operator Protocol

0: **procedure** DECRYPTED AGGREGATES($payload\_in$)
1: T^c_{under} = $Dec\left(\{T^c_{under}\}_{pub\_GridOp}, priv\_GridOp\right)$
2: T^c_{over} = $Dec\left(\{T^c_{over}\}_{pub\_GridOp}, priv\_GridOp\right)$
3: T^p_{under} = $Dec\left(\{T^p_{under}\}_{pub\_GridOp}, priv\_GridOp\right)$
4: T^p_{over} = $Dec\left(\{T^p_{over}\}_{pub\_GridOp}, priv\_GridOp\right)$
5: **return** $payload\_out = (T^c_{under} \| T^c_{over} \| T^p_{under} \| T^p_{over})$

2. Decrypt each of the homomorphically encrypted values using the corresponding private key of the grid operator $priv\_GridOp$:

$$decrypt\left(\{X\}_{pub\_GridOp}, priv\_GridOp\right) = X, \text{where } \{X\}_{pub\_GridOp} \in payload\_in \tag{15}$$

3. Send the plaintext versions of the received values back to the trading platform;

$$payload\_out = (T^c_{under} \| T^c_{over} \| T^p_{under} \| T^p_{over}) \tag{16}$$

In addition to these four incoming aggregates, the trading platform also uses the total deviation (TD), total demand deviation (TDD), and total supply deviation (TSD) in some of the billing models (see Sections 4 and 5). However, all of them can be derived from the more specific deviation aggregates and should not be redundantly communicated over the network:

$$\text{TDD} = T^c_{over} - T^c_{under} \tag{17}$$

$$\text{TSD} = T^p_{over} - T^p_{under} \tag{18}$$

$$\text{TD} = \text{TSD} - \text{TDD} \tag{19}$$

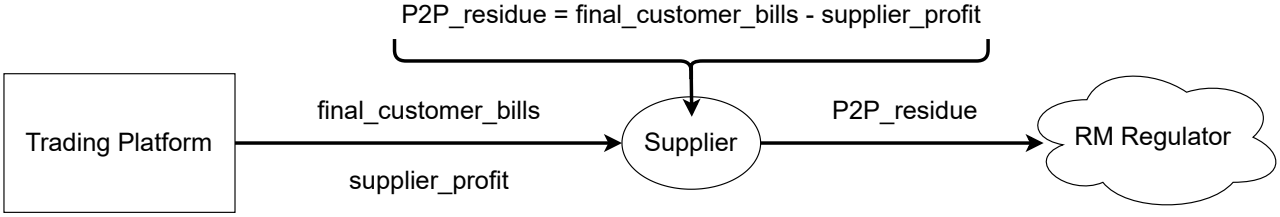


Fig. 15. Supplier protocol.

4.5 Supplier Protocol

Energy suppliers are responsible for settling the final monthly bills with their contracted customers, as well as ensuring that all payments to/from the P2P market sent/received by these customers, which are included in their final bill, are distributed accordingly across the other suppliers, as illustrated in Figure 15. The supplier operates in two phases:

- Every trading period, the supplier receives its aggregate profit from all customer transactions in that slot $\{S_k^{bal\_i}\}_{pub\_S_k}$, which is decrypted using their homomorphic private key $priv\_S_k$:

$$decrypt\left(\{S_k^{bal\_i}\}_{pub\_S_k}, priv\_S_k\right) = S_k^{bal\_i} \tag{20}$$

  From this value, whether negative or positive, they can infer if the market is trending more toward supply or demand, adjusting their offer and preparing for the next trading period appropriately.

- At the end of every billing period, the supplier must resolve the final bills, a process which is separated into multiple steps and illustrated in Algorithm 7:

  1. Calculate total monthly profit using the partial profits communicated throughout the billing period:

$$S_k^{bal} = \sum_{i=1}^{no\_slots} S_k^{bal\_i} \tag{21}$$

  2. Receive from the trading platform the final electricity bill of each of their customers, which includes both the value these users need to pay to the P2P market and to the RM. They decrypt each of the bills using their homomorphic private key $priv\_S_k$:

$$decrypt\left(\{P2P^x \text{ bill/reward}\}_{pub\_S_k}, priv\_S_k\right) = P2P^x \text{ bill/reward} \tag{22}$$

  3. Carry out the billing process with customers by receiving compensation for the bills from their overall net buyers and paying out the rewards of their overall net sellers of electricity.

  4. Calculate the left-over capital which was traded at the P2P market by subtracting the total supplier profit from the aggregate customer bills:

$$S_k^{P2P} = \left(\sum_{i=1}^{P2P_{n,k}^c} P2P_c^i \text{ bill} - \sum_{j=1}^{P2P_{n,k}^p} P2P_p^j \text{ reward}\right) - S_k^{bal} \tag{23}$$

  5. Submit the value of the P2P trade residue S_k^{P2P} to the retail market regulator in order to facilitate the fair redistribution of the remaining capital among the other suppliers.

Algorithm 7 Supplier Protocol

0: **procedure** SUPPLIER PROFIT
1: **for** each i in no_slots **do**
2: S_k^{bal} += $S_k^{bal\_i}$
3: **end for**
4: **for** each i, j in $P2P_{n,k}^c$, $P2P_{n,k}^p$ **do**
5: $P2P_c$ bills += $Dec\left(\{P2P_c^i \text{ bill}\}_{pub\_S_k}, priv\_S_k\right)$
6: $P2P_p$ rewards += $Dec\left(\{P2P_p^j \text{ reward}\}_{pub\_S_k}, priv\_S_k\right)$
7: **end for**
8: **return** S_k^{P2P} = $(P2P_c \text{ bills} - P2P_p \text{ rewards}) - S_k^{bal}$

The intuition behind the left-over balance from the P2P market associated with each supplier is best explained by studying a simple example. Let us assume a system with only one consumer C_1 contracted to supplier S_1 and only one prosumer P_1 contracted to another supplier S_2, where C_1 buys electricity from P_1 at the P2P market. In this case, S_1 will receive money from C_1 for that volume of energy, while S_2 will have to send money to P_1 accordingly. What is left is for S_1 to pay the appropriate value to S_2, and the bill settlement is complete. In a sense, suppliers act as intermediaries for P2P trades. Therefore, without a mechanism for redistributing the capital between suppliers, some would be left with unfair deficits, and others with a surplus of capital.

After all these left-over balances are submitted to the market regulator, it is checked whether their sum is equal to zero (since the electricity sold must be equal to the electricity bought), indicating that the entire P2P trade has been accounted for and that the values communicated by the suppliers are accurate. In the case of a non-zero value, the grid operator is called upon to verify the calculated values using the backup information stored by the trading platform, encrypted using the grid operator's homomorphic public key. Subsequently, any dishonest supplier is punished accordingly to prevent such behaviour in the future.

If the data-gathering step proceeds smoothly, with no inconsistencies detected, the retail market regulator is tasked with managing the fair transfer of funds between energy suppliers, such that all P2P trade residues are sorted out. An example of such a regulator in the UK is Elexon [60], whose main role is to facilitate the implementation of the Balancing and Settlement Code (BSC), coordinating the settlement processes in the wholesale energy market [61].

5 Evaluation

This section assesses the privacy and security properties of the proposed protocol and evaluates it in terms of the computational complexity imposed on different entities in the system, as well as the communication overheads incurred between the various agents.

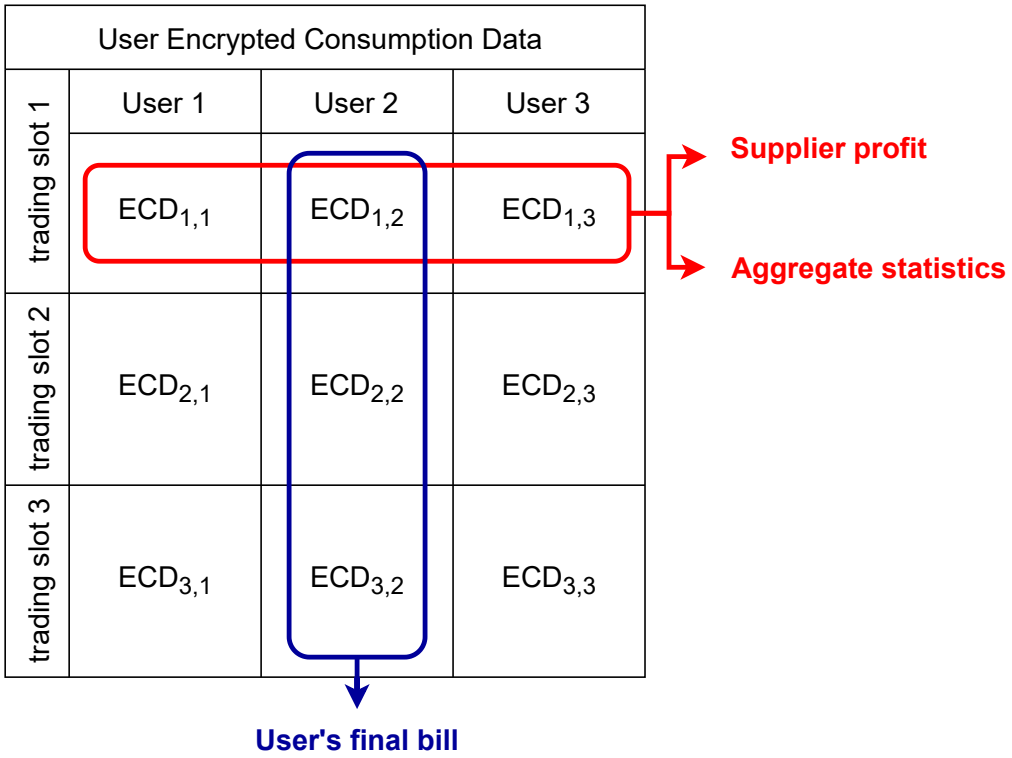


Fig. 16. Privacy-preserving use of encrypted user data through aggregation.

