Towards a Local Electricity Trading Market based on Secure Multiparty Computation

Aysajan Abidin, Abdelrahaman Aly, Sara Cleemput, and Mustafa A. Mustafa

KU Leuven, ESAT-COSIC and iMinds,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
{firstname.lastname}@esat.kuleuven.be

Abstract. This paper presents a local electricity trading market that allows users to trade excess electricity among themselves in a decentralised and privacy-preserving manner. Users who have more electricity generated by their renewable energy sources than they need for themselves, can sell this electricity to other users using a bidding mechanism based on secure multiparty computations. Based on the bidding prices the market computes the clearance price at which the electricity will be traded. Furthermore, it performs bid selection, as well as other market tasks. The use of secure multiparty computations ensures that neither external nor internal adversaries can compromise the privacy of any user.

Keywords: Secure Multiparty Computation, Smart Grid, Electricity Trading, Local Electricity Market, Renewable Energy Sources.

1 Introduction

The Smart Grid (SG) is an extension of the traditional electricity grid with bidirectional communication between the main components in the grid. For example, households will be equipped with smart meters, which not only measure electricity consumption, but also report these data to a supplier and/or grid operator on a regular basis, allowing real-time grid management [1]. The smart grid has many potential advantages, such as improved grid management, increased efficiency and reliability of the grid, and seamless integration of a vast number of Renewable Energy Sources (RESs) into the distribution grid. The latter mainly consist of solar panels and/or wind turbines, owned by individual households.

These RESs generate electricity, which can be consumed directly by the household itself. However, if the RES generates more electricity than required by the household at a specific moment in time, the RES owner may choose to sell this excess electricity to other consumers. Currently, households can only sell such excess electricity to their own suppliers, usually for a regulated, non-competitive price. To address this limitation, a local electricity market that allows RES owners to sell their excess electricity directly to other households in their neighbourhood has been proposed by Mustafa et al. [2]. Such a market (as shown in Fig. 1) has many advantages: it (i) generates less green house gas

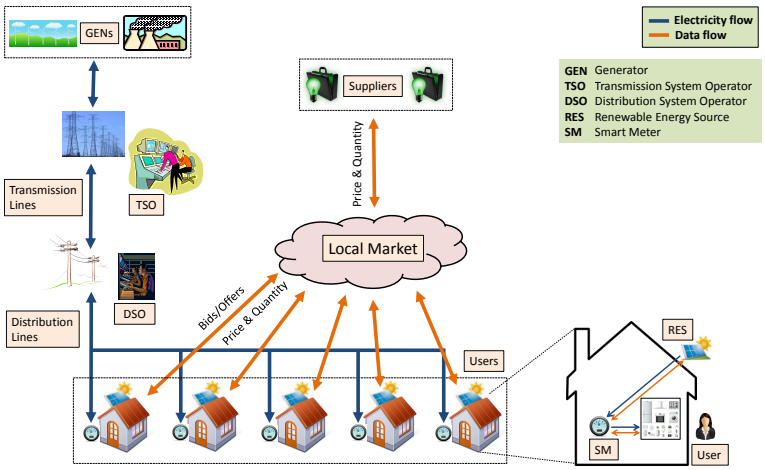

Fig. 1. A local market for trading electricity from RESs [2].

emissions and is thus more environmentally friendly, (ii) allows better utilisation of the present electricity lines, (iii) reduces costs, and (iv) increases users' profits.

However, a potential problem with such a local electricity market are the threats to the trading users' privacy [2]. Users' bids and offers reveal a significant amount of private information about their lifestyle. For example, from the pattern of a user's bids one can infer his/her consumption profile, since bids always include the required amount of electricity. This consumption profile has already been shown to reveal a lot of sensitive private information [3–7].

There are various proposals for an electricity trading market that allows users to sell (or buy) directly to (or from) each other or suppliers, using game-theoretic approaches (cf. Section 2). None of these, however, addresses privacy concerns. The security and privacy concerns in such a local market have been analysed by Mustafa et al. [2], however, no concrete solution has been proposed. In this work, we not only propose an intuitive bidding market for trading electricity, but we also address both the security and privacy concerns.

