Towards Privacy Preserving Local Energy Markets

Kamil Erdayandi[1], Lucas C. Cordeiro[1], and Mustafa A. Mustafa[1,2]

[1] *Department of Computer Science, The University of Manchester, UK*
[2] *imec-COSIC, KU Leuven, Belgium*
Email: {kamil.erdayandi, lucas.cordeiro, mustafa.mustafa}@manchester.ac.uk

Keywords: Privacy, Game Theory, Local Energy Trading, Decentralised Architectures

Abstract

In this paper, we provide a technical discussion and analysis of emerging privacy-preserving local energy trading markets based on a game theoretical approach where buyers and sellers can trade electricity in a (semi-)decentralised manner. Firstly, we present a general overview of energy trading mechanisms and privacy-enhancing techniques. Secondly, we compare privacy-preserving market models and provide a further discussion on potential local trading market architectures based on a game theoretical approach. Lastly, we provide technical analysis for the discussed game-theoretical market architectures. This paper draws a roadmap for future designs of privacy-preserving local energy trading markets, which are based on a game theoretical approach.

1 Introduction

Electricity generation has been largely dependent on non-renewable and non-green energy sources such as coal, gas and fuel oil [1]. Thanks to the global commitment to reduce carbon emission, the utilisation of renewable energy sources (RES), including wind, solar and hydro energy sources, is increasing. However, several challenges need to be tackled when a substantial amount of electricity comes from RES. Green energy sources, such as solar and wind, are intermittent energy sources. Their output fluctuates based on weather conditions [2]. In addition, load demands are usually uncertain throughout the day. Regardless of power sources, a user demands continuous energy supply and also desires to minimise his/her electricity bill.

Furthermore, in a dynamic pricing environment, the price of electricity varies throughout the day. In this situation, major electricity producers and retailers have the leverage to offer better prices with non-intermittent energy supplies. Due to this, as an example, in the UK, excess electricity generated from residential RES automatically is injected back into the grid for a fixed price, Feed-in-Tariff (FiT), which is much lower than a retail price [3]. Thus, under these circumstances, traditional non-renewable sources like coal and gas are still used as primary energy sources for electricity generation in most parts of the world [4].

In order to encourage the usage of RES, local electricity producers should be able to sell their excess electricity for a price higher than the FiT price. At the same time, consumers should be able to buy their needed electricity from local RES owners for a price lower than the retail price. Furthermore, smart grids support bi-directional electricity and communication flows [5]. With this infrastructure, users owning RES can sell their excess electricity to other users and major electricity producers/retailers. Thus, RES owners can collaboratively or individually maximize their profits and reduce their bills by utilising trading mechanisms in smart grids [6]. Thanks to the multi-agent optimisation techniques in energy trading [7–23], they can sell their excess electricity to other users for a price lower than the retail but still higher than the FiT price.

However, these trading mechanisms may also allow malicious entities to misbehave to maximise their profits. Potential threats are impersonation, data manipulation, eavesdropping, and privacy breaches [24]. For example, some entities may use users' information to infer who sells or buys how much electricity and when. Such data is closely correlated to users' consumption patterns. These situations may create privacy risks in which private information of the users may be leaked [13, 25].

In literature, energy trading algorithms have been extensively studied but mostly without taking into account any security or privacy issues [7–23]. There are only a few privacy preserving solutions for energy trading [26–35]. However, these solutions either do not use multi-agent trading mechanisms [26, 27], are prone to single point of failure [28, 29], are not scalable [30, 31], is not fully optimised [32] or do not provide performance evaluation [33]. Among the privacy-preserving game theoretical energy trading solutions, the solutions [34] and [35] are not competitive and cooperative, respectively.

As a result, the above limitations indicate that there is room for improvement on previous studies to explore and propose novel techniques for privacy-preserving game theoretical energy trading. Hence, this paper focuses on roadmapping emerging privacy-preserving game theoretical local energy trading mechanisms. Specifically, the contributions of this paper are three-fold:

- First, it presents a general overview of local electricity markets, trading mechanisms and privacy-enhancing mechanisms.
- By utilising the background information provided, it provides a comparison between privacy-preserving market models. After this, further discussion on potential local trading market architectures based on game theoretical approaches is provided.
- Lastly, it provides functionality, security, privacy, scalability and key management analyses for the provided game-theoretical market architectures. It also assesses the applicability of Privacy Enhancing Technologies (PETs) for the discussed architectures.

The remainder of the paper is organised as follows. Background information on local electricity markets, trading and privacy-preserving mechanisms are presented in Section 2. Critical analysis of privacy-preserving energy trading systems is provided in Section 3. In Section 4, the discussed energy trading markets are analysed in terms of functionality, security, privacy, key management and applicability of privacy-enhancing technologies. Finally, the paper is concluded in Section 5.

2 Background

This section provides background information on local energy markets, trading and privacy-preserving mechanisms.

2.1 Local Electricity Markets

Electricity trading has been widely discussed with the development of smart grid [7–23, 26–38]. Unlike other market models, demand and supply should be matched in each trading period in electricity markets. Keeping balance is not easy concerning the fluctuating outputs of renewable energy resources, so there is a need for local markets with more active local sellers and buyers. Below, we list some of the key players in any local electricity market [39].

- *Users* are electricity consumers who buy and pay for the amount of electricity consumed. If they have facilities to produce electricity, such as RES, they can also sell electricity. In this case, this type of user is named *prosumer*. Users are usually equipped with home energy management systems (i.e., smart agents) that represent the users on the local market to maximise users' welfare – reduce cost or increase profit.
- *Market operator a.k.a trading platform* is responsible for clearing the market by following the clearing and pricing rules of the market. In fully decentralised markets, there is no market operator as no single centralised market player performs the market clearance. Instead, this is done in a decentralised way by the users themselves via their smart agents.
- *Suppliers* are responsible for supplying electricity from major electricity generators to consumers who could not meet their electricity demand from the local energy market.
- *Distribution System Operator (DSO)* is responsible for the maintenance and management of the distribution network. It charges distribution network fees.
- *Transmission System Operator (TSO)* is responsible for maintaining the transmission network and balancing the grid. It charges transmission network fees.

There are already a few ongoing projects, e.g., LO3 Energy [40], which focus on commercial electricity trading to encourage residential units to trade with their neighborhoods. SNIPPET [24] is another project that investigates the design and evaluation of secure and privacy-friendly peer-to-peer electricity trading in smart grids.

2.2 Trading Mechanisms

In the literature, major contributions to energy trading can be divided into two categories: *Game Theory* and *Auction Theory*. A brief description, specific methods used and research articles for each category are given in Table 1.

Game theoretical methods can be specified as *"Stackelberg game"* or *"Nash game"*. For each, the rule of playing is different. For the former, selected leaders propose their strategies first and others (followers) response with their optimised strategies accordingly. For the latter, both players act and propose their strategies at the same time. Furthermore, game theoretical methods can be divided into two basic sub-categories: cooperative games and non-cooperative games. A cooperative game is a game where groups of players enforce cooperative behaviour, and hence the game is played between coalitions of players, rather than between individual players. A non-cooperative game is a game in which players make decisions independently [12].

In Auction Theory, the quantity and types of participants in an auction might vary. Double auction has multiple sellers and multiple buyers, there is a single buyer and several sellers in a reverse auction, whereas a forward auction has multiple bidders and a single seller. Participants bid openly against one another in Open-Bid Auction, whereas bidders submit sealed bids at the same time, so no-one knows what the other bidders are offering in Sealed-Bid Auction.

Table 1: Comparison of Trading Algorithms.

Approach	Brief Description	Specific Methods	Literature
Game Theory	Mathematical models of strategic interactions among rational decision-makers [41]. In game theory, decision of action taken by one player depends on and affects the actions of other players [42].	Stackelberg game Nash Game Cooperative Game Non-cooperative Game	[7–9, 34, 35] [10–12] [8, 13–15] [7, 10–12, 16]
Auction Theory	The process of buying and selling products or services by offering them up for bids, taking bids, and then selling the item to the highest bidder or buying the item from the lowest bidder [43].	Double Auction Reverse Auction Open-Bid Auction Sealed-Bid Auction	[8, 10, 17, 18, 28–33] [36] [37] [38]

2.3 Privacy Preserving Mechanisms

Utilisation of trusted third parties (TTPs) can provide some security guarantees and partial privacy protection when designing local energy markets. The limitation of solutions relying on TTPs is that these TTPs usually have access to users' confidential data. In critical applications, it may not always be preferable for any entity (including TTPs) to access any private data. To avoid reliance on TTPs, privacy preserving mechanisms exist. These include Anonymisation (Anon), Differential Privacy (DP), Homomorphic Encryption (HE) and Secure (multi-party) computation (MPC).

Anonymisation [44] is the process of removal of personally identifiable information from datasets. In this mechanism, identifiable information is usually replaced with non-identifiable information, and the relations between the two types of information are stored in a separate table. In most cases, computation cost of Anonymisation is low. However, there are techniques [45] which can de-anonymise the data.

Differential Privacy [46] is the modification or perturbation of a data to obfuscate individual data while the ability to manipulate data within a specific scope is still retained. Computation cost of this mechanism is relatively low, however accuracy of the data is lost to some degree.

Homomorphic Encryption is a technique that preserves the ability to perform mathematical operations on encrypted data as if it was non-encrypted (plain text) such that the result decrypted after HE operations is identical to the output for which HE is not utilised [47, 48]. HE can be divided into two subcategories: full and partial HE. In full HE, all arithmetic operations are supported, while in partial HE, only a limited number of operations are supported. Computational costs is relatively high. However, full accuracy of data can be preserved by using partial HE or full HE with the consideration of an error budget.

Secure (multi-party) computation is a technique that enable two or more parties to split up data among them to perform joint computations [49]. This mechanism prevents any single party from gaining knowledge of the data but in which the computational results are preserved. Accuracy of data is preserved in this mechanism, however communication cost is relatively high so it may not be applicable for applications where communication overhead is a concern.

3 Critical Analysis of Privacy Preserving Energy Trading Systems

In this section, we provide a comparison of existing privacy preserving market models and present markets based on game theoretical approaches.

3.1 Comparison of Existing Privacy Preserving Energy Market Models

Existing privacy preserving energy trading solutions [26–35] are summarised in Table 2. A technique is proposed in [26] to aggregate smart metering data which is used in utility provider billing. Consumption data exchanged is anonymously authenticated. A semi-trusted third party is used in which trust is distributed among multiple entities. Although reliance on a single point of trust is avoided, TTPs may still have access to private data of users. A trading framework is proposed in [27] where energy traders and electrical vehicle (EV) owners work together to meet the energy demands of EVs collectively. Energy traders directly send offers to EV owners, who, in return, reserve their desired charging station. All transactions are stored on a blockchain and payment to EVs are anonymous. Nevertheless, these solutions [26, 27] are not based on multi-agent energy trading. In addition, anonymisation techniques used in these works may be reversed by using techniques from [45].

A privacy preserving double auction mechanism is proposed in [28] for cases when power requested and power consumed are not matched and spare energy is traded between households. Tokens are bought by the households from the energy providers to be used for trading. Data is split into random pieces and each piece is encrypted with different key pairs so that data owners can not be identified when tokens are re-used. A control center manages the market, adapting to the changing needs of users. As it is a centralised structure, there is a risk of single point of failure.

Security protocols are provided in [29] for safely deploying various double auction mechanisms in smart grids. A pseudo-identity is assigned to each participant to provide anonymity, and the bids are encrypted using the Paillier cryptosystem to preserve the users' privacy. Pedersen com-

Table 2: Privacy Preserving Trading Mechanisms with Their Privacy Enhancing Techniques.

Paper	Approach	Trading Method	PET
Dimitriou et al. *2013* [26]	Not Multi-agent trading	-	Anon
Radi et al. *2019* [27]	Not Multi-agent trading	-	Anon
Li et al. *2018* [28]	Auction Theory	Double Auction	Anon
Sarenche et al. *2020* [29]	Auction Theory	Double Auction	Anon & HE
Abidin et al. *2016* [30]	Auction Theory	Double Auction	MPC
Zobiri at al. *2022* [31]	Auction Theory	Double Auction	MPC
Zobiri at al. *2022* [32]	Auction Theory	Double Auction	MPC
Liu et al. *2020* [33]	Auction Theory	Double Auction	HE
Xie et al. *2020* [34]	Game Theory	Stackelberg Game	HE
Erdayandi et al. *2022* [35]	Game Theory	Stackelberg Game	HE

mitment scheme is used to verify that users correctly and honestly followed the auction protocol. However, the proposed framework is not applicable for decentralised applications since a central party performs the majority of operations. Thus, it is vulnerable to single point of failure.