5.1 Privacy and Security Analysis

5.1.1 Metering Data Confidentiality

Each user's consumption data (CD) is encrypted at its source (SM) using Paillier's partially homomorphic cryptosystem, once using the grid operator's public key and once separately using their contracted supplier's public key. This encrypted consumption data (ECD) is then sent to the trading platform where it is temporarily stored and used in bill calculation in its encrypted format, as the platform does not have access to either of the private keys necessary to decrypt the metering data. A part of each user's ECD, the individual deviation, is aggregated with that of all the other households participating in the P2P market, before being sent to the grid operator for decryption. Therefore, the most fine-grained CDs which the trading platform and the grid operator have access to are the aggregate CDs (ACD) of the entire set of users participating in the local energy market, with the size of this set being on the order of thousands. Thus, even authorised entities such as the trading platform,

the grid operator and suppliers do not have access to individual metering data. Figure 16 demonstrates the aggregation of ECDs for calculating market statistics. In order to also mitigate the risk of data breaches from the trading platform's databases, the individual ECDs are removed from storage after the partial bill calculation for each trading period has ended. Due to the assumed public-key encryption and digital signature infrastructure underlying the communication between authorised entities, the ECD and ACD are also resistant to any eavesdropping attacks whilst in transit between SM-to-TrPlat, TrPlat-to-GridOp, and GridOp-to-TrPlat.

5.1.2 Partial Bill Confidentiality

The ECD of each user is used in the calculation of the partial bill by the trading platform. Therefore, there are two separate ciphertexts describing the user's bill for each trading period, one encrypted with the homomorphic public key of the grid operator and one encrypted using the public key of the corresponding supplier, with the trading platform being incapable of decrypting either of them as it does not have access to the respective private keys.

After every trading slot, the trading platform calculates an aggregate encrypted profit for each supplier using a part of the partial bills of their respective users, which is then communicated to the specific supplier. Because PPBSP follows the "principle of least privilege", only allowing an entity access to the data it needs to carry out its duties and nothing more [62], the suppliers are not informed of the individual fine-grained electricity bills of their customers. Instead, an energy supplier only receives the aggregate encrypted profit incurred from trading with its customer base (see Figure 16), which it can decrypt using its own private key. Assuming a large enough number of users contracted to the same supplier, it is impossible for that supplier to extract any detailed information about a specific user's fine-grained individual deviation, let alone their entire CD.

At the end of each billing period, the partial bills of a user (encrypted with the supplier's homomorphic public key) are summed up into a single encrypted value, which is sent to their respective electricity supplier for bill settlement purposes. Figure 16 also illustrates this method of aggregation. Assuming half-hourly trading slots over the period of an entire month, this final energy bill would represent the aggregate of at least 1344 partial bills. Therefore, the supplier is unable to deduce any detailed sensitive data from the final communicated bill. Moreover, since the Paillier cryptosystem is semantically secure against chosen-plaintext attacks, as the decisional composite residuosity assumption (DCRA) is considered intractable [44], and assuming secure and authentic communication channels connecting the system entities, only the corresponding supplier and the grid operator have access to the final monthly bill of any specific user.

5.1.3 Supplier Accountability

The entire partial bill calculation process performed by the trading platform every trading period is carried out once using the data encrypted by the suppliers' homomorphic public keys, and repeated again using the CDs encrypted with the grid operator's public key. Therefore, instead of each individual supplier being the only one capable of decrypting their users' final bills and being trusted to communicate accurate values to the market regulator, the grid operator also has the capacity to verify any of their calculations using the backup encrypted partial bills. Such, the risk of a supplier deviating from their preimposed protocol is minimised, because of the grid operator's implicit ability to audit their transactions, which would lead to pertinent punishments if found to have behaved in a dishonest manner.

5.2 Performance Evaluation

The following analysis will focus only on the computational load and communication cost inflicted by the privacy-preserving billing and settlements protocol, as described in Section 4, which is exclusively concerned with protecting sensitive user data from authorised entities. As a result, the additional overhead of implementing the assumed secure and authentic communication channels (e.g. established using Transport Level Security [63]) is omitted.

Table 1. Computational complexity of PPBSP

Entity	Operations per trading period
SM	$4 \times$ HomoEnc
TrPlat	$(2 \times N_u) \times$ BillCalc
GridOp	$4 \times$ HomoDec
Supplier	$1 \times$ HomoDec
Entity	**Operations per billing period**
SM	-
TrPlat	-
GridOp	- / $(2 \times N_s) \times$ HomoDec *
Supplier	$N_{u,s} \times$ HomoDec

* only on request for inspection.

5.2.1 Computational Complexity

Computationally expensive operations used in PPBSP are (homomorphic) key generation, (homomorphic) asymmetric encryption/decryption, and encrypted bill calculation. They are denoted as KeyGen, HomoEnc, HomoDec, and BillCalc respectively. Table 1 summarises the computational complexity of PPBSP.

