An MPC-based protocol for secure and privacy-preserving smart metering

DOI:
10.1109/ISGTEurope.2017.8260202

Document Version
Accepted author manuscript

Published in:
2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings

An MPC-based Protocol for Secure and Privacy-Preserving Smart Metering

Mustafa A. Mustafa, Sara Cleemput, Abdelrahaman Aly, and Aysajan Abidin
imec-COSIC, KU Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Email: {firstname.lastname}@esat.kuleuven.be

***Abstract*—In this paper we propose a novel protocol that allows suppliers and grid operators to collect users' electricity metering data in a secure and privacy-preserving manner, based on secure multiparty computation. Our protocol is designed for a realistic scenario where the data need to be sent to various parties, such as grid operators and suppliers, and users can switch supplier at any point in time. It also facilitates an accurate calculation of electricity transmission, distribution and grid balancing fees in a privacy-preserving manner. We also present a security analysis as well as performance estimations based on well known multiparty computation protocols in C++.**

***Index Terms*—Secure Multiparty Computation, Smart Grid, Advanced Metering Infrastructure, Security, Privacy**

I. Introduction

The Smart Grid (SG) is the electrical grid of the future, adding a communication network to the traditional electrical grid infrastructure. This allows bidirectional communication between its different entities and components, facilitating automated grid management. The overall aim is to make the electrical grid more reliable and efficient [1]. This is achieved by automatically collecting fine-grained metering data from Smart Meters (SMs). These metering data include both electricity consumption and production measurements. Electricity production takes place if households own a Distributed Energy Resource (DER), e.g., solar panels. All the collected data are sent to the grid operators and suppliers several times per hour.

Access to fine-grained metering data gives suppliers two main advantages. Firstly, these data allow them to predict their customers' electricity consumption and production more accurately. This is vital for calculating the amount of electricity they need to buy on the wholesale market as they pay heavy imbalance fines for every deviation of the actual consumption compared to their purchase. Secondly, these data also allow for accurate settling of all the fees and fines after each trading period. Currently, the distribution, transmission and balancing fees, as well as the imbalance fines for the suppliers are estimated based on their number of customers in each neighbourhood. With SM data, accurate settling of fees becomes possible. The same is true for the distribution and transmission fees which suppliers pay to the Distribution Network Operator (DNO) and Transmission System Operator (TSO). Fine-grained metering data, as suggested in [2], will also play an important role in local electricity trading markets.

Unfortunately, fine-grained metering data also have disadvantages, as they pose a serious privacy threat to consumers. Any entity having access to individual users' fined-grained metering data can use non-intrusive load monitoring [3] to analyse the consumption pattern and infer user activities [4]. The Netherlands abandoned their planned mandatory roll-out of SMs because of these privacy concerns [5]. The smart metering architecture proposed by the UK government contains a centralised entity, the Data Communications Company (DCC), which collects all the metering data and provides a privacy-friendly version to the authorised entities by anonymising or aggregating the data [6]. Although this ensures privacy protection against the authorised entities (assuming the privacy-friendly version is properly generated), the sensitive data are in no way hidden from the DCC, which can access all data of all users. In Germany the Federal Office for Information Security has written a 'Protection Profile for the Gateway of a Smart Metering System' [7], according to the Common Criteria. As pointed out by von Oheimb [8], this protection profile offers relatively good security, but the cost and overheads are high.

Anonymisation and aggregation are the techniques usually used for protecting privacy. Proper anonymisation is difficult to achieve [9]. Aggregation is a more promising approach, but the current proposals [10]–[12] have several shortcomings: they are not designed for the current liberalised electricity markets in which many entities need access to users' data; they do not consider electricity generated by residential DERs and fed back into the grid, and finally they do not support transmission, distribution and balancing fee calculation.

In this paper we propose a secure and privacy-preserving protocol for collecting metering data. Our protocol ensures that authorised entities can collect the aggregated data of only the users they provide services to. Our contributions are twofold:

- We design a privacy-preserving protocol for collecting operational metering data. We use multiparty computation (MPC) to assist several data recipients in collecting the required metering data for calculating distribution, transmission and balancing fees and the imbalance fines.
- We analyse the protocol's security and complexity in realistic setting based on the UK smart metering architecture.

The rest of this paper is structured as follows. Section II discusses the related work. Section III gives the necessary preliminaries. Section IV introduces the protocol. Sections V and VI analyse the protocol's security and privacy properties, and evaluate its performance. Section VII concludes the paper.

II. Related Work

Security and privacy concerns with smart metering have been raised [4] in the past and various protocols have already been proposed [10]–[18] to address this issue. Efthymiou and Kalogridis [13] proposed that each SM uses two IDs: an attributable ID for reporting billing data, and an anonymous ID for reporting operational metering data. They assume that data recipients are not able to link both IDs. However, Tudor et al. [9] have shown that de-anonymisation is possible.

Li et al. [11] used data aggregation as privacy-preserving mechanism. To protect users' privacy during the aggregation process they proposed to use homomorphic encryption. However, their protocol does not protect against active adversaries and uses a single-recipient model. Mustafa et al. [17], [18] addressed these limitations by using digital signatures and a selective data aggregation and delivery method. Garcia and Jacobs [12] combined homomorphic encryption with a data sharing scheme to allow the data recipient to perform the aggregation. Kursawe et al. [10] proposed a lightweight aggregation scheme which requires SMs to mask their data with noise that cancels out when the data are added together. Defend et al. [19] demonstrated the feasibility of the scheme using real SMs. However, the scheme requires a complex reinitialisation process when adding or removing SMs and does not support flexible aggregation groups. Engel and Eibl [20] combined wavelet transform with homomorphic encryption method to improve the access control on metering data.

Another approach to aggregate data in a privacy-preserving and efficient manner is MPC, which has been already deployed in the SG domain [21]. Danezis et al. [14] used secret-sharing based MPC to detect fraud and SM short-cuts, and to extract advanced grid statistics. Rottondi et al. [15], [16] proposed two novel security architectures for aggregation of metering data. However, each architecture requires additional nodes placed in the grid and at the users' households, respectively.

Unlike the aforementioned work, we propose an MPC-based privacy-preserving protocol for operational metering data collection which (i) is based on a real smart metering architecture, i.e., the UK one [6], (ii) is readily applicable to a liberalised electricity market that consists of various stakeholders, (iii) takes into account not only the electricity consumption, but also generation fed back to the grid by households, and (iv) allows the TSO, DNOs and suppliers to calculate the exact distribution, transmission and balancing fees, as well as the imbalance fines based on real metering data rather than estimates.

III. Preliminaries

In this section we describe the system model and threat model, our assumptions, design requirements and notations used in the rest of the paper.

A. System Model

As shown in Fig. 1, our system model consists of the following entities:

- **Users** consume electricity and are billed by their supplier.

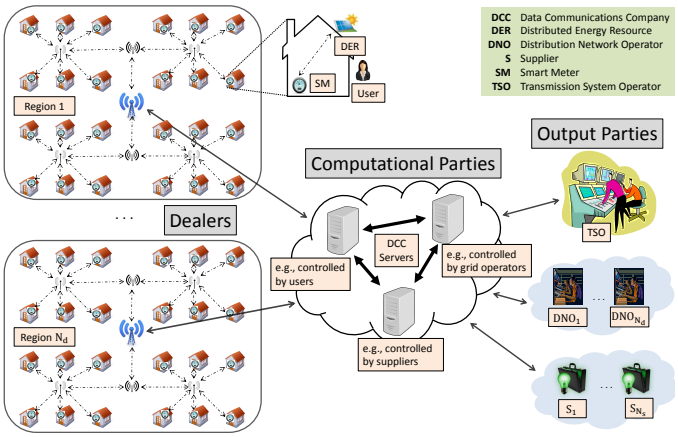

Fig. 1. System model.

- **Distributed Energy Resources (DERs)** are mini electricity generators (e.g., solar panels) located on users' premises. Most of the electricity they generate is consumed by their owners. However, surplus electricity may be injected into the grid to be consumed by other users.
- **Smart Meters (SMs)** are advanced electricity metering devices which measure the amount of electricity flowing from the grid to the house and vice versa, per time slot, t_k. The SMs regularly communicate with other authorised SG entities, such as suppliers, DNOs and TSO.
- **Suppliers** are responsible for supplying electricity to all users whose DERs did not generate sufficient electricity for their needs. They buy this electricity on the wholesale market and sell it to users. They are also obliged to buy any electricity their customers inject into the grid. If they buy an incorrect amount of electricity on the wholesale market, they must pay heavy imbalance fines.
- **Distribution Network Operators (DNOs)** are responsible for managing and maintaining the low and middle voltage distribution lines in their respective regions. They also charge suppliers distribution fees based on the electricity consumption of their customers in each time period t_k. Suppliers then charge their customers this fee in turn.
- The **Transmission System Operator (TSO)** is responsible for managing and maintaining the high voltage transmission lines, and for continuously keeping the electricity consumption and production in balance. It charges suppliers transmission and balancing fees based on the electricity consumption of their customers in each time period t_k. Suppliers pass this cost on to the users as well.
- The **Data Communications Company (DCC)** is a centralised entity that consists of several servers run by different parties. It is responsible for collecting metering data and delivering it to the TSO, DNOs and suppliers.

B. Threat Model and Assumptions

For our protocol design we use the following threat model. Users, TSO, DNOs and suppliers are considered malicious. They may manipulate users' metering data in an attempt to

gain financial advantage. Users want to lower their bills, the others want to manipulate the transmission, distribution and balancing fees as well as the imbalance fines calculations. They may also try to learn individual users' consumption data, or the aggregate consumption of a group of users located in different regions or contracted by their competitors. The DCC is considered honest but curious. It follows the protocol specifications, but it may try to learn the consumption data of individual users or the aggregate data of any group of users. External entities are considered malicious. They may eavesdrop or modify data in transit in order to gain access to confidential data or to disrupt the SG.

We also make the following assumptions. Each entity in the system model has a unique identifier. All entities are time synchronised and the communication channels among them are encrypted and authenticated. SMs are tamper-proof, thus no one can tamper with them without being detected. Note that this can be achieved by using protected SM module architectures [22], [23].

The notations used for the requirements and protocol descriptions can be found in Table I. The square brackets $[x]$ denotes secretly shared or encrypted data.

TABLE I
NOTATIONS

Symbol	Meaning
t_k	k^{th} time slot, $k = \{1, \ldots, \mathrm{N_t}\}$
d_j	the DNO operating in region j, $j = \{1, \ldots, \mathrm{N_d}\}$
s_u	u^{th} supplier, $u = \{1, \ldots, \mathrm{N_s}\}$
SM_i	the SM belonging to household i
$\mathbb{SM}$	set of all the SMs in a specific country
$\mathbb{SM}_{\mathrm{d}_j}$	set of all the SMs operated by DNO d_j
$\mathbb{SM}^{\mathrm{imp}}_{\mathrm{s}_u}$	set of all the SMs whose users buy electricity from s_u
$\mathbb{SM}^{\mathrm{exp}}_{\mathrm{s}_u}$	set of all the SMs whose users sell electricity to s_u
$\mathbb{SM}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}$	set of all the SMs operated by d_j and whose users buy electricity from s_u
$\mathbb{SM}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}$	set of all the SMs operated by d_j whose users sell electricity to s_u
$\mathrm{E}^{\mathrm{imp},t_k}_i$	amount of electricity imported by household i during t_k
$\mathrm{E}^{\mathrm{exp},t_k}_i$	amount of electricity exported by household i during t_k
$\mathbb{E}^{\mathrm{imp},t_k}$	aggregate data of all $\mathrm{E}^{\mathrm{imp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}$
$\mathbb{E}^{\mathrm{exp},t_k}$	aggregate data of all $\mathrm{E}^{\mathrm{exp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}$
$\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j}$	aggregate data of all $\mathrm{E}^{\mathrm{imp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}_{\mathrm{d}_j}$
$\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j}$	aggregate data of all $\mathrm{E}^{\mathrm{exp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}_{\mathrm{d}_j}$
$\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{s}_u}$	aggregate data of all $\mathrm{E}^{\mathrm{imp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}^{\mathrm{imp}}_{\mathrm{s}_u}$
$\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{s}_u}$	aggregate data of all $\mathrm{E}^{\mathrm{exp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}^{\mathrm{exp}}_{\mathrm{s}_u}$
$\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$	aggregate data of all $\mathrm{E}^{\mathrm{imp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}$
$\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$	aggregate data of all $\mathrm{E}^{\mathrm{exp},t_k}_i$ for $\mathrm{SM}_i \in \mathbb{SM}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}$

C. Design Requirements

The smart metering protocols should satisfy the following functional and security requirements.

1) Functional Requirements:

(F1) For each time period t_k, each DNO d_j should access:
- a) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j}$, in order to better manage the distribution network in its region,
- b) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$, $u = \{1, \ldots, \mathrm{N_s}\}$, in order to split the distribution fees fairly among the suppliers.

(F2) For each time period t_k, each supplier s_u should access:
- a) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{s}_u}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{s}_u}$, to predict its customers' electricity consumption and production accurately,
- b) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$ for $j = \{1, \ldots, \mathrm{N_d}\}$, in order to be assured that it pays the correct transmission and distribution fees to the TSO and each DNO, respectively. Note that transmission fees can also be made region-dependent to encourage suppliers to buy electricity from sources located as close to the demand as possible.

(F3) For each time period t_k, the TSO should access:
- a) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j,\mathrm{s}_u}$, $u = \{1, \ldots, \mathrm{N_s}\}$, to split transmission fees fairly among suppliers,
- b) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{s}_u}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{s}_u}$, for $u = \{1, \ldots, \mathrm{N_s}\}$, to calculate the balancing fee and imbalance fine for each supplier,
- c) $\mathbb{E}^{\mathrm{imp},t_k}_{\mathrm{d}_j}$ and $\mathbb{E}^{\mathrm{exp},t_k}_{\mathrm{d}_j}$, for $j = \{1, \ldots, \mathrm{N_d}\}$, to know which regions are the source of an imbalance, thus to decide which measures to take to avoid the imbalance, and
- d) $\mathbb{E}^{\mathrm{imp},t_k}$ and $\mathbb{E}^{\mathrm{exp},t_k}$, in order to balance the grid efficiently.

2) Security Requirements:

(S1) Confidentiality of users' data: the aggregates (over several users) of users' consumption and production data should only be accessed by authorised entities.

(S2) User privacy preservation: individual users' fine-grained consumption data should not be revealed to any SG entity.

(S3) Authorisation: Entities should only access the aggregate data of users to whom they provide services. For an DNO this means only the users living in the region it operates, for a supplier this means only its contracted users.

D. Cryptographic Notation

We adopt the arithmetic circuits paradigm, a common feature for many MPC frameworks [24], [25], under which any function can be constructed as a circuit that is composed of addition and multiplication gates. This kind of approach, which can be seen as secure under the hybrid model introduced by Canetti [26], allows us to assemble circuits to compute any function as long as no information leakage is produced; we call this characteristic obliviousness. The MPC component of our protocol can be seen as a single arithmetic circuit in charge of the consumption and production aggregation. It uses gate subsets in our unique circuit as subprotocols, oblivious equality tests and permutations.

Equality Test: Any comparison protocol devised for MPC, e.g., [27]–[29], can be used for our protocol. To simplify this process, SMs could share their ID in its bit representation. Then, as shown in Algorithm 1, the generic bitwise comparison would only require σ multiplications, where σ corresponds to the bit size of the supplier ID. These multiplications can be parallelised such that only $log(\sigma)$ communication rounds are needed.

Algorithm 1: Generic Equality Test Protocol

Input: Secret share bit representation of x, $[x]_\sigma$, where σ is its bit-size
Public scalar y to which x is compared, and its bit representation y_σ
Output: A secret share of the output of the equality test [c]

$[c] \leftarrow 0$;
for $i \leftarrow 1$ **to** σ **do**
  $[c'] \leftarrow [x]_i + y_i - 2 \cdot ([x]_i \cdot y_i)$;
  $[c] \leftarrow [c] + [c'] - [c] \cdot [c']$;
end

Number Codification: We assume all secret shared values are members of a field $\mathbb{Z}_p$ bounded by some sufficiently large prime or RSA modulus p, such that no overflow occurs. Negative numbers are coded in the standard way: the lower half of the field represents positive numbers and the upper half negative numbers. In case fixed point precision is needed, the entries can be multiplied with a sufficiently large constant to code the precision before secret sharing them, such that they can be shared as elements of $\mathbb{Z}_p$.

Parties: Our protocol comprises the following parties:

- *The dealers* are the SMs. They generate input data, including the electricity consumption and generation data measured per time slot, and send these data to the computational parties.
- *The computational parties* are appointed by the DCC. They must be parties with competing interests. We set the number of computational parties to three. They obtain input data from the dealers, cooperate with each other to perform the necessary calculations and provide the output parties with the results of the calculations.
- *The output parties* are the TSO, DNOs and suppliers. Each of them receives shares of the results of the calculations performed by the computational parties and then it combines these shares to construct its required results.

IV. Privacy-preserving Smart Metering Protocol

Our proposed protocol consists of the following four steps. Note that the protocol should be executed at every time period t_k. However, for simplicity, we omit t_k in our notation for the rest of the paper.

1. **Generation and distribution of input data:** Each SM, SM_i, in every region j, generates a tuple $\{[\mathrm{s}_u^{\mathrm{imp}}], [\mathrm{s}_u^{\mathrm{exp}}], [\mathrm{E}_i^{\mathrm{imp}}], [\mathrm{E}_i^{\mathrm{exp}}]\}$ which contains the shares of the user's contracted suppliers, consumption and generation data, and sends it to the computational parties.
2. **Region-based data aggregation:** Once all SMs have sent their tuples, the computational parties aggregate the electricity consumption and production data for each region as shown in Algorithm 2. Specifically, they loop over all the secret shared inputs to examine them one at the time. They then proceed to associate (*on lines* 4 and 9) the consumption and production data with the appropriate supplier. This is achieved by performing an oblivious equality test per loop operation (*on lines* 4 and 10). Using this result, the aggregation (*on lines* 6 and 11) can be performed by means of a multiplication and addition operation in such a way that the protocol fulfils all the functional requirements specified in Section III. The protocol is scalable as it supports an ever growing number of suppliers. Performance results are presented in Section VI. The output produced by the protocol is in shared form and represents the region-based aggregate consumption and production data per supplier.
3. **Grid-based data aggregation:** The computational parties compute the shares of all the grid-based aggregate consumption and production data by simply adding the corresponding shares of the region-based aggregate consumption and production data.
4. **Output data distribution:** Following the functional requirements specified in Section III, the shares of the previously calculated aggregations are distributed to the TSO, DNOs and suppliers, accordingly. Finally, these entities reconstruct their required results by adding the corresponding shares.

Algorithm 2: Region-based Data Aggregation

Input: Tuples from region j, $\{[\mathrm{s}_u^{\mathrm{imp}}], [\mathrm{s}_u^{\mathrm{exp}}], [\mathrm{E}_i^{\mathrm{imp}}], [\mathrm{E}_i^{\mathrm{exp}}]\}$ for $\mathrm{SM}_i \in \mathbb{SM}_{\mathrm{d}_j}$
Output: Shares of aggregate consumption data per supplier, $[\mathbb{E}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}]$
Shares of aggregate production data per supplier, $[\mathbb{E}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}]$

1 $[\mathbb{E}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}] \leftarrow \{0_1, ..., 0_{\mathrm{N_s}}\}$;
2 $[\mathbb{E}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}] \leftarrow \{0_1, ..., 0_{\mathrm{N_s}}\}$;
3 **for** $i \leftarrow 1$ **to** $|\mathbb{SM}_{\mathrm{d}_j}|$ **do**
4 **for** $u \leftarrow 1$ **to** $\mathrm{N_s}$ **do**
5 $[c] \leftarrow [\mathrm{s}_u^{\mathrm{imp}}] \stackrel{?}{=} \mathrm{s}_u$;
6 $[\mathbb{E}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}] \leftarrow [\mathbb{E}^{\mathrm{imp}}_{\mathrm{d}_j,\mathrm{s}_u}] + [c] * [\mathrm{E}_i^{\mathrm{imp}}]$;
7 **end**
8
9 **for** $u \leftarrow 1$ **to** $\mathrm{N_s}$ **do**
10 $[c] \leftarrow [\mathrm{s}_u^{\mathrm{exp}}] \stackrel{?}{=} \mathrm{s}_u$;
11 $[\mathbb{E}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}] \leftarrow [\mathbb{E}^{\mathrm{exp}}_{\mathrm{d}_j,\mathrm{s}_u}] + [c] * [\mathrm{E}_i^{\mathrm{exp}}]$;
12 **end**
13 **end**

V. Security Analysis

Our security assumptions, listed in Section III, cover some of the threats in our threat model. For instance, the natural assumption that the SMs are tamper proof and sealed protects against malicious users attempting to modify the metering data for financial advantage. The assumption that the communication channel is encrypted and authenticated, which can be achieved using TLS, protects against adversaries attempting to eavesdrop or modify the data in transit. Thus, we analyse the security of our protocol against malicious DNOs, TSO, and suppliers as well as a semi-honest (honest-but-curious) DCC.

MPC allows to compute any function with perfect (information-theoretic) security when an honest majority is assumed [24], [30]. Furthermore, according to the seminal result on MPC by Ben-Or, Goldwasser, and Wigderson (BGW) [24], perfect security against semi-honest adversaries can be achieved by using the linear secret sharing scheme introduced by Shamir [31], as long as half of the parties remain honest. Hence, for the semi-honest adversary, our protocol satisfies the specified functional requirements with no leakage, achieving perfect security under MPC [24], [30].

Consequently our protocol is secure against malicious DNOs, TSO, and suppliers as well as against a semi-honest DCC [26]. More specifically, DNOs, TSO, and suppliers cannot learn anything about individual users' consumption data from the output of the DCC's computation other than what can be learned from the output itself. As each DCC server, assumed to be semi-honest, has only the secret shares of the users' input data, it cannot learn anything about individual users' metering data. The security follows directly from the security of the underlying MPC protocols (see composability theorem [26]).

For the case of a malicious adversary, it is necessary to use verifiable secret sharing techniques [24] so that security can be achieved against collusion amongst up to two thirds of the computational parties. A complete set of simulation based proofs for the BGW protocols was introduced by Lindell et al. [32]. In recent years, various MPC protocols that offer security against dishonest majorities have been introduced, we refer to [25], [33] for the state-of-the-art.

VI. Performance and Scenario Evaluation

We evaluated the performance of our protocol using synthetically generated electricity data and the smart metering architecture proposed in the UK.

A. Electrical Grid and Smart Metering Architecture in the UK

The electrical grid in the UK is balanced by one TSO and divided into 14 regions, each managed by a distinct DNO [34]. By 2030 the UK will have around 30 million SMs [35]. Furthermore, the retail electricity market is liberalised, i.e., users can freely choose their own supplier. Currently there are more than 20 suppliers in operation in the UK, with six main ones holding an 86% retail market share [36]. Moreover, the excess electricity fed back to the grid is automatically bought by the user's contracted supplier. However, users are also free to choose a different supplier to buy back their excess electricity. Currently, only a limited subset of the suppliers buy electricity back from their consumers. Finally, a centralised entity, the DCC, will collect all the metering data from users and distribute these data to the TSO, DNO and suppliers.

B. Parameters Setting and Data Generation

Based on the UK's electrical grid and smart metering architecture, we set the following parameters. We assume there are 30 million SMs in the entire grid, equally distributed over 14 regions (each operated by a distinct DNO), one TSO, 20 suppliers and one DCC which consists of three computational servers, each managed by a different party. To avoid collusion, these parties should have contradicting interests, e.g., one could be managed by a users' association, one by the suppliers and a third one by the grid operators.

The largest six suppliers combined hold 86% of the retail market, more specifically, 23%, 15%, 15%, 12%, 11% and 10%, respectively. The other 14 suppliers hold the following market shares: one holds 3%, two hold 2% each, three hold 1% each and eight hold 0.5% each. We assume that only the largest six suppliers buy back electricity from users and that 90% of their customers sell electricity to their own supplier, whereas the other 10% sell their electricity to one of the other five suppliers. The customers of the smaller suppliers sell electricity to one of the six large suppliers. We assume that 20% of all the users have a DER installed in their homes and that during every settlement period each of these users sells between 0.5 and 2 kW of electricity to their contracted supplier. Also, for the same settlement period, all of the users buy between 0.05 and 1 kW electricity. Note that the performance of our protocol does not depend on the electricity data but rather on the smart metering architecture, which, in our case, is set using parameters from the UK's real electrical grid architecture and retail electricity market shares.

C. Environment Setting

For our experimentation, we use C++ and the custom implementations of Shamir's secret sharing scheme [31], its linear addition and the improved BGW protocol from Gennaro et al. [24], [37] for multiplication. A detailed description of the implementation is present in [38]. Our implementation considers inputs of length 32 bits when comparisons protocols that provide statistical security are being used, e.g., [39]. In our case, we make use of the generalised equality test from Algorithm 1. This allows us to use up to 63-bits-long inputs. We run the three computational parties on the same machine, a 64-bit 2*2*10-cores Intel Xeon E5-2687 server at 3.1GHz, thus our results do not consider network latency.

D. Computational Complexity

We project the computational complexity of our protocol as follows. The protocol requires $|\mathrm{s}_u| \times \mathrm{N_s} + \mathrm{N_s}$ number of multiplications per inner loop (of Algorithm 2) for each SM, where $|\mathrm{s}_u|$ is the bit-length size of the supplier ID and $\mathrm{N_s}$ is the number of suppliers in the retail market. The first term is related to the number of multiplications needed to perform the equality tests and the second for the aggregation. This results in a total computational complexity of $|\mathbb{SM}_{\mathrm{d}_j}| \times (|\mathrm{s}_u| \times \mathrm{N_s} + \mathrm{N_s})$ number of multiplications taking into account that the two inner loops of Algorithm 2 can be preformed in parallel.

Additionally, we measured the performance of the multiplication implementation by executing 2 million multiplications and averaging the computational time, yielding a multiplication per 20.8×10^{-6} seconds. Furthermore, we estimated the computational cost of Algorithm 2 for various number of SMs located in each region in a setting with a fixed number of suppliers, $\mathrm{N_s} = 10$ and $|\mathrm{s}_u| = 8$. Our results are shown in Table II. Note that these results show all the necessary CPU time to be allocated regardless of the number of processors, i.e, one processor would take such time, two processors roughly half and so forth. Considering that in each UK region there will be on average 2.2 million SMs, our protocol could easily be executed in less than 10 minutes by simply dividing the work between eight threads, thus making it practical to use for the UK smart metering architecture.

TABLE II
COMPUTATIONAL RESULTS.

SMs per region	Multiplications	CPU time in seconds
$0.1M$	$9M$	187.2
$0.5M$	$45M$	936.0
$1.0M$	$90M$	1 872.0
$2.5M$	$225M$	4 680.0
$5.0M$	$450M$	9 360.0

VII. CONCLUSIONS

We introduced an MPC-based protocol for aggregating electricity metering data used for operational purposes in a secure and privacy-friendly manner. Such data can be used by operators and suppliers to calculate transmission, distribution and balancing fees, as well as imbalance fines. To the best of our knowledge this is the first protocol to aggregate consumption as well as production electricity data for different suppliers with perfect security. We also analysed the complexity of the protocol to show its feasibility in practice.

ACKNOWLEDGMENTS

This work was supported by the Research Council KU Leuven: C16/15/058 and European Commission through KU Leuven BOF OT/13/070, H2020-DS-2014-653497 PANORAMIX and H2020-ICT-2014-644371 WITDOM.

REFERENCES

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, January 2010.

[2] M. A. Mustafa, S. Cleemput, and A. Abidin, "A local electricity trading market: Security analysis," in *IEEE PES ISGT-Europe*, 2016, pp. 1–6.

[3] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[4] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Systems Journal*, vol. 8, no. 2, June 2014.

[5] W. Heck, "Smart energy meter will not be compulsory," *NRC Handelsblad*, April 2009, http://vorige.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory.

[6] DECC, "Smart metering implementation programme data access and privacy," 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf.

[7] Federal Office for Information Security - BSI, "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP) - Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen," SMGW-PP Version 1.3, 2014, https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf.

[8] D. von Oheimb, "IT Security Architecture Approaches for Smart Metering and Smart Grid," in *First International Workshop on Smart Grid Security (SmartGridSec)*, 2013, pp. 1–25.

[9] V. Tudor, M. Almgren, and M. Papatriantafilou, "A study on data depseudonymization in the smart grid," in *ACM 8th European Workshop on System Security*, 2015, pp. 1–6.

[10] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *11th Int. Symposium on Privacy Enhancing Technologies (PETs)*. Springer, 2011, pp. 175–191.

[11] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *IEEE 1st Int. Conf. on Smart Grid Communications (SmartGridComm)*, Oct 2010, pp. 327–332.

[12] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *6th Int. Workshop on Security and Trust Management (STM)*. Springer, 2011, pp. 226–238.

[13] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *IEEE 1st International Conference on Smart Grid Communications (SmartGridComm)*, October 2010, pp. 238–243.

[14] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin, "Smart meter aggregation via secret-sharing," in *1st ACM Workshop on Smart Energy Grid Security (SEGS 2013)*. ACM, 2013, pp. 75–80.

[15] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," *Computer Networks*, vol. 57, no. 7, pp. 1699–1713, 2013.

[16] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1342–1354, July 2013.

[17] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "MUSP: Multi-service, user self-controllable and privacy-preserving system for smart metering," in *Int. Conf. on Communications (ICC)*, 2015, pp. 788–794.

[18] ——, "DEP2SA: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure," *IEEE Access*, vol. 3, pp. 2828–2846, 2015.

[19] B. Defend and K. Kursawe, "Implementation of privacy-friendly aggregation for the smart grid," in *1st ACM Workshop on Smart Energy Grid Security (SEGS 2013)*, 2013, pp. 65–74.

[20] D. Engel and G. Eibl, "Multi-resolution load curve representation with privacy-preserving aggregation," in *IEEE PES Innovative Smart Grid Technologies (ISGT Europe 2013)*, Oct 2013, pp. 1–5.

[21] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An MPC-based privacy-preserving protocol for a local electricity trading market," in *15th Int. Conf. on Cryptology and Network Security (CANS 2016)*, ser. LNCS, vol. 10052. Springer, 2016, pp. 615–625.

[22] S. Cleemput, M. A. Mustafa, and B. Preneel, "High assurance smart metering," in *IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2016, pp. 294–297.

[23] J. T. Mühlberg, S. Cleemput, M. A. Mustafa, J. Van Bulck, B. Preneel, and F. Piessens, "An implementation of a high assurance smart meter using protected module architectures," in *11th Int. Conf. on Information Security Theory and Practice (WISTP 2016)*. Springer, 2016, pp. 53–69.

[24] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *STOC*. ACM, 1988, pp. 1–10.

[25] M. Keller, E. Orsini, and P. Scholl, "Mascot: Faster malicious arithmetic secure computation with oblivious transfer."

[26] R. Canetti, "Security and composition of multiparty cryptographic protocols," *Journal of Cryptology*, vol. 13, no. 1, pp. 143–202, 2000.

[27] I. Damgård, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft, "Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation," in *TCC 2006*, ser. LNCS, vol. 3876. Springer, 2006, pp. 285–304.

[28] H. Lipmaa and T. Toft, "Secure equality and greater-than tests with sublinear online complexity," in *ICALP (2)*, 2013, pp. 645–656.

[29] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-preserving Aggregation of Multi-domain Network Events and Statistics," in *USENIX Security 2010*, 2010, