# A Privacy-Preserving Three-Step Demand Response Market Using Multi-Party Computation

Fairouz Zobiri*, Mariana Gama†, Svetla Nikova†, and Geert Deconinck*
*Dept. of Electrical Engineering (ESAT-ELECTA) & EnergyVille, KU Leuven, Leuven, Belgium
†Dept. of Electrical Engineering (imec-COSIC), KU Leuven, Leuven, Belgium
Emails: fairouz.zobiri@kuleuven.be, mariana.botelhodagama@kuleuven.be, svetla.nikova@kuleuven.be, geert.deconinck@kuleuven.be

***Abstract*—Demand response has emerged as one of the most promising methods for the deployment of sustainable energy systems. Attempts to democratize demand response and establish programs for residential consumers have run into scalability issues and risks of leaking sensitive consumer data. In this work, we propose a privacy-friendly, incentive-based demand response market, where consumers offer their flexibility to utilities in exchange for a financial compensation. Consumers submit encrypted offer which are aggregated using Computation Over Encrypted Data to ensure consumer privacy and the scalability of the approach. The optimal allocation of flexibility is then determined via double-auctions, along with the optimal consumption schedule for the users with respect to the day-ahead electricity prices, thus also shielding participants from high electricity prices. A case study is presented to show the effectiveness of the proposed approach.**

***Index Terms*—Demand response, democratization, multi-party computation, market-based control.**

## I. Introduction

The transition toward sustainable energy production requires a change in behavior from both the supply and demand sides. The supply side is shifting from the reliance on large fossil-fueled plants to distributed renewable sources at a smaller scale. The demand side is exchanging its traditional inelasticity for more flexibility via Demand Response (DR) programs. DR is defined as the ability of consumers to decrease, increase, or shift their consumption in order to offer services to a power utility. The beneficiaries of such programs are usually System Operators (SO), either transmission or distribution, or Balance Responsible Parties (BRP).

For residential consumers to make an impact on the operation of the grid, a large number of households have to take part in the DR program. As the number of households and flexible devices grows, scalability becomes a major issue for the aggregator who needs to optimally deploy the devices' flexibility. From the consumers' point of view, sharing such sensitive information as electricity consumption or device planning is seen as a privacy violation. These concerns, added to the relatively low gain, has decreased the enthusiasm of residential users for DR programs.

This work was supported in part by the Research Council KU-Leuven: C16/15/058, by the Research Foundation - Flanders through FWO SBO project SNIPPET S007619, by CyberSecurity Research Flanders with reference number VR20192203, and by ERC Advanced Grant ERC-2015-AdG-IMPaCT.

Several works have tackled these issues separately. For instance, [1] proposes an incentive-based DR program that relies on the anonymity of the participants. The authors of [2] suggest cryptography methods to ensure user privacy ahead of aggregation. Decentralized methods are among the strategies that combine privacy and scalability, e.g., [3], and blockchain in [4]. However, none of these works have combined incentive-based programs, privacy protection, inclusion of all types of controllable devices, and respect of device constraints. For example, [5] suggests a secure computation procedure for auctions in the smart grid, but does not include device constraints as required by DR programs. Likewise, [6] only includes electric vehicles.

Therefore, in this work, we propose the creation of a privacy-friendly flexibility market that uses Secure Multi-Party Computation (MPC), which is a form of Privacy Enhancing Technology (PET). The market is open to residential consumers as DR providers, with all types of flexible devices, and to utilities requiring DR. Sellers submit their volumes and prices in encrypted form to a trading platform (TP). The offers and energy constraints of the consumers are aggregated for scalability, and only then decrypted, so that no private data is disclosed. The TP performs a double auction to allocate DR from the selected sellers to the winning buyers and computes the optimal consumption schedule, while respecting device constraints. Therefore, consumers are rewarded for their flexibility (via auctions) and shielded from high prices of electricity (via device scheduling).

## II. Multi-Party Computation

Multi-Party computation is a cryptography technique that allows a set of mistrustful parties to perform a computation on their inputs without revealing anything but the result itself.