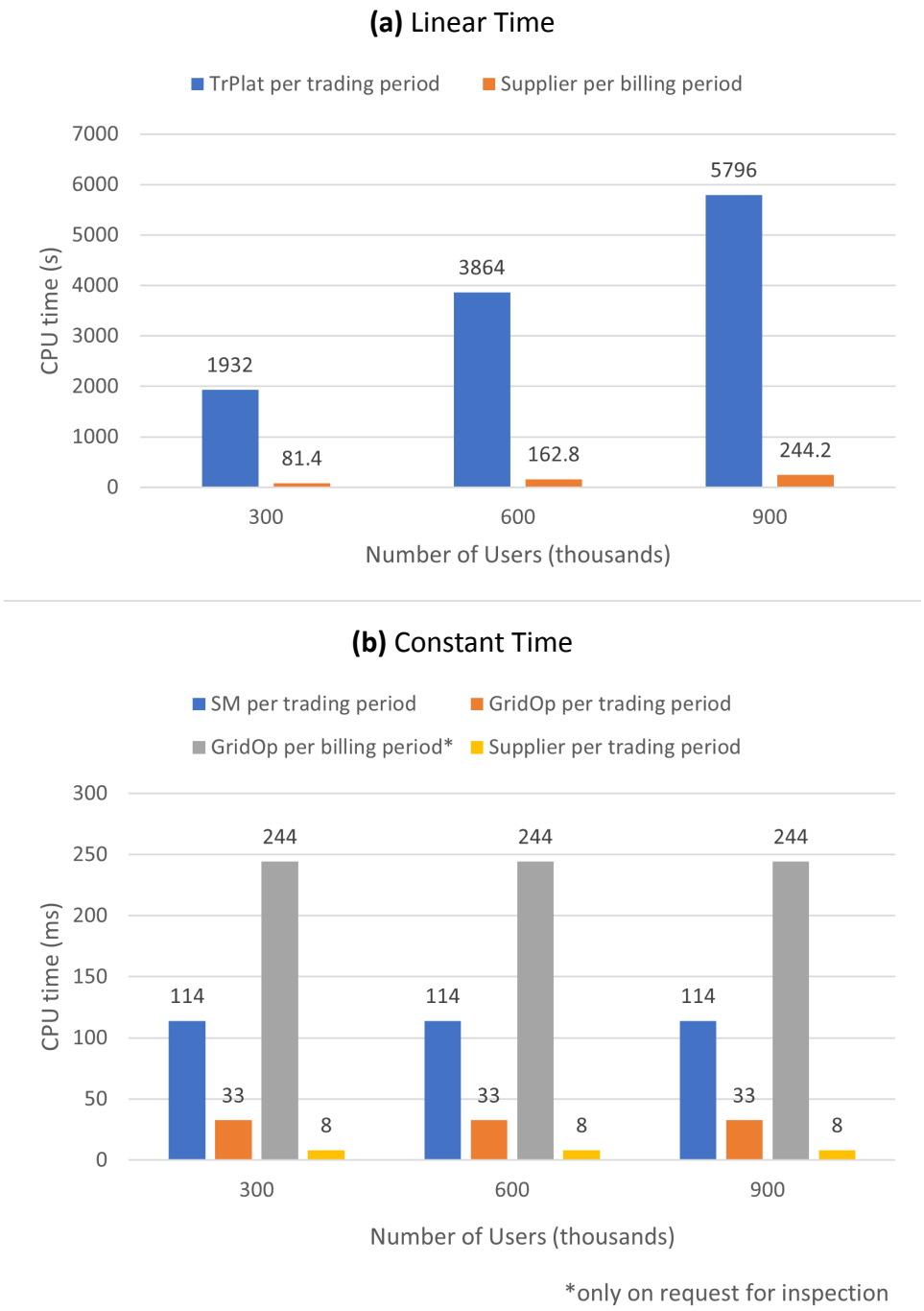


Fig. 17. Computational cost of each PPBSP entity.

As described in Section 4.1, PPBSP can be split into three phases:

1. At system initialisation, the grid operator and each supplier generate a pair of public-private keys: $1 \times$ KeyGen
2. Every trading period (e.g. 30 minutes, one hour, etc.):
    - Each SM performs four HomoEnc, encrypting its committed volume and its individual deviation with the respective supplier's homomorphic public key, and separately with the grid operator's public key: $4 \times$ HomoEnc

- The trading platform computes two separate partial bills for each user. Crucially, this operation can be parallelised as each partial bill is independent of the others: $(2 \times N_u) \times$ BillCalc
- The grid operator carries out four HomoDec, decrypting the aggregate market statistics received from the trading platform: $4 \times$ HomoDec
- Each supplier performs one HomoDec, decrypting their aggregate profit: $1 \times$ HomoDec

3. Every billing period (e.g. one month):
   - The SMs do not perform any computationally expensive operations.
   - The trading platform does not carry out computationally intensive calculations either.
   - The grid operator does not perform any computation unless the suppliers have communicated erroneous results, in which case it aggregates the final customer bills per supplier and then decrypts these aggregates and each of the monthly supplier profits: $(2 \times N_s) \times$ HomoDec
   - Each supplier decrypts their customers' bills: $N_{u,s} \times$ HomoDec

I also ran simulations on an Intel Core i7-8565U CPU (1.80GHz) with 16GB of RAM in order to demonstrate the scalability of PPBSP. For the experiments, homomorphic encryption was implemented using the python-paillier library [64] with 2048-bit keys, which meets the current NIST recommendation [65]. The mean run time (over 1000 simulations) of each operation is the following:

- KeyGen $= 339.53$ ms $= 0.3395$ s
- HomoEnc $= 28.48$ ms $= 0.0284$ s
- HomoDec $= 8.14$ ms $= 0.0081$ s
- BillCalc $= 3.22$ ms $= 0.0032$ s

The computational complexity of PPBSP for a system with 30 suppliers ($N_s = 30$), varying the number of users (N_u) from 300k to 900k is plotted in Figure 17. The results illustrate the practicality and scalability of PPBSP in real-world scenarios, especially if the trading platform is hosted on a more powerful machine such as a server cluster, since partial bills are independently computable and thus the entire operation can be parallelised (e.g. 2 CPUs would cut the computation time in half, 4 CPUs to a quarter of the time, etc.). Most importantly, the computational load on the SM, a device that has limited computational resources, is very low.