In [30], a bidding mechanism based on secure MPC is given in which mutually distrustful parties make computation without disclosing sensitive data. The trading platform performs a double auction to determine the trade price, the volume of electricity sold, and the auction winners. However, this work is not scalable for short trading periods. Similarly, the work in [31] proposes a privacy-friendly and incentive-based demand response market in which users trade their flexibility. Aggregation of users' offers is performed over encrypted data using MPC to provide privacy of the users. Double-auctions determine the distribution of flexibility as well as the consumer consumption schedule. However, the computational cost has not been thoroughly evaluated. Performance of the offline phase has not been included while, the online phase computations need to be optimised for trading periods shorter than 30 minutes. In the same way, the authors in [32] propose a privacy preserving energy trading market in which excess electricity of users and their flexibility are traded. Users submit their offers/bids in encrypted form and computations are performed with MPC mechanism. Allocation of resources are determined considering the device constrains. However, the communication cost is not evaluated.

In [33], a novel privacy-aware double auction trading system is proposed by applying HE for aggregation functions. However, despite the employment of HE, a computationally intensive technique, a performance evaluation is not performed. In [34], a privacy preserving distributed energy trading framework is proposed with game theoretical approach. Buyers privately compute a fixed optimal price for their trading, and sellers allocate pairwise energy trading amounts without disclosing sensitive data with HE. The trading problem is modelled as a non-cooperative Stackelberg game for all the agents as buyers are selected as leaders to determine the optimal price, and then sellers as followers, to derive the trading amounts. TTP is not needed in this work. However, the market designed is not competitive. A fixed market price is determined by the buyers and trading is performed over this price. To address this limitation, a privacy-friendly energy trading platform (PFET) based on game theoretical approach – more specifically Stackelberg competition – has been proposed in [35]. PFET provides a competitive market in which prices and demands are determined based on competition, and computations are performed in a decentralized manner which does not rely on TTPs. The main imitation of this work is the scalability.

3.2 Potential Privacy Preserving Local Energy Markets Based on Game Theoretical Approaches

In this section, we first list some of the main requirements for designing a privacy-preserving local energy markets (LEM) before providing potential architectures of such markets based on game theoretical approaches.

3.2.1 Functional and Privacy Requirements

The main requirements of any LEM should include *social welfare provision*, *individual rationality*, and *equilibrium* as functional requirements, and *user data confidentiality*, *transaction anonymity* and *authorisation* as privacy requirements. These are summarised as below;

- **Social welfare provision:** LEM should provide social welfare in which utilities of users are maximised.
- **Individual rationality:** LEM should ensure individual rationality – agents receive higher payoffs for participating.
- **Equilibrium:** LEM should ensure stability – market reaches to equilibrium where no agent can improve its payoff by changing its strategies any more.
- **User data confidentiality:** LEM should not reveal any private information of users.
- **Transaction anonymity:** LEM should not reveal the identities of users who trade between each other.
- **Authorisation:** LEM should reveal aggregated volumes traded only to authorised market players.

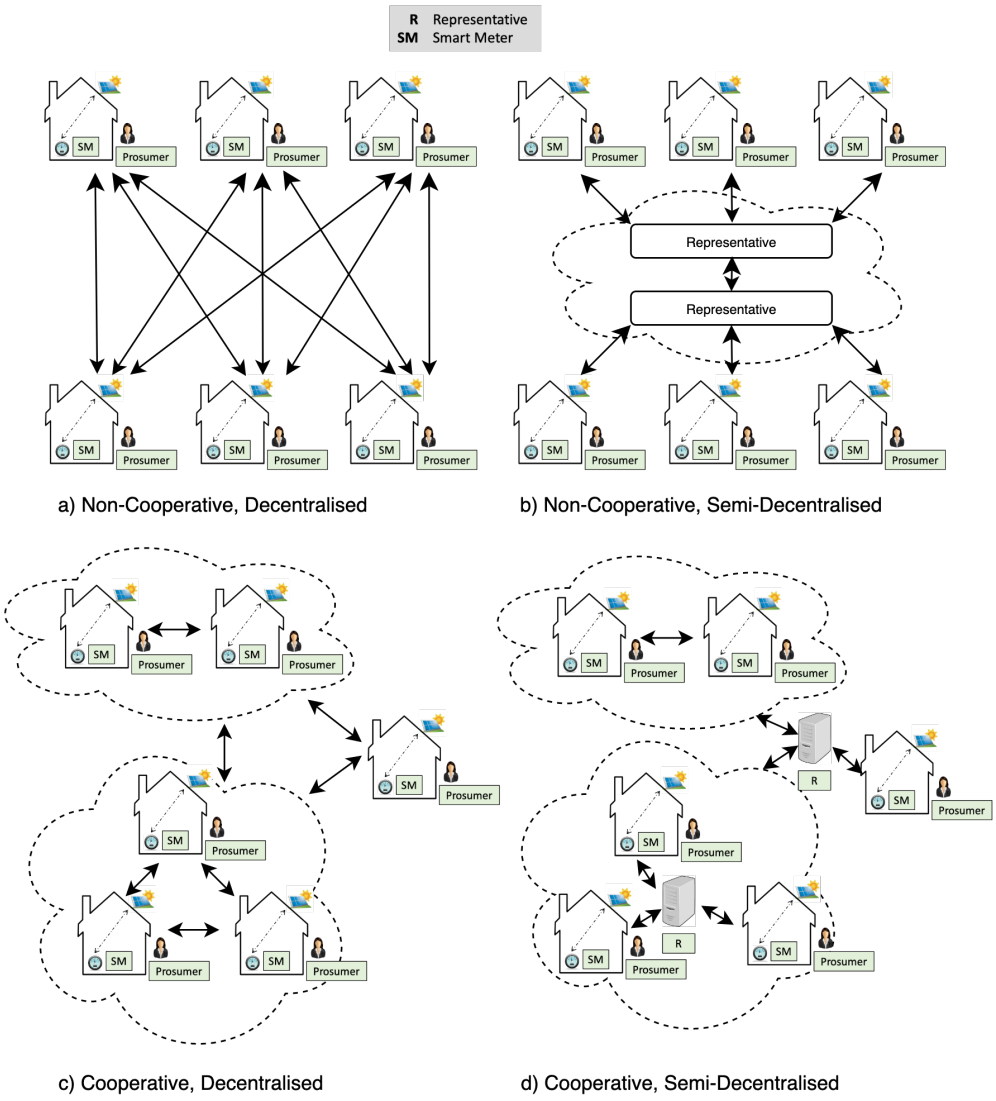

Figure 1: Prospective System Architectures of Local Energy Markets that use Game Theoretical Approaches.

3.2.2 Potential Energy Trading Architectures Based on Game Theoretical Approach

Next, different energy trading architectures are provided to which game theoretical approaches can be applied. Each provided architecture is displayed in Fig. 1.

Non-Cooperative, Decentralised: As depicted in Fig. 1-a), each user communicate directly with any other users and is actively involved in trading. Computations are performed by the users in a decentralised manner.

Non-Cooperative, Semi-Decentralised: As shown in Fig. 1-b), users do not have direct contacts with other users and are not involved in trading directly. Instead, representatives trade on their behalf. Bids are offered by the users; computations are performed by the representatives.

Cooperative, Decentralised: As depicted in Fig. 1-c), users are able to form coalitions/communities for their benefits to leverage better payoffs and utility. Users in a community directly communicate with each other to make decisions. Communities can trade with other communities.

Cooperative, Semi-Decentralised: As depicted in Fig. 1-d), users are able to form coalitions and communities for their benefits similar to the system in Fig. 1-c). However, users inside a community do not necessarily communicate directly with each other. Representatives are actively involved for decision making inside communities and perform the trading between communities on behalf of users.

4 Analysis of Market Architectures

In this section, the presented trading architectures are analysed in terms of functionality, security, privacy, scalability, key management, and applicability of privacy enhancing technologies.

4.1 Functional Analysis

In non-cooperative architectures, users compete with each other to maximise their own utilities whereas in cooperative arhitectures, they aim to maximise the utilities of coalitions they belong to. Nevertheless, utility functions need to have local maxima points for the LEM to reach to an equilibrium. In game theoretical approaches, e.g., Stackelberg games, utility functions usually depend on the strategies or reactions of opponents.

In our previous work [35], we have designed and implemented a non-cooperative local electricity trading platform based on game theoretical approach using Stackelberg game. Sellers propose their strategies with electricity selling prices as leaders, and buyers, as followers, react to leaders with electricity demands. Leaders and followers iteratively propose their strategies until the market reaches to an equilibrium. We have proved that the market has reached an equilibrium, both with formal theoretical proofs and simulations. Simulation results show that individual rationality is provided such that each agents gets a higher payoff for participating vs not participating.

4.2 Security and Privacy Analysis

For all four trading architectures, secure authentication must be provided to mitigate impersonation attacks as well as message authentication codes or signatures are needed to prevent data manipulation and to provide data integrity. The semi-decentralised architectures, where representatives are implicated for trading and communication, are more prone to single point of failure attacks. Similarly, cooperative architectures are more prone to such attacks compared to non-cooperative architectures. Data can be stored securely in a distributed manner and the number of representatives can be increased to prevent such attacks [25].

In decentralised architectures, each user has information about other users with whom s/he has previously traded, so each user's information must be hidden from each other with the help of secure computation techniques. In semi-decentralised architecture, users share their information with representatives for them to be able to trade on their behalf. Representatives may have access to sensitive data of users and external attackers may target them since representatives have more information than a single user, so computations by the representatives must be performed on encrypted data. Representatives in semi-decentralised architectures and formation of communities in cooperative architectures would increase the anonymity set and provide better privacy. Such communities may require group signature schemes to provide non-reputation of their messages in their communities [25].

4.3 Scalability and Key Management

In terms of communication (i.e., number of communication links), semi-decentralised architectures are more scalable compared to decentralised architectures, while cooperative architectures are more scalable compared to non-cooperative architectures. Due to iterative nature of game theoretical approaches, the amount of data to be transmitted between entities is expected to be high, so it is advantageous to select LEM architectures that require less communication cost.

Higher number of unique cryptographic keys are needed for decentralised architectures to provide security/privacy guarantees, whereas a lower number of such keys are needed for semi-decentralised and cooperative LEM architectures.

4.4 Applicability of Privacy Enhancing Technologies

Anonymisation techniques may not always provide full privacy as anonymised IDs can be reversed by using techniques described in [45]. TTPs may have access to sensitive data of users and they may not always fit the concrete use-case. Accuracy of data is partially lost with differential privacy techniques. As the price information should be accurately calculated when trading, differential privacy may not be always applicable in energy trading scenarios.

Secure MPC method has high communication intensity, and due to this, it might be less applicable for decentralised architectures where communication density is already high. Considering these circumstances, HE might be the most applicable PET for energy trading among these methods as the accuracy is not lost if the system is delicately designed with the consideration of an error budget.

Although the computational cost of HE is relatively high, it is still possible to achieve feasible performance results. As an example, in our previous work [35], we have demonstrated the practicality of privacy preserving energy trading platform for up to 100 users, implemented with HE and based on a game theoretical approach.

5 Conclusion

In this paper, we have presented a general overview of trading and privacy preserving mechanisms, provided a comparison between existing privacy preserving local energy market models and further discussed potential architectures of such local energy markets based on game theoretical approaches. In addition, we have performed functionality, security, privacy, scalability and key management analysis, and discussed the applicability of well-known privacy enhancing techniques for the proposed market architectures. By doing so, this work establishes a road map for future designs of privacy-preserving local energy trading marketplaces using a game theoretic approach. It can

be used as a reference to make decisions/evaluations on different market architectures and mechanisms before the design/implementation stage of privacy preserving game theoretical local energy markets.

As a future work, we plan to extend our previous non-cooperative energy trading platform solution [35] by designing and implementing *"cooperation"* mechanism by considering the aspects presented in this article.

Acknowledgement

This work was supported in part by the EPSRC through the project EnnCore EP/T026995/1 and by the Flemish Government through the FWO SBO project SNIPPET S007619. K.E is funded by The Ministry of National Education, Republic of Turkey. M.A.M. is funded by the DKO Fellowship awarded by The University of Manchester.

References

[1] *BP Statistical Review of World Energy*. `https://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html`.

[2] Xiaodong Liang. "Emerging power quality challenges due to integration of renewable energy sources". In: *IEEE Transactions on Industry Applications* 53.2 (2016), pp. 855–866.