In this work, the MPC algorithm is implemented in SCALE-MAMBA [7], a framework that implements actively-secure-with-abort MPC protocols. If a set of adversaries deviates from the protocol, the honest parties will catch it with overwhelming probability and then abort the procedure. SCALE works in the pre-processing model, where the computation can be split into two phases: an offline phase, during which input-independent data is generated, and an online phase, where this data is used to perform the desired computation. This allows us to execute more expensive operations ahead of time, resulting in a fast online phase. We will be using Shamir Secret Sharing based MPC, where each secret value is divided into several shares and each party is given one of them. The secret value cannot be recovered unless a certain number of parties join their respective shares. In this scheme, it is assumed that there is an honest majority among the parties participating in the protocol, or else its security will collapse.

The actual computation is expressed (to a first approximation) in terms of additions and multiplications. While additions are performed locally, multiplications require communication between parties, meaning that a large number of parties becomes costly in terms of performance. The computation is hence delegated to a small number of MPC parties, which should have conflicting interests in order to prevent collusion. In one case, the parties might consist of a user representative, a supplier, an aggregator, and the TP.

## III. System Architecture

Similarly to [8], the DR market is operated in three steps: bid/offer submission and aggregation, optimization, and final allocation. We assume our market to be a day-ahead (DA) market divided into time steps of size $\Delta t$. As in current electricity markets, $\Delta t$ ranges from 1 hour down to 5 minutes. The market is run in an interval $[0, T]$, $T$ being the final time.

The auction mechanism used is a closed-gate double-auction. Before gate opening, as suggested in [9], the TP publishes a set of price points. Residential DR providers select a price from this set and submit a DR offer to reshape/defer a device's consumption in a time interval $[t_{min}, t_{max}]$. Within a household, the home energy management service (HEMS) decides which devices can offer their flexibility, the interval $[t_{min}, t_{max}]$, and the price. Since this operation is carried out at household level, the information contained in an offer remains private. The bid is then divided into shares, and each share is sent to one of the parties responsible for the MPC.

SOs and BRPs are usually the buyers requesting DR services [10]. The buyers submit a bid containing the amount of DR that they wish to acquire and the price that they are willing to pay, for each time slot of the following day.

The computing parties jointly compute each device's flexibility, power and energy demands at each time step of the following day. Flexibility offers with similar prices are aggregated, while energy and power constraints are all added up, regardless of price. The aggregated quantities are then decrypted. Due to the large number of devices compared to the number of price points, coupled with the anonymity of the users at this stage, no party has the possibility to know the individual offers. Buyers' bids are also aggregated if they enclose similar prices. Otherwise, since the number of buyers is usually lower than the number of price points, their bids are not aggregated, and buyer bids are only anonymized.

After gate closure the TP runs an auction for each time slot of the following day. The auctions are carried out simultaneously using linear programming. The optimization results in a control sequence containing how much flexibility to activate and how much power can be consumed. The results of the

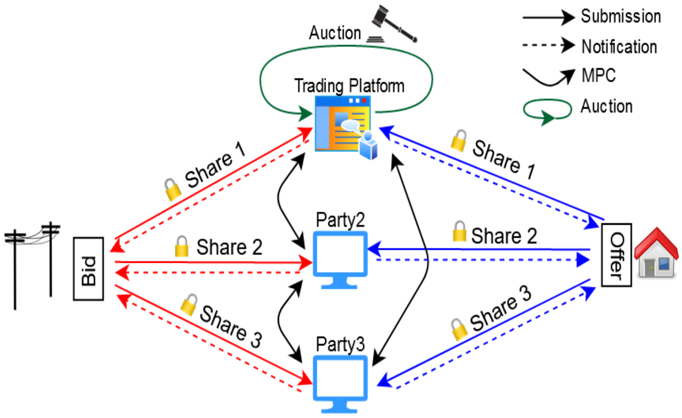


Fig. 1. Bid/Offer submission and DR market flow.

first time step are then divided among the market participants. As devices statuses change at this point, the horizon shifts to $[0 + \Delta t, T]$ and the optimization is repeated, until $[T - \Delta t, T]$ is reached. Fig. 1 illustrates the market flow. The solid straight arrows represent order submission (red for demand, blue for supply). The curved black arrows indicate the communications between parties in order to obtain the aggregated data. The TP then performs the auction (green circular arrow), and sends the results to the other parties, and jointly compute the quantities allocated to each market participant. The results are shared with the buyers and sellers, as shown by the dashed arrows.

## IV. Bid/Offer Submission and Aggregation

In this section, we explain the first stage of the DR market. In what follows, residential consumers are referred to as sellers, and the SO or BRP are referred to as buyers. We consider that we have $N$ devices and $N$ offers, whereas we have $M$ buyers with $M$ bids.

### A. *Offer and Bid Format*

During the first stage of the market operation, the buyers and sellers need to submit their bids and offers, respectively. First, the market operator publishes a set of price points, $\lambda_1, ..., \lambda_K$, from which the sellers can choose. Each seller then selects a price for each flexible device and submits an offer. A seller's offer has the following format

$$Sell = [id, P_{max}, \lambda, type, t_{min}, t_{max}, t_{run}]. \quad (1)$$

The above quantities represent:

- $id$: user's unique identifier (name or pseudonym),
- $P_{max}$: max. power that a device uses in a cycle in kW,
- $\lambda$: ask price, such that $\lambda \in \{\lambda_1, ..., \lambda_K\}$, in €/kW,
- $type$: device type 1, 2, or 3 (see below),
- $t_{min}$: min. time at which the device can start,
- $t_{max}$: max. time by which device cycle must be completed, such that $t_{max} > t_{min} + t_{run}$,
- $t_{run}$: running time of the device.

Sellers' devices are split into three types. Type1 devices are interruptible with no energy constraints e.g., an air-conditioning unit that can reduce its set-point for a period of time. Type2 devices are interruptible with an energy constraint e.g., charging an electric vehicle can be interrupted to offer DR, but has to reach a certain state of charge by $t_{max}$. Type3 devices are uninterruptible with a fixed cycle e.g., a washing machine. Note that a simplified load model is used, as a detailed model is not necessary for the TP.

As for the buyers, since their aim is to buy DR reserves for the following day, they submit their desired quantities for each time step. A buy bid has the following format

$$Buy = [Q_t, \lambda_t, t], \qquad 0 \le t \le T, \tag{2}$$

where $Q_t$ is the quantity that the buyer wishes to buy at time instant $t$ in $kW$, and $\lambda_t$ is the limit price.

### *B. Flexibility Modelling*

In this work, we consider flexibility coming from a decrease in consumption, referred to as a consumer's upward flexibility or simply flex.

From the seller's offer in (1), we can model the initial flex as follows ($f_t$ denotes the flex of a device, $E_t$ refers to the total energy consumed by a device up to time $t$)

- Type1

$$\begin{cases} 0 \le f_t \le P_{max}, \text{ for } t_{min} \le t < t_{max}, \\ 0, \text{otherwise.} \end{cases} \tag{3}$$

- Type2

$$\begin{cases} 0 \le f_t \le P_{max}, \text{ for } & t_{min} \le t < \\ & t_{max} - t_{run} + \lfloor \frac{E_t}{P_{max}} \rfloor, \\ 0, \text{otherwise,} & \end{cases} \tag{4}$$

  where $\lfloor . \rfloor$ is the floor function.
- Type3

$$f(t) = \begin{cases} P_{max}, \text{ for } & t_{min} \le t < t_{max} - t_{run}, \text{ and} \\ & E_t = 0, \\ 0, \text{otherwise.} & \end{cases} \tag{5}$$

Equation (3) indicates that a Type1 device can offer any amount of flex up to $P_{max}$ at any time between $t_{min}$ and $t_{max}$. Type2 storage devices, as seen in (4), can provide flex until the time $t_{max} - t_{run}$. However, if the device has received some power prior to $t_{max} - t_{run}$ then this interval is extended to $t_{max} - t_{run} + \lfloor \frac{E_t}{P_{max}} \rfloor$. A Type3 device, as seen in (5), can offer flex up to the time $t_{max} - t_{run}$. However, once the device is started, it can no longer offer any flex. For all types, a device with a completed cycle does not offer any flex.

### *C. Energy Constraints*

We will assume, without a loss of generality, that the initial energy state of each device is zero, i.e. $E_0^i = 0, \ \forall\, 1 \le i \le N$. Then, the energy requirements of each device at the deadline $t_{max}^i$ is $E_{max}^i = P_{max}^i \ t_{run}^i$.

At each time instant, Type1 devices have no energy constraints, while the energy constraints of a Type2 device, $\forall t \in [t_{min}, t_{max}]$, can be expressed as

$$E_{min,t}^i = \max(E_{t-1}^i, P_{max}^i(t_{run}^i + t - t_{max}^i)), \tag{6}$$

$$E_{max,t}^i = \min(P_{max}^i(t - t_{min}^i), \ E_{max}^i), \tag{7}$$

where $E_{min,t}^i$ and $E_{max,t}^i$ denote the minimum and maximum energy levels of device $i$ at time $t$. Equation (6) indicates that a Type2 device does not need any energy until $t_{max} - t_{run}$, while (7) indicates that the maximum energy it can have depends on $E_{max}^i$ and the amount of time passed since $t_{min}$.

The cycle of a Type3 device cannot be interrupted. Its energy constraints, $\forall \ t \in [t_{min}, t_{max}]$, are then ($E_{t-1}^i$ is the energy during the previous time step)

$$E_{min,t}^i = \begin{cases} 0, \text{if } E_{t-1}^i = 0 \text{ and } t_{min}^i \le t < t_{max}^i - t_{run}^i, \\ P_{max}\Delta t + E_{t-1}^i, \text{if } \ E_{t-1}^i > 0 \text{ or} \\ \qquad\qquad\qquad\qquad t \ge t_{max}^i - t_{run}^i, \end{cases} \tag{8}$$

$$E_{max,t}^i = \min(P_{max}^i(t - t_{min}^i), \ E_{max}^i). \tag{9}$$

### *D. Aggregation*

For the next stage of the algorithm to preserve user privacy, and for the approach to remain scalable regardless of the number of bids, we need to aggregate consumers flex values and energy constraints. The available flexibility of all users is aggregated at each price point and at each time instant.

Let $F_t^k$ denote the aggregated flexibility at price point $k$ and at time $t$. $F_t^k$ is the sum of the flexibility of all sellers whose ask price is $\lambda_k$, and is given by the expression below

$$F_t^k = \sum_{\substack{i=1, \\ \lambda_i = \lambda_k}}^{N} f_t^i, \ \forall\ 0 \le t \le T, \ 1 \le k \le K. \tag{10}$$

Therefore, for the horizon $[0, T]$, the aggregated flexibility is a sequence $F_0, ..., F_T$, where each element $F_t$ is a vector given by $F_t = [F_t^1, ..., F_t^K]$.

If several buyers bid the same price at time $t$, their quantities are aggregated. Let $B_t^k$ be the sum of the quantities bid by the $M > 0$ buyers engaged in the auction at time $t$, at price $\lambda_k$,

$$B_t^k = \sum_{\substack{j=1, \\ \lambda_j = \lambda_i}}^{M} Q^j, \ \forall\ 0 \le t \le T, \ 1 \le k \le K. \tag{11}$$

Likewise, the buyers' aggregated quantities form a sequence $B_0, B_1, ..., B_T$, where each element $B_t$ is a vector given by $B_t = [B_t^1, ..., B_t^K]$.

The energy constraints of each device are all aggregated at each time slot, regardless of price. Therefore, $\forall\ 0 \le t \le T$

$$E_{min,t} = \sum_{i=1}^{N} E_{min,t}^i, \ E_{max,t} = \sum_{i=1}^{N} E_{max,t}^i. \tag{12}$$

The computations so far have been carried out on encrypted data. After aggregation, the sequences $F_0, ..., F_T$, $E_{min,0}, ..., E_{min,T}$, and $E_{max,0}, ..., E_{max,T}$ are revealed to run the auction and compute device schedules.

## V. AUCTION

In this section, we describe the winner determination and power allocation problem. It is formulated as a linear programming problem. Its objective is twofold. The first objective is the fair allocation of the flex resources based on price. The second objective is to ensure that the residential consumers meet their power and energy constraints by consuming when the day-ahead price $\lambda_t^{DA}$ is at its lowest. Let $P_{av,t}$ be the maximum power that can be consumed by all the devices at time $t$. It is given by

$$P_{av,t} = \sum_{i=1}^{N} P^i_{max}, \ \forall i, \ t \in [t^i_{min}, t^i_{max}), E^i_t < E^i_{max}. \quad (13)$$

The optimization problem that we need to solve is then,

$$\max_{x,y,z} \sum_{t=0}^{T} \Big( \sum_{k=1}^{K} x_t^k B_t^k \lambda^k - \sum_{j=1}^{K} y_t^j F_t^j \lambda^j - z_t \lambda_t^{DA} P_{av,t} \Big), \quad (14a)$$

$$\text{subject to} \quad 0 \le x_t^k, y_t^j, z_t \le 1, \forall k, \forall t, \quad (14b)$$

$$\sum_{k=1}^{K} x_t^k B_t^k = \sum_{j=1}^{K} y_t^j F_t^j, \ \forall \ t, \quad (14c)$$

$$E_{t+1} = E_t + z_t P_{av,t} \Delta t, \ \forall \ t, \quad (14d)$$

$$E_{min,t} \le E_t \le E_{max,t}, \ \forall \ t. \quad (14e)$$

The first two terms of (14a) correspond to the auction winner determination problem, while the third term optimizes the total power consumption with respect to $\lambda_t^{DA}$. Constraint (14b) ensures that the market clearing volumes of buyers and sellers are below their bids and offers, respectively. It also ensures that the consumed power does not exceed the capacity of the devices. Equation (14c) indicates that demand must equal supply when the market clears. Equation (14d) indicates the simplified evolution of the sum of energy consumed by all the devices at time, $E_t = \sum_{i=1}^{N} E_t^i$. Constraint (14e) ensures that $E_t$ remains within the energy limits introduced in Section IV-C.

The above optimization problem is solved recursively with a rolling horizon. The first horizon, as indicated by (14a), is given by the interval $[0, T]$. The allocated flex and power for the first time step are divided among sellers and buyers. The horizon then becomes $[\Delta t, T]$. The flex and energy constraints are recomputed according to (3)-(9) for each device, and aggregated according to (10)-(12). The optimization problem is solved for $t \in [\Delta t, T]$, and the process is repeated again.

## VI. FLEXIBILITY AND POWER ALLOCATION

Let $F^1_{al,t}, ..., F^K_{al,t}$, where $F^k_{al,t} = y_t^k F_t^k$, be the total flexibility allocated at each price at time $t$. Let also $P_{con,t} = z_t P_{av,t}$ denote the total allocated consumption power at $t$. Another round of MPC divides these values among the users.

We start by dividing the consumption power, so that DR providers who need to consume urgently are given priority. The sellers whose offers are active ($t_{min} \le t \le t_{max}$) are first ranked according to the following criteria

1) Type3 devices already running,
2) Type2 and Type3 devices with $E^i_t < E^i_{min,t+1}$,
3) the remaining devices are ranked according to $t_{max} - t_{run}$ from the earliest to the latest.

The consumption power is then divided on each device as follows. All devices of $Type3$ and all devices up to the one-before-last receive $P^i_{max}$. The last non-$Type3$ device receives the remaining power after subtracting all the above allocations. Once $P_{con,t}$ is depleted, the remaining devices can offer their flexibility.

At each price point $\lambda_k$, where $F^k_{al,t} > 0$, the sellers asking for $\lambda_k$ are ranked according to their remaining time ($t_{max}$ minus the time it takes to complete the device's cycle) from the earliest to the latest. As an example, all the sellers asking for a price $\lambda_1$ are ranked according to their remaining time. The quantity $F^1_{al,t}$ is divided among them as follows. All devices of $Type3$ and all other devices up to the one-before-last receive a flex value equal to $P^i_{max}$. The last non-$Type3$ device receives the remaining flex after subtracting all the above flex allocations. As to the buyers, the flex is also divided among them proportionally to the bid volumes.

## VII. CASE STUDY

We have tested our approach on a data set containing 200 devices that submit a bid to the platform. The set contains 4 types of devices; air-conditioning units considered devices of Type1, electric vehicles (EV) of Type2, washing machines and dishwashers of Type3. For simplicity, we have chosen $\Delta t = 1\text{h}$. The minimum and maximum running time of each appliance, normally determined by the HEMS, are chosen randomly. The TP publishes 6 price points for the sellers to choose from. We assume there is only one buyer, who is free to choose its prices.

Fig. 2 shows the DR provided by the sellers (red dashed line) versus the regulation requested by the buyer (solid blue line). On some intervals, DR covers a large part of the buyer's requests, such as the interval $t = 07\text{h}00$ to $t = 13\text{h}00$, whereas on some intervals, very little DR is allocated. Fig. 3 shows the consumed power and the DA prices. While DR allocation depends on the ask prices of the sellers and the bid prices of the buyers, Fig. 3 shows that when the DA price is low, sellers are encouraged to consume electricity, whereas when the prices are high, sellers have an incentive to provide their flexibility.

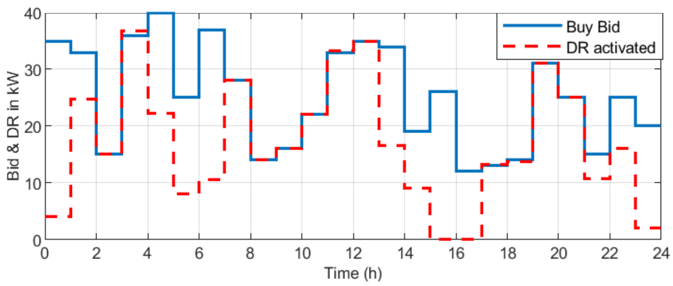


Fig. 2. Activated demand response and buyer's bid.

Fig. 4 shows the energy of two devices. The solid red line represents the energy of an EV, while the starred black line

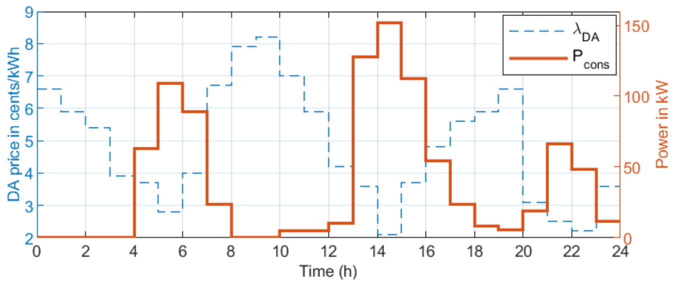


Fig. 3. Consumption power with the DA price.

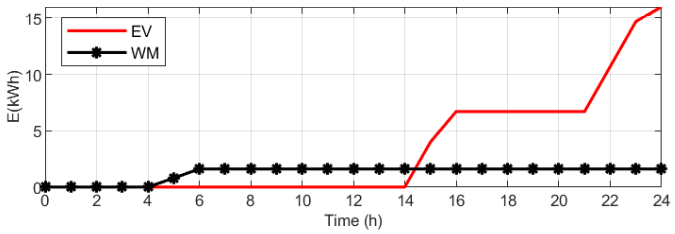


Fig. 4. Evolution of the energy of two different devices.

shows the energy consumed by a washing machine (WM). The EV needs to be charged to 16 kWh by $t = 00\text{h}00$ at the end of the day. We can see that since it is a Type2 device, charging can be interrupted, as occurred from $t = 16\text{h}00$ to $t = 21\text{h}00$. However, the EV battery reaches the required charge in time. The cycle of 2h of the WM cannot be interrupted, and it can be seen on Fig. 4 that it runs continuously. The device was available from $t = 01\text{h}00$ to $t = 13\text{h}00$, while its cycle completes at $t = 06\text{h}00$.

The MPC part of our scheme is implemented in SCALE-MAMBA using Shamir Secret Sharing between 3 parties. The aggregation step of the algorithm only requires additions to be performed, and thus it has virtually no impact on the total runtime. On the other hand, computing the device's flexibility and energy constraints, as well as ordering the devices according to consumption urgency prior to the allocation steps, will require multiple comparisons over encrypted data. These operations consume a large amount of preprocessed data and need multiple communication rounds, therefore having a noticeable effect on the runtime. To reduce the cost associated with ordering the devices according to $t_{max} - t_{run}$ during the allocation step, we sort the devices into five urgency categories, where devices in the same category are in no particular order. For the tested setting, the total runtime of the online phase of all the MPC steps for the entire auction is around 30 minutes. All the MPC parties run identical machines with an Intel i-9900 CPU and 128GB of RAM. The ping time between the machines is 1.003 ms.

## VIII. Conclusion

In this work, we presented a privacy-friendly auction mechanism to match residential DR providers and grid operators. This approach has several advantages. Firstly, it is privacy-friendly by design, as individual offers remain encrypted. Operations on them are only carried out via MPC. An advantage of MPC compared to other Computation Over Encrypted Data techniques is its somewhat low computational overhead, allowing efficient computation of relatively complex operations. The drawback of MPC is potentially high communication overhead, restricting the number of computing parties. Secondly, users are encouraged to comply with the DR programs via remuneration and optimization of their energy bills. An auction ensures a fair allocation of the DR resources, while also matching electricity consumption with periods of low prices. Additionally, the aggregation and dispatch algorithms ensure the scalability of the approach and privacy when MPC cannot be used.

As future work, attention will be focused on opening the market to downward regulation as well. We also plan to increase the security by deploying our method entirely with MPC. Additionally, optimization from the utilities' side can be considered.

## IX. Acknowledgment


The authors would like to thank Prof. N. P. Smart for his help and advice during the course of this work.


## References


[1] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, pp. 1304–1313, May 2016.

[2] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "Eppdr: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053–2064, 2014.

[3] K. Sakurama and M. Miura, "Communication-based decentralized demand response for smart microgrids," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5192–5202, 2017.

[4] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "Guardian: Blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, 2020.

[5] R. Sarenche, M. Salmasizadeh, M. H. Ameri, and M. R. Aref, "A secure and privacy-preserving protocol for holding double auctions in smart grid," *Information Sciences*, vol. 557, pp. 108–129, 2021.

[6] D. Li, Q. Yang, W. Yu, D. An, X. Yang, and W. Zhao, "A strategy-proof privacy-preserving double auction mechanism for electrical vehicles demand response in microgrids," in *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–8, 2017.

[7] A. Aly, M. Keller, E. Orsini, D. Rotaru, P. Scholl, N. P. Smart, and T. Wood, "SCALE and MAMBA documentation," 2018.

[8] S. Vandael, B. Claessens, M. Hommelberg, T. Holvoet, and G. Deconinck, "A scalable three-step approach for demand side management of plug-in hybrid vehicles," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 720–728, 2013.

[9] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft, "Secure multiparty computation goes live," in *Financial Cryptography and Data Security*, pp. 325–343, Springer Berlin Heidelberg, 2009.

[10] K. Coninx, G. Deconinck, and T. Holvoet, "Who gets my flex? an evolutionary game theory analysis of flexibility market dynamics," *Applied Energy*, vol. 218, pp. 104 – 113, 2018.