Table 2. Communication cost of PPBSP

Protocol segment	Number of bits per trading period
SM-to-TrPlat	$(4 \times N_u) \times (\|ciphertext\| + \|boolean\|)$
TrPlat-to-GridOp	$4 \times \|ciphertext\|$
GridOp-to-TrPlat	$4 \times \|float\|$
TrPlat-to-Sup	$N_s \times \|ciphertext\|$
Protocol segment	**Number of bits per billing period**
SM-to-TrPlat	-
TrPlat-to-GridOp	- / $(2 \times N_s) \times \|ciphertext\|$ *
GridOp-to-TrPlat	-
TrPlat-to-Sup	$N_u \times \|ciphertext\|$

* only on request for inspection.

5.2.2 Communication Overhead

The communication overhead introduced by PPBSP can be separated into four distinct parts: data sent from smart meters to the trading platform (denoted SM-to-TrPlat), from the trading platform to the grid operator (TrPlat-to-GridOp), from the grid operator back to the trading platform (GridOp-to-TrPlat), and from the trading platform to suppliers (TrPlat-to-Sup). Table 2 illustrates the communication cost of PPBSP.

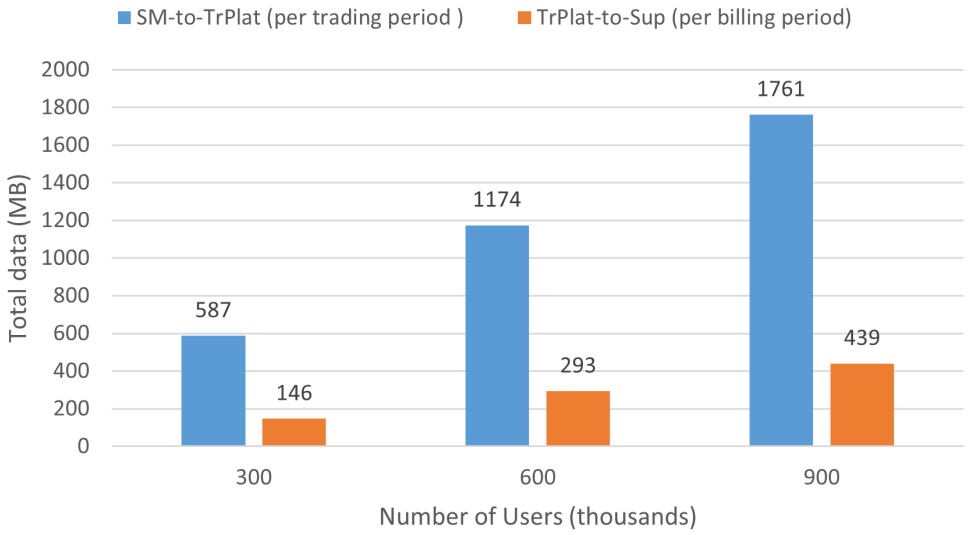
1. Every trading period (e.g. 30 minutes, one hour, etc.):

    - Each SM sends the trading platform four ciphertexts and four Boolean flags, so the communication cost of SM-to-TrPlat is: $(4 \times N_u) \times (|ciphertext| + |boolean|)$
    - The trading platform communicates four ciphertexts to the grid operator, representing the encrypted market aggregates: $4 \times |ciphertext|$
    - The grid operator sends back four floating point numbers, which are the decrypted market aggregates: $4 \times |float|$
    - The trading platform sends each supplier a ciphertext representing their balance change: $N_s \times |ciphertext|$

2. Every billing period (e.g. one month):

    - SMs do not send any information over the network.
    - The trading platform does not send the grid operator data unless the suppliers are misbehaving, in which case it sends it the encrypted aggregate bills per supplier and also each supplier's encrypted final profits: $(2 \times N_s) \times |ciphertext|$
    - The grid operator does not send anything back to the trading platform.

(a) Linear Functions



(b) Constant Functions

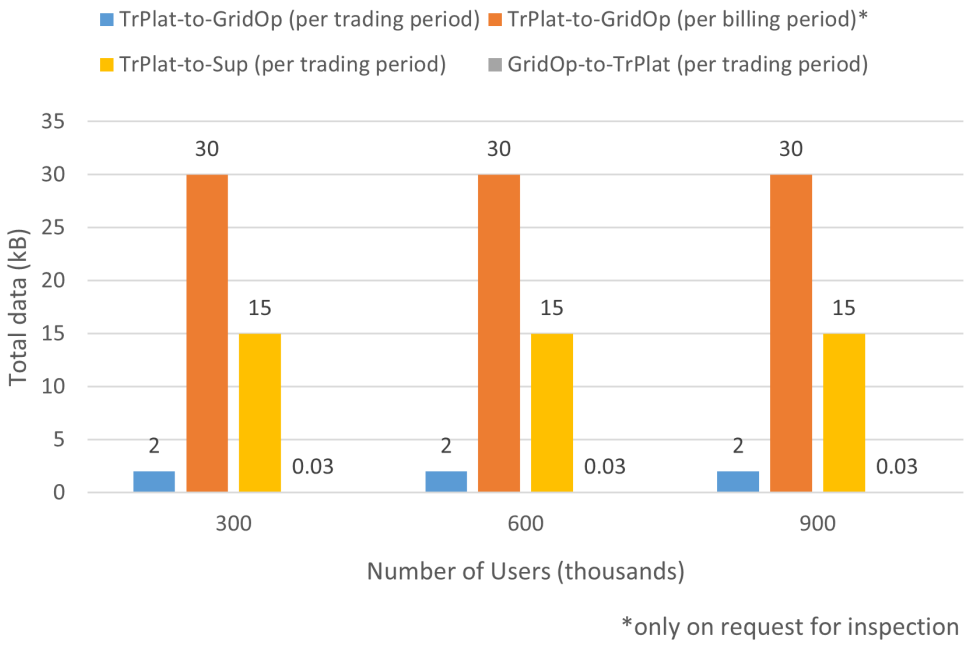


Fig. 18. Communication overhead of PPBSP.

- The suppliers receive from the trading platform their customers' encrypted monthly bills: $N_u \times |ciphertext|$

Moreover, I simulate the communication overhead in Figure 18, using the following parameters: $|ciphertext| = 4096$ bits, $|boolean| = 8$ bits (assuming sparse representation of Boolean flags), $|float| = 64$ bits, the number of suppliers $N_s = 30$, and the user number varying from 300k to 900k.

6 Conclusions and Future Work

6.1 Conclusions

In this report, I have designed a novel privacy-preserving billing and settlements protocol for computing and settling bills for users participating in P2P local energy markets. PPBSP uses partial homomorphic encryption through Paillier's cryptosystem in order to satisfy the LEM's billing requirements in a private manner, while taking into account each user's potential differences between its real meter reading and the electricity volume previously committed at the P2P market auction. The proposed protocol also supports the proportional redistribution of the costs incurred from these deviations among the market's participants, which I have illustrated in the last two proposed billing models. An overview of the entire protocol is presented, before detailing each individual entity's responsibilities and behaviour, as well as explaining the rationale behind these design decisions.

Through an informal analysis, I have demonstrated the privacy-protecting properties of PPBSP, fulfilling all of the imposed requirements. Moreover, I have implemented the billing protocol in Python in order to test its performance on a physical, real-world machine. The simulation results and the theoretical cost analysis indicate PPBSP's computational efficiency and the scalability of its communication overheads to realistic-sized P2P markets, especially when considering the contrast in hardware between the powerful trading platform machines and the households' smart meters, devices with very limited computational resources.

6.2 Future Work

In terms of future work, it consists of providing formal proofs of the privacy properties of PPBSP and running large-scale simulations on a real-world SG system, alongside an appropriate trading algorithm, in order to validate the protocol's feasibility. Furthermore, PPBSP could be integrated into the creation of a novel end-to-end protocol for local energy markets, including bid/offer formulation and submission, electricity trading, bill calculation, and bill settlements.

The protocol's privacy-preserving characteristics could also be further improved by eliminating the need for communicating homomorphically unencrypted metadata about each household's consumption values to the trading platform, which is currently used in the bill calculation process.

References

[1] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE power and energy magazine*, vol. 3, no. 5, pp. 34–41, 2005 (cited on p. 13).

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011 (cited on p. 13).

[3] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in *2013 IEEE Green Technologies Conference (GreenTech)*, IEEE, 2013, pp. 57–64 (cited on p. 13).

[4] M. Kerai, *Smart meter statistics in great britain: Quarterly report to end june 2022*, Aug. 2022. [Online]. Available: `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1099629/Q2_2022_Smart_Meters_Statistics_Report.pdf` (cited on p. 13).

[5] May 2022. [Online]. Available: `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1076878/final_publication_targets_framework_churn_adjustment_government_response.pdf` (cited on p. 13).

[6] S. Cleemput, "Secure and privacy-friendly smart electricity metering," 2018 (cited on pp. 13, 14, 19).

[7] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, pp. 18–28, 2009 (cited on p. 13).

[8] P. Bradley, M. Leach, and J. Torriti, "A review of the costs and benefits of demand response for electricity in the uk," *Energy Policy*, vol. 52, pp. 312–327, 2013 (cited on p. 13).

[9] S. Karnouskos, "Demand side management via prosumer interactions in a smart city energy marketplace," in *2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies*, IEEE, 2011, pp. 1–7 (cited on p. 13).

[10] C. Zhang, J. Wu, M. Cheng, Y. Zhou, and C. Long, "A bidding system for peer-to-peer energy trading in a grid-connected microgrid," *Energy Procedia*, vol. 103, pp. 147–152, 2016 (cited on p. 13).

[11] F. Teotia and R. Bhakar, "Local energy markets: Concept, design and operation," in *2016 National Power Systems Conference (NPSC)*, IEEE, 2016, pp. 1–6 (cited on p. 14).

[12] J. M. Schwidtal, P. Piccini, M. Troncia, *et al.*, "Emerging business models in local energy markets: A systematic review of peer-to-peer, community self-consumption, and transactive energy models," *Community Self-Consumption, and Transactive Energy models (January 06, 2022)*, 2022 (cited on p. 14).

[13] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, "Peer-to-peer energy trading in a microgrid," *Applied Energy*, vol. 220, pp. 1–12, 2018 (cited on p. 14).

[14] M. Hamlich, N. eddine Belbounaguia, *et al.*, "Short-term load forecasting using machine learning and periodicity decomposition," *AIMS Energy*, vol. 7, no. 3, pp. 382–394, 2019 (cited on p. 14).

[15] Y. Fu, Z. Li, H. Zhang, and P. Xu, "Using support vector machine to predict next day electricity load of public buildings with sub-metering devices," *Procedia Engineering*, vol. 121, pp. 1016–1022, 2015 (cited on p. 14).

[16] V. Dudjak, D. Neves, T. Alskaif, *et al.*, "Impact of local energy markets integration in power systems layer: A comprehensive review," *Applied Energy*, vol. 301, p. 117 434, 2021 (cited on p. 14).

[17] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992. DOI: 10.1109/5.192069 (cited on pp. 15, 20).

[18] M. A. Mustafa, S. Cleemput, and A. Abidin, "A local electricity trading market: Security analysis," in *2016 IEEE PES innovative smart grid technologies conference Europe (ISGT-Europe)*, IEEE, 2016, pp. 1–6 (cited on pp. 15, 18, 23).

[19] F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, "Smart grid privacy: Issues and solutions," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, IEEE, 2012, pp. 1–5 (cited on p. 15).

[20] J. Martinez, A. Ruiz, J. Puelles, I. Arechalde, and Y. Miadzvetskaya, "Smart grid challenges through the lens of the european general data protection regulation," in *Advances in Information Systems Development: Information Systems Beyond 2020 28*, Springer, 2020, pp. 113–130 (cited on p. 15).

[21] L. Stankovic, V. Stankovic, J. Liao, and C. Wilson, "Measuring the energy intensity of domestic activities from smart meter data," *Applied Energy*, vol. 183, pp. 1565–1580, 2016 (cited on p. 15).

[22] M. Fell, H. Kennard, G. Huebner, M. Nicolson, S. Elam, and D. Shipworth, "Energising health: A review of the health and care applications of smart meter data," *London, UK: SMART Energy GB*, 2017 (cited on p. 15).

[23] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, The Steering Committee of The World Congress in Computer Science, Computer …, 2012, p. 1 (cited on p. 15).

[24] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, no. 2, pp. 12–16, 1989 (cited on p. 15).

[25] A. Gupta, V. Garud, U. Rodney, and S. Bapat, *Systems and methods for improving the accuracy of appliance level disaggregation in non-intrusive appliance load monitoring techniques*, US Patent 9,612,286, Apr. 2017 (cited on p. 15).

[26] S. B. Leeb and J. L. Kirtley Jr, *Transient event detector for use in nonintrusive load monitoring systems*, US Patent 5,483,153, Jan. 1996 (cited on p. 15).

[27] A. Haghighat-kashani, J. T.-n. Cheam, and J. M. Hallam, *System and method of compiling and organizing power consumption data and converting such data into one or more user actionable formats*, US Patent App. 14/372,056, Jan. 2015 (cited on p. 15).

[28] E. L. Quinn, "Privacy and the new energy infrastructure," *Available at SSRN 1370731*, 2009 (cited on p. 15).

[29] A. Alabdulatif, I. Khalil, H. Kumarage, and M. Atiquzzaman, "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure," *IET Wireless Sensor Systems*, vol. 7, Jul. 2017. DOI: 10.1049/iet-wss.2017.0061 (cited on pp. 16, 24).

[30] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An mpc-based privacy-preserving protocol for a local electricity trading market," in *Cryptology and Network Security: 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings 15*, Springer, 2016, pp. 615–625 (cited on pp. 16, 24, 31).

[31] ——, "Secure and privacy-friendly local electricity trading and billing in smart grid," *arXiv preprint arXiv:1801.08354*, 2018 (cited on pp. 16, 24).

[32] R. Thandi and M. A. Mustafa, "Privacy-enhancing settlements protocol in peer-to-peer energy trading markets," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2022, pp. 1–5 (cited on pp. 16, 17, 24, 29).

[33] A. Madhusudan, F. Zobiri, and M. A. Mustafa, "Billing models for peer-to-peer electricity trading markets with imperfect bid-offer fulfillment," in *2022 IEEE International Smart Cities Conference (ISC2)*, IEEE, 2022, pp. 1–7 (cited on pp. 16, 17, 20, 24, 35).

[34] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010. DOI: 10.1109/MPE.2009.934876 (cited on p. 18).

[35] T. Capper, A. Gorbatcheva, M. A. Mustafa, *et al.*, "Peer-to-peer, community self-consumption, and transactive energy: A systematic literature review of local energy market models," *Renewable and Sustainable Energy Reviews*, vol. 162, p. 112 403, 2022, ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2022.112403. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032122003112 (cited on p. 19).

[36] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy electrical appliances based on load signaturesof," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 2, pp. 653–660, 2007. DOI: 10.1109/TCE.2007.381742 (cited on p. 20).

[37] M. Lisovich and S. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," *IEEE PROCEEDINGS ON POWER SYSTEMS*, vol. 1, Jan. 2008 (cited on p. 20).

[38] G. Bauer, K. Stockinger, and P. Lukowicz, "Recognizing the use-mode of kitchen appliances from their current consumption," in *Proceedings of the 4th European Conference on Smart Sensing and Context*, ser. EuroSSC'09, Guildford, UK: Springer-Verlag, 2009, pp. 163–176, ISBN: 3642044700 (cited on p. 20).

[39] M. Newborough and P. Augood, "Demand-side management opportunities for the uk domestic sector," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 146, no. 3, pp. 283–293, 1999 (cited on p. 21).

[40] O. Goldreich, *Foundations of Cryptography, Volume 2*. Cambridge university press Cambridge, 2004 (cited on p. 21).

[41] W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th. Prentice Hall, 2005 (cited on p. 21).

[42] M. A. Mustafa, *Smart Grid Security: Protecting Users' Privacy in Smart Grid Applications*. The University of Manchester (United Kingdom), 2015 (cited on p. 22).

[43] R. L. Rivest, L. Adleman, M. L. Dertouzos, *et al.*, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978 (cited on p. 22).

[44] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*, Springer, 1999, pp. 223–238 (cited on pp. 22, 52).

[45] S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Computers & Security*, vol. 84, pp. 148–165, 2019 (cited on p. 23).

[46] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE security & privacy*, vol. 7, no. 3, pp. 75–77, 2009 (cited on p. 23).

[47] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 641–654, 2013 (cited on p. 23).

[48] S. Uludag, M. F. Balli, A. A. Selcuk, and B. Tavli, "Privacy-guaranteeing bidding in smart grid demand response programs," in *2015 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2015, pp. 1–6 (cited on p. 24).

[49] M. F. Balli, S. Uludag, A. A. Selcuk, and B. Tavli, "Distributed multi-unit privacy assured bidding (pab) for smart grid demand response programs," *IEEE Transactions on Smart grid*, vol. 9, no. 5, pp. 4119–4127, 2017 (cited on p. 24).

[50] R. Deng, F. Luo, J. Yang, D.-W. Huang, G. Ranzi, and Z. Y. Dong, "Privacy preserving renewable energy trading system for residential communities," *International Journal of Electrical Power Energy Systems*, vol. 142, p. 108 367, 2022, ISSN: 0142-0615. DOI: https://doi.org/10.1016/j.ijepes.2022.108367. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061522003829 (cited on p. 24).

[51] A. C. Yao, "Protocols for secure computations," in *23rd annual symposium on foundations of computer science (sfcs 1982)*, IEEE, 1982, pp. 160–164 (cited on p. 24).

[52] A. Aly and M. Van Vyve, "Practically efficient secure single-commodity multi-market auctions," in *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20*, Springer, 2017, pp. 110–129 (cited on p. 24).

[53] V. Pillitteri and T. Brewer, *Guidelines for smart grid cybersecurity*, en, 2014-09-25 2014. DOI: https://doi.org/10.6028/NIST.IR.7628r1 (cited on p. 24).

[54] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart grids using homomorphic encryption,” in *2010 first IEEE international conference on smart grid communications*, IEEE, 2010, pp. 327–332 (cited on p. 24).

[55] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, “Musp: Multi-service, user self-controllable and privacy-preserving system for smart metering,” in *2015 IEEE International Conference on Communications (ICC)*, IEEE, 2015, pp. 788–794 (cited on p. 24).

[56] ——, “Dep2sa: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure,” *IEEE Access*, vol. 3, pp. 2828–2846, 2015 (cited on p. 24).

[57] Y. Wang, W. Saad, Z. Han, H. V. Poor, and T. Başar, “A game-theoretic approach to energy trading in the smart grid,” *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1439–1450, 2014 (cited on p. 24).

[58] T. Capper, J. Kuriakose, and M. Sharmina, “Impact of energy imbalance on financial rewards in peer-to-peer electricity markets,” *IEEE Access*, vol. 10, pp. 55 235–55 254, 2022 (cited on p. 24).

[59] A. Paverd, A. Martin, and I. Brown, “Modelling and automatically analysing privacy properties for honest-but-curious adversaries,” *Tech. Rep*, 2014 (cited on p. 27).

[60] Elexon, *What we do - Elexon*, Feb. 2022. [Online]. Available: `https://www.elexon.com/what-we-do/` (cited on p. 50).

[61] ——, *What is the BSC?* Sep. 2020. [Online]. Available: `https://www.elexon.co.uk/knowledgebase/about-the-bsc/` (cited on p. 50).

[62] J. H. Saltzer and M. D. Schroeder, “The protection of information in computer systems,” *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975 (cited on p. 52).

[63] T. Dierks and E. Rescorla, “The transport layer security (tls) protocol version 1.2,” Tech. Rep., 2008 (cited on p. 53).

[64] C. Data61, *Python paillier library*, `https://github.com/data61/python-paillier`, 2013 (cited on p. 55).

[65] E. Barker and Q. Dang, “Nist special publication 800-57 part 1, revision 4,” *NIST, Tech. Rep*, vol. 16, 2016 (cited on p. 55).