Contribution. Specifically, we propose a secure local market that allows users to trade electricity among themselves in a privacy-preserving manner. This market uses secure multiparty computation (MPC) to ensure that neither external nor internal adversaries can compromise the privacy of any of the users. The main contributions of this paper are the following:

- A novel scheme for local electricity trading that allows users to trade electricity among themselves.
- A novel application of MPC to identify the selected bids, calculate the clearance price, and compute the total amount of electricity traded by the users belonging to each individual supplier in a data oblivious and secure manner.

Outline. Section 2 describes the related work. Section 3 elaborates on the system model, threat model, assumptions, functional and security requirements and MPC. Sections 4 and 5 describe our proposed secure local market. Finally, in Section 6 we conclude the paper and give directions for future work.

2 Related Work

2.1 Privacy in Smart Grid

The importance of preserving users' privacy in SG has been already recognised by the research community [8–10]. However, the majority of the proposed solutions focus on privacy-preserving smart metering used for efficient grid management and billing. Some work rely on anonymisation of the metering data sent by smart meters [11–13], whereas others on aggregation of data using homomorphic cryptographic schemes [14–17]. For example, Petrlic [12] proposed equipping each smart meter with a trusted module so the meter can act as a tamper-resistance device, and calculate users' bills. Molina-Markham et al. [13] proposed to use zero-knowledge proofs to allow smart meters to calculate their monthly bills without providing suppliers with metering data, while at the same time allowing the suppliers to verify the correctness of these calculations. Jawurek et al. [18] proposed a plug-in component placed at the communication link between each meter and a supplier. This component intercepts all data sent by the meter, generates signed commitments of these data and forwards only the commitments to the supplier. Then, it obtains the pricing data from the supplier, calculates the bill and sends only the user's final bill to the supplier. A similar approach to the one just mentioned is proposed by Rial and Danezis [19]. However, instead of having a plug-in component, the authors suggest to have a more powerful user device which could deal with more complex electricity tariffs. Danezis et al. [20] proposed an improved version of the aforementioned protocol by Jawurek et al. [18]. In their protocol, each meter adds some random noise to its final bill, so that the supplier can not deduct any useful information about the user's consumption pattern from the bill itself. However, this comes at a cost. The user has to pay a deposit to the supplier upfront, so the supplier can be assured that, even if the user reports a lower than the actual bill, the deposit can cover this difference.

2.2 Local Electricity Markets

Yaagoubi and Mouftah [21] proposed a market that allows buyers to find a seller with cheaper electricity prices and enough supply to minimize their electricity bill. A modified regret matching procedure used by by buyers to determine the best seller. Vytelingum et al. [22] proposed an electricity market that is based on continuous double auction and automatically manages the congestion within the grid. Lee et al. [23] proposed a direct trading between small-scale suppliers and users without the involvement of traditional retailers. Tushar et al. [24] argued that allowing RES users to choose the price at which they are willing to sell

their excess electricity is beneficial for them. Ampatzis et al. [25] proposed a local electricity market for coordinating RESs and concluded that the uniform pricing, i.e., a single trading price for all, increases revenues for users. Bayram et al. [26] provided an overview of distributed energy trading concepts in smart grid and argued that the biggest motivation for users to take part in such markets is the cost savings and increased profits. Mustafa et al. [2] performed a comprehensive security analysis of a local electricity market and raised the privacy concerns of such a market. However, they proposed no concrete solution.