[3] *Feed-in tariffs: get money for generating your own electricity*. `https://www.gov.uk/feed-in-tariffs`.

[4] Bello Mufutau Opeyemi. "Path to sustainable energy consumption: The possibility of substituting renewable energy for non-renewable energy". In: *Energy* 228 (2021), p. 120519.

[5] Hassan Farhangi. "The path of the smart grid". In: *IEEE power and energy magazine* 8.1 (2009).

[6] Jan Marc Schwidtal et al. "Emerging business models in local energy markets: A systematic review of Peer-to-Peer, Community Self-Consumption, and Transactive Energy models". In: *SSNR* (2022).

[7] Amrit Paudel et al. "Peer-to-peer energy trading in a prosumer-based community microgrid: A game-theoretic model". In: *IEEE Transactions on Industrial Electronics* 66.8 (2018), pp. 6087–6097.

[8] Wayes Tushar et al. "Grid influenced peer-to-peer energy trading". In: *IEEE Transactions on Smart Grid* 11.2 (2019), pp. 1407–1418.

[9] Wei Wei, Feng Liu, and Shengwei Mei. "Energy pricing and dispatch for smart grid retailers under demand response and market price uncertainty". In: *IEEE transactions on smart grid* 6.3 (2014).

[10] Walid Saad et al. "A noncooperative game for double auction-based energy trading between PHEVs and distribution grids". In: *2011 IEEE international conference on smart grid communications (SmartGridComm)*. IEEE. 2011, pp. 267–272.

[11] Bilal Ahmad Bhatti and Robert Broadwater. "Energy trading in the distribution system using a non-model based game theoretic approach". In: *Applied Energy* 253 (2019), p. 113532.

[12] Chenghua Zhang et al. "Peer-to-Peer energy trading in a Microgrid". In: *Applied Energy* 220 (2018).

[13] Woongsup Lee et al. "Direct electricity trading in smart grid: A coalitional game analysis". In: *IEEE Journal on Selected Areas in Communications* 32.7 (2014), pp. 1398–1411.

[14] Fengji Luo et al. "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain". In: *IEEE Transactions on Power Systems* 34.5 (2018), pp. 4097–4108.

[15] Wayes Tushar et al. "Peer-to-peer energy trading with sustainable user participation: A game theoretic approach". In: *IEEE Access* 6 (2018), pp. 62932–62943.

[16] Perukrishnen Vytelingum et al. "Trading agents for the smart electricity grid". In: *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1*. 2010.

[17] Weijia Liu, Donglian Qi, and Fushuan Wen. "Intraday residential demand response scheme based on peer-to-peer energy trading". In: *IEEE Transactions on Industrial Informatics* 16.3 (2019), pp. 1823–1835.

[18] Kaixuan Chen, Jin Lin, and Yonghua Song. "Trading strategy optimization for a prosumer in continuous double auction-based peer-to-peer market: A prediction-integration model". In: *Applied energy* (2019).

[19] Amir Anees, Tharam Dillon, and Yi-Ping Phoebe Chen. "A novel decision strategy for a bilateral energy contract". In: *Applied Energy* 253 (2019), p. 113571.

[20] Yang Wang et al. "Shadow price based co-ordination methods of microgrids and battery swapping stations". In: *Applied Energy* 253 (2019), p. 113510.

[21] Thomas Morstyn, Alexander Teytelboym, and Malcolm D McCulloch. "Bilateral contract networks for peer-to-peer energy trading". In: *IEEE Transactions on Smart Grid* 10.2 (2018), pp. 2026–2035.

[22] Kevin A Melendez et al. "Empowering end-use consumers of electricity to aggregate for demand-side participation". In: *Applied Energy* 248 (2019).

[23] Jianxiao Wang et al. "Incentivizing distributed energy resource aggregation in energy and capacity markets: An energy sharing scheme and mechanism design". In: *Applied Energy* 252 (2019), p. 113471.

[24] Aysajan Abidin et al. "Poster: SNIPPET—Secure and Privacy-Friendly Peer-to-Peer Electricity Trading". In: *Network and Distributed System Security Symposium*. 2020.

[25] Mehdi Montakhabi et al. "Sharing economy in future peer-to-peer electricity trading markets: Security and privacy analysis". In: *Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS), San Diego, CA, USA*. 2020, pp. 1–6.

[26] Tassos Dimitriou and Ghassan Karame. "Privacy-friendly tasking and trading of energy in smart grids". In: *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. 2013, pp. 652–659.

[27] Eman Mohammed Radi et al. "Privacy-Preserving Electric Vehicle Charging for Peer-to-Peer Energy Trading Ecosystems". In: *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE. 2019, pp. 1–6.

[28] Shaohua Li et al. "Privacy-preserving prepayment based power request and trading in smart grid". In: *China Communications* 15.4 (2018), pp. 14–27.

[29] Roozbeh Sarenche et al. "A secure and privacy-preserving protocol for holding double auctions in smart grid". In: *Information Sciences* 557 (2021), pp. 108–129.

[30] Aysajan Abidin et al. "An MPC-based privacy-preserving protocol for a local electricity trading market". In: *International Conference on Cryptology and Network Security*. Springer. 2016, pp. 615–625.

[31] Fairouz Zobiri et al. "A Privacy-Preserving Three-Step Demand Response Market Using Multi-Party Computation". In: *13th Int. Conf. Innov. Smart Grid Technol.(ISGT North America 2022), Washington DC, USA*. 2022.

[32] Fairouz Zobiri et al. "A Privacy-Preserving Peer-to-Peer Market using Demand Response and Multi-Party Computation". In: *CIGRE 2022 Kyoto Symposium, Japan*. 2022.

[33] Bingyu Liu, Shangyu Xie, and Yuan Hong. "PANDA: Privacy-Aware Double Auction for Divisible Resources without a Mediator". In: *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems*. 2020, pp. 1904–1906.

[34] Shangyu Xie et al. "Privacy Preserving Distributed Energy Trading". In: *arXiv preprint arXiv:2004.12216* (2020).

[35] Kamil Erdayandi et al. "Privacy-Friendly Peer-to-Peer Energy Trading: A Game Theoretical Approach". In: *arXiv preprint arXiv:2201.01810* (2022).

[36] Weifeng Zhong et al. "Efficient auction mechanisms for two-layer vehicle-to-grid energy trading in smart grid". In: *2017 IEEE International Conference on Communications (ICC)*. IEEE. 2017, pp. 1–6.

[37] Sebastian Lange et al. "Using revealed-bidding in power markets: A paradigmatic model". In: *2019 IEEE 28th International Symposium on Industrial Electronics (ISIE)*. IEEE. 2019, pp. 183–188.

[38] Jema Sharin PankiRaj, Abdulsalam Yassine, and Salimur Choudhury. "An auction mechanism for profit maximization of peer-to-peer energy trading in smart grids". In: *Procedia Computer Science* 151 (2019), pp. 361–368.

[39] Mustafa A Mustafa, Sara Cleemput, and Aysajan 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.

[40] *lo3energy*. `https://lo3energy.com/`.

[41] Roger B Myerson. *Game theory*. Harvard university press, 2013.

[42] Tamer Başar and Geert Jan Olsder. *Dynamic noncooperative game theory*. SIAM, 1998.

[43] *Auction Definition*. `https://en.wikipedia.org/wiki/Auction`.

[44] Suntherasvaran Murthy et al. "A comparative study of data anonymization techniques". In: *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity)*. IEEE. 2019, pp. 306–309.

[45] Marek Jawurek, Martin Johns, and Konrad Rieck. "Smart metering de-pseudonymization". In: *Computer security applications conference*. 2011, pp. 227–236.

[46] Tianqing Zhu et al. *Differential privacy and applications*. Springer, 2017.

[47] Frederik Armknecht et al. *A Guide to Fully Homomorphic Encryption*. Cryptology ePrint Archive, Report 2015/1192. `https://ia.cr/2015/1192`. 2015.

[48] Pascal Paillier. "Public-key cryptosystems based on composite degree residuosity classes". In: *International conference on the theory and applications of cryptographic techniques*. Springer. 1999, pp. 223–238.

[49] David Chaum, Ivan B Damgård, and Jeroen van de Graaf. "Multiparty computations ensuring privacy of each party's input and correctness of the result". In: *Conference on the Theory and Application of Cryptographic Techniques*. Springer. 1987, pp. 87–119.