2.3 MPC Protocols for Electricity Markets

Since Yao's seminal contribution [27] MPC has grown from a theoretical result, to a mechanism used in real life applications [28]. This is in part motivated by the development of various Frameworks e.g., VIFF, Tasty, Sharemind [29–31], but also for the continuous improvements in terms of efficiency and security of the protocols by themselves [32–34]. On the topic at hand, contributions on problems like secure comparisons, secure sorting, network flows [35–38] opened the door for the design of auction mechanisms based on day-ahead electricity markets [39] where electricity suppliers and generators can interact among themselves in a secure and privacy-preserving manner. The present work introduces a secure scheme focused on the local electricity market, i.e., the relationship between the users (RES) and the suppliers. This is, to the best of our knowledge, the first work that tackles the privacy issues in local markets from an MPC perspective.

3 Preliminaries

This section elaborates on the system model, threat model, assumptions and functional, security and privacy requirements on which our solution is based.

3.1 System Model

As shown in Fig. 2, the local electricity trading market analysed in [2] comprises the following entities:

- **Renewable Energy Sources (RESs)** are mini electricity generators (e.g., solar panels) located on users' premises. The electricity they generate is usually consumed by their owners. However, surplus electricity may be injected into the grid.
- **Smart Meters (SMs)** are advanced metering devices which can measure the amount of electricity flowing from the grid to the house and vice versa. They also perform two-way communications with other entities, e.g., a supplier, a grid operator and/or an in-home display.
- **Users** are people who consume electricity and are billed for this.

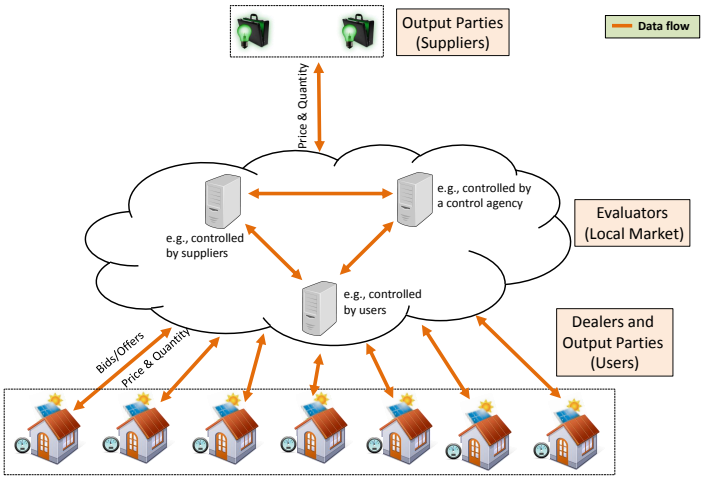

Fig. 2. A proposed local market with MPC for trading electricity from RESs.

- **Suppliers** are responsible for supplying electricity to all users who could not get a sufficient amount of electricity from their own RES or on the local market. They buy this electricity from generators and sell it to users. They are also obliged to buy the electricity their customers inject into the grid, if the customer did not manage to trade it on the local market.
- The **Local Electricity Market** is the entity responsible for receiving users' bids and offers, computing the electricity trading price, selecting the trading users, and informing the selected users as well as the suppliers of the amount of electricity traded on the local market. The calculations can be done by several servers owned by representatives of different entities, e.g., users, suppliers, operators or control agencies.

3.2 Threat Model

The treat model used in our design is as follows.

- Users are malicious. They may try to modify data sent by their (or other users') SMs in an attempt to gain financial advantage and/or learn other users' bids, offers or data.
- Suppliers are malicious. They may try to modify users' bids/offers to the local market in an attempt to influence the electricity trading price on the market. They may also try to learn individual users' consumption data and/or data of any group of customers contracted by their competitors.
- The local electricity market is honest-but-curious. It follows the protocol specification, but may attempt to learn individual users' offers/bids or consumption data.

– External entities are malicious. They may eavesdrop data in transit trying to discover confidential data and/or modify the data in an attempt to disrupt the local electricity market and/or the SG.

3.3 Assumptions

Taking into account the above presented threat model, our proposed solution is subject to the following assumptions.

(A1) Each entity in the system model has a unique ID.
(A2) SMs are tamper-evident. No one (including their users) can tamper with them without being detected.
(A3) All entities are time synchronized.
(A4) Each SM, LEM server and supplier is equipped with a distinct public/private key pair. The public keys are certified by a trusted authority. Each entity is aware of other entities' certificates.
(A5) The communication channels between entities are secure and authentic.
(A6) Users are rational, i.e., they try to reduce their electricity bills by looking for the cheapest possible electricity source; if they own RESs, they try to sell the excess electricity at the highest possible price.

3.4 Design Requirements

The local electricity market should satisfy the functional and security requirements below.

Functional Requirements. We first describe the functional requirements.

(F1) The local market should receive users' bids, calculate the clearing price, and inform the users and suppliers about the outcome of the market.
(F2) Each user should learn if their bid was accepted, the market clearing price and the amount of electricity to be traded by them.
(F3) Each supplier should learn the amount of electricity imported into and exported from the grid by all its customers located in a region for each settlement (electricity trading) period, such that it can predict its customers' demand accurately. This is important to avoid imbalance fines and to be assured that it pays the correct distribution fee to the corresponding distribution system operator.

Security and Privacy Requirements. We require that the proposed market satisfies the following requirements.

(R1) **Confidentiality of users' data:** No entity (apart from the users themselves) should have access to each individual user's (i) bids or offers and (ii) traded amount of electricity for each trading period.

(R2) **Users' privacy preservation:**

a) **RES identity privacy:** The identity of a user's RES should not be disclosed to any entity.
b) **RES user identity privacy:** The identity of a RES user should not be disclosed to any entity.
c) **Trading RES user identity privacy:** The identity of a trading RES user should not be disclosed to any entity.
d) **Location privacy:** The location of a RES user should not be disclosed to any entity.
e) **Session unlinkability:** No entity (except herself) should be able to link the different tradings of a single RES user.

(R3) **Minimum data disclosure:** Suppliers should only access data that is necessary for them to avoid imbalance fines.

3.5 Used Cryptographic Primitives

MPC. Secure multiparty computation (MPC) allows any set of mutually distrustful parties to compute any function such that no party learns more than their original input and what can be inferred from the output. Secure MPC can be achieved using various cryptographic primitives. Different flavors include secret sharing [40, 41], garbled circuits [27] and homomorphic encryption [42]. In short, parties $P_i, ..., P_n$ want to compute $y = f(x_1, ..., x_n)$ guaranteeing correctness, where x_i corresponds to the secret input of party P_i, in a distributed fashion such that P_i learns y and nothing more.

Security under MPC. We can characterize the security notion as follows: a secure protocol over MPC discloses to an adversary the same information, as if the computation were carried out by a trusted ideal (non-corruptible) third party. This security notion implies that a secure MPC protocol emulates the "ideal" (trusted third party) setting, in which the third party would only need to execute a trivial (non-secure) version of the protocols introduced by this work or any other efficient mechanism. This definition allows for a variety of adversarial and communication models, offering various security levels: perfect, statistical, or computational. Seminal results prove that any functionality can be calculated with perfect security against active and passive adversaries [40, 41]. More recent results focus on efficiency and more realistic scenarios such as dishonest majorities [32–34].

4 Local Electricity Market Overview

This section gives an overview of a local electricity market by briefly describing the different stages of the market.

Offer/Bid Submission: Prior to each trading period, users submit their offers/bids to the local electricity market. With these offers/bids users inform the market on how much electricity they are willing to sell or buy during the trading period and for what price per unit. Users are free to set their own offer/bid prices. Each user's bid/offer contains: the amount of electricity, the desired price per unit and the ID of the user's contracted supplier.

Trading Price Computation The local market performs a double auction trading as follows.

- It sorts the sellers (RES owners) in increasing order of offer price and the buyers (users) in decreasing order of bid price. Whenever two or more buyers/sellers have equal offer/bid prices, the local market groups them into a single virtual buyer/seller.
- It generates the supply and demand curve. The intersection of these two curves is used to determine the trading price and the amount of electricity traded on the local market, as well as which users will trade on the market, i.e., the sellers whose offer price is lower than or equal to the trading price and the buyers whose bidding price is higher than or equal to the trading price.

Informing Users/Suppliers: The market informs the users about the amount of electricity they traded for that trading period and the price. It also informs the suppliers of the trading users about the amount of electricity agreed to be traded, so the suppliers can adjust their bids/offers on the wholesale electricity market accordingly (to avoid imbalance fines).

Delivering Electricity: During the electricity trading period sellers (buyers) should export (import) the amount of electricity they sold (bought) on the local market. If the amount of electricity the trading users import or export is different from the amount they traded, these users automatically buy (sell) the shortage (excess) of electricity from (to) their contracted supplier.

Rewards/Costs Calculation: At the end of the trading period, each SM measures the amount of electricity it imported and exported for this period, and reports these values to its user's corresponding supplier and grid operators.

Settling Payments: Once the suppliers receive the imported and exported electricity values from their customers' SMs, they use them - in conjunction with the users' trades for that trading period and the trading price - to adjust the customers' bills in order to reflect the effect of their participation in the local electricity market.

5 Secure Local Electricity Market Exchange

We propose a distributed virtual market that employs secure MPC to guarantee secrecy. Moreover, we devise a series of mechanisms that guarantee secrecy and produce the different outputs expected and needed at the various process stages.

In our scheme, bidders provide their private inputs to a virtualised third party composed of multiple computational parties. Bidders submit their bids to a series of servers that function as evaluators. The selection and the number of evaluators depend solely on the application and the needs of the parties involved, and it could rise, for instance, to as many as the number of parties involved in the computation. This approach, however, would be rather costly in terms of performance. In the current setting, we suggest that one computational party could come from the RES owners (bidders), another from the suppliers and a third one from a local control agency so that the need for a trusted third party is eliminated, while still guaranteeing security and correctness. We classify the parties involved in our scheme as follows.

Dealers are any subset of parties in charge of providing input data in shared form and distributing it among the computational parties. In our protocol, the input information is provided directly by the bidders (users via their SMs), who are thus the dealers.

Computational Parties (Evaluators) are the subset of parties in charge of the function evaluation. They operate on the shares/ciphertext they receive from the dealers (bidders).

Output Parties are any subset of parties that have access to the output shares, so that they can reconstruct the output. At the end of the computation stage, the computational parties send the output shares to the correct output parties. For instance, some information may be made public to all parties, while other information is only revealed to a specific subset, e.g., the suppliers, the bidders and the control agencies.

5.1 System Initialization

Some pre-computations (randomizations) might be performed in an "offline phase". This can be achieved by the intervention of a trusted dealer that is not directly involved at any level of the computations [32]. The amount and the purpose of the randomly generated numbers depends on the underlying security model and primitives used by the market.

Private bids for trading period t_i have to be submitted before the beginning of t_{i-2}. The auction for t_i is computed at period t_{i-2} and the outcome is announced to the users and suppliers before the end of this period. This is done to allow suppliers to trade in the wholesale electricity market during t_{i-1} so they can adjust their wholesale deals according to the outcome of the local market.

5.2 Secure MPC Market Scheme

Preprocessing for trading period t_i

1. `Bidders.` Before the start of period t_{i-2}, each individual bid is prepared by the bidder and sent to the computational parties. In the case of secret sharing, this means share generation, using the Linear Secure Secret Sharing Scheme of choice, e.g., [43], generating as many shares as needed for the computational parties participating in the scheme. This is the only input required from the bidders. Bidders then send the corresponding shares of their bids to the respective computational parties.
2. `Evaluators.` To randomly permute the bidders' input, upon reception, each (encrypted) share should be multiplied with a column of a randomized permutation matrix which can be generated following the approach of Bogdanov et al. [31]. This can be executed "offline" and should be performed before the start of period t_{i-2}.

Evaluation for trading period t_i

3. `Evaluation`. The evaluation should be performed at period t_{i-2}. In this phase, the clearance price, traded volume, and accepted and rejected bids, can be calculated and identified in a data-oblivious fashion using the shares of the users' bids. This phase allows the market to identify the clearance price, the volume of electricity traded and the adjudicated demand and supply bids in a privacy-preserving manner.

Inform Bidders and Suppliers (before the end of period t_{i-2})

4. `Bidders.` To avoid any information leakage, the order of the bids has to be hidden from any party involved in the computation. The evaluators will proceed to use the `open` operation of the underlying MPC primitive, e.g., Linear Secret Sharing, on the electricity price for period t_i. The evaluators should follow this process by opening all the submitted bids. Each evaluator will send the shares corresponding to the result of the computation to the bidder that originated the bid. The bidder can proceed to reconstruct the shares and verify the integrity of the information contained in them and whether his bid was accepted or rejected.
5. `Suppliers.` In the same fashion the evaluators send the shares of the aggregation volume to the corresponding supplier. Suppliers also learn the market clearance price. Both bidders and suppliers are informed of the results at period t_{i-2}.

5.3 Security

The MPC mechanisms used to realise the market can be achieved with perfect security under the information theoretic model against semi-honest and active adversaries with an honest majority. As previously mentioned, seminal results in [40, 41] showed that any function can be computed using MPC with the aforementioned security levels by providing secure addition and multiplication under

an arithmetic circuit paradigm. Security of our market follows from the fact that the operations are executed in a predetermined order following the arithmetic circuit paradigm. In other words, the protocol simulation can be achieved by invoking the corresponding simulators of the MPC used, and/or atomic operations in its predefined order.

6 Conclusions and Future Work

6.1 Conclusions

As the deployment of RESs, such as solar panels and wind turbines, at individual households becomes increasingly widespread, so does the demand and/or need for selling the excess electricity produced by such sources. Currently, these so-called micro-producers can only sell their excess electricity to their contracted suppliers, albeit at a considerably lower price than the retail market price. Although there have been previous attempts to address this issue by proposing an electricity trading market, none of them ensures the users' privacy. In this work we presented a novel market scheme based on MPC for trading electricity on a local market. Our scheme employs MPC to guarantee correct billing, as well as the privacy of all users.

6.2 Future Work

The present work introduces a working model as well as the generalities of a secure local market based on secure multiparty computation. Future work should use this work as a starting point, expand this scheme and introduce the design for the arithmetic circuits that would implement each of its stages related to the market calculation, and evaluate their impact on the overall scheme. This invariably would affect the input data provided by the users, hence adaptations to other stages of this scheme should be considered as well in the form of a secure local market protocol for MPC. Furthermore, such protocol must necessarily minimize any information leakage, respecting the guidelines introduced in this work, whilst providing the corresponding security and correctness analysis and security proofs if necessary. Any such protocol could make use of well known building blocks (arithmetic circuits), such as equality tests on MPC evaluating the best suitable alternative and any adaptation if needed.

Moreover, future work should focus on reducing running times and keeping the asymptotic complexity of the market calculation linear in the number of bids. Applicability in real scenarios is a priority, hence, they should consider the inclusion of an implementation for its evaluation and tuning, e.g., optimization on the usage of the underlying MPC protocols. Such testing must consider different security models and primitives, over realistic data sets using state-of-the-art equipment.

Given the real-life limits imposed by the trading markets, e.g., duration of any period t_i, possible trade-offs between performance and security should be

explored. In case such trade-offs produce any level of leakage, more in-depth analysis could be done.

Additionally, any future work should assess topics related to the homomorphic aggregation for the billing, by introducing a protocol that can work well in combination with the available information and this scheme.

Finally, topics related to balancing suppliers' accounts based on the private volumes of the electricity that was traded, without violating privacy, should also be addressed.

Acknowledgments. This work was supported by KIC InnoEnergy SE via KIC innovation project "Secured smart grid metering architecture (SAGA)", the European Commission FP7 project "Harmonized framework allowing a sustainable and robust identity for European Citizens (EKSISTENZ)" grant number: 607049, and the European Commission through the ICT programme under contract FP7-ICT-2013-10-SEP-210076296 (PRACTICE).

References

1. Farhangi, H.: The path of the smart grid. IEEE Power and Energy Magazine **8**(1) (January 2010) 18–28
2. Mustafa, M.A., Cleemput, S., Abidin, A.: A local electricity trading market: Security analysis. In: ISGT-Europe, IEEE (2016)
3. Lisovich, M.A., Wicker, S.B.: Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems. In: Clemson University Power Systems Conference, Clemson University (mart 2008)
4. Hart, G.W.: Nonintrusive appliance load monitoring. Proceedings of the IEEE **80**(12) (1992) 1870–1891
5. Laughman, C., Lee, K., Cox, R., Shaw, S., Leeb, S., Norford, L., Armstrong, P.: Power signature analysis. IEEE Power and Energy Magazine **1**(2) (mart–april 2003) 56–63
6. Bauer, G., Stockinger, K., Lukowicz, P.: Recognizing the Use-Mode of Kitchen Appliances from Their Current Consumption. In Barnaghi, P., Moessner, K., Presser, M., Meissner, S., eds.: EuroSSC'09 Proceedings of the 4th European conference on Smart sensing and context. Volume 5741 of LNCS. Springer-Verlag (2009) 163–176
7. Lam, H.Y., Fung, G.S.K., Lee, W.K.: A Novel Method to Construct Taxonomy of Electrical Appliances Based on Load Signatures. IEEE Transactions on Consumer Electronics **53**(2) (may 2007) 653–660
8. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Security Privacy **7**(3) (May 2009) 75–77
9. Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C.L.P.: Cyber security and privacy issues in smart grids. IEEE Communications Surveys Tutorials **14**(4) (Fourth 2012) 981–997
10. Kalogridis, G., Sooriyabandara, M., Fan, Z., Mustafa, M.A.: Toward unified security and privacy protection for smart meter networks. IEEE Systems Journal **8**(2) (June 2014) 641–654
11. Efthymiou, C., Kalogridis, G.: Smart grid privacy via anonymization of smart metering data. In: SmartGridComm. (2010) 238–243

12. Petrlic, R.: A privacy-preserving concept for smart grids. In: Sicherheit in vernetzten Systemen 18. DFN Workshop. Books on Demand GmbH (2010) 1–14
13. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building. BuildSys '10, New York, NY, USA, ACM (2010) 61–66
14. Li, F., Luo, B., Liu, P.: Secure information aggregation for smart grids using homomorphic encryption. In: SmartGridComm. (2010) 327–332
15. Lu, R., Liang, X., Li, X., Lin, X., Shen, X.: Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Transactions on Parallel and Distributed Systems **23**(9) (Sept 2012) 1621–1631
16. Mustafa, M.A., Zhang, N., Kalogridis, G., Fan, Z.: MUSP: Multi-service, user self-controllable and privacy-preserving system for smart metering. In: 2015 IEEE International Conference on Communications (ICC). (June 2015) 788–794
17. Mustafa, M.A., Zhang, N., Kalogridis, G., Fan, Z.: DEP2SA: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure. IEEE Access **3** (2015) 2828–2846
18. Jawurek, M., Johns, M., Kerschbaum, F.: Plug-in privacy for smart metering billing. In Fischer-Hbner, S., Hopper, N., eds.: Privacy Enhancing Technologies. Volume 6794 of LNCS. Springer Berlin Heidelberg (2011) 192–210
19. Rial, A., Danezis, G.: Privacy-preserving smart metering. In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society. WPES '11, New York, NY, USA, ACM (2011) 49–60
20. Danezis, G., Kohlweiss, M., Rial, A.: Differentially private billing with rebates. In: Information Hiding. Volume 6958 of LNCS. Springer Berlin Heidelberg (2011) 148–162
21. Yaagoubi, N., Mouftah, H.T.: Energy trading in the smart grid: A game theoretic approach. In: Smart Energy Grid Engineering (SEGE), 2015 IEEE International Conference on. (Aug 2015) 1–6
22. Vytelingum, P., Ramchurn, S.D., Voice, T.D., Rogers, A., Jennings, N.R.: Trading agents for the smart electricity grid. In: Proceedings of the 9th Int. Conf. on Autonomous Agents and Multiagent Systems: Volume 1. AAMAS '10, Richland, SC, Int. Foundation for Autonomous Agents and Multiagent Systems (2010) 897–904
23. Lee, W., Xiang, L., Schober, R., Wong, V.W.S.: Direct electricity trading in smart grid: A coalitional game analysis. IEEE Journal on Selected Areas in Communications **32**(7) (July 2014) 1398–1411
24. Tushar, W., Yuen, C., Smith, D.B., Poor, H.V.: Price discrimination for energy trading in smart grid: A game theoretic approach. IEEE Transactions on Smart Grid **PP**(99) (2016) 1–12
25. Ampatzis, M., Nguyen, P.H., Kling, W.: Local electricity market design for the coordination of distributed energy resources at district level. In: IEEE PES Innovative Smart Grid Technologies, Europe. (Oct 2014) 1–6
26. Bayram, I.S., Shakir, M.Z., Abdallah, M., Qaraqe, K.: A survey on energy trading in smart grid. In: Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on. (Dec 2014) 258–262
27. Yao, A.C.C.: Protocols for secure computations (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science, IEEE (1982) 160–164
28. Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft,

T.: Secure multiparty computation goes live. In: Financial Cryptography, Springer (2009) 325–343
29. Geisler, M.: Cryptographic protocols: theory and implementation. PhD thesis, Aarhus University Denmark, Department of Computer Science (2010)
30. Henecka, W., Kögl, S., Sadeghi, A.R., Schneider, T., Wehrenberg, I.: Tasty: tool for automating secure two-party computations. In: CCS, ACM (2010) 451–462
31. Bogdanov, D., Laur, S., Willemson, J.: Sharemind: A Framework for Fast Privacy-Preserving Computations. In: ESORICS. Volume 5283 of LNCS., Springer (2008)
32. Damgård, I., Pastro, V., Smart, N.P., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: CRYPTO. Volume 7417 of LNCS., Springer (2012) 643–662
33. Damgård, I., Keller, M., Larraia, E., Pastro, V., Scholl, P., Smart, N.P.: Practical covertly secure mpc for dishonest majority or: Breaking the SPDZ limits. In: ESORICS. Volume 8134 of LNCS. Springer (2013) 1–18
34. Bendlin, R., Damgård, I., Orlandi, C., Zakarias, S.: Semi-homomorphic encryption and multiparty computation. In: EUROCRYPT. Volume 6632 of LNCS., Springer (2011) 169–188
35. Damgård, I., Fitzi, M., Kiltz, E., Nielsen, J.B., Toft, T.: Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In: TCC. (2006) 285–304
36. Lipmaa, H., Toft, T.: Secure equality and greater-than tests with sublinear online complexity. In: ICALP (2). (2013) 645–656
37. Huang, Y., Evans, D., Katz, J., Malka, L.: Faster secure two-party computation using garbled circuits. In: USENIX Security Symposium. (2011)
38. Aly, A., Van Vyve, M.: Securely solving classical network flow problems. In Lee, J., Kim, J., eds.: ICISC 2014. Volume 8949 of LNCS., Springer (2015) 205–221
39. Aly, A., Van Vyve, M.: Practically efficient secure single-commodity multi-market auctions. In: Financial Cryptography. LNCS, Springer (2016)
40. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: STOC, ACM (1988) 1–10
41. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: STOC, ACM (1988) 11–19
42. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT. (1999) 223–238
43. Shamir, A.: How to share a secret. Commun. ACM **22**(11) (1979) 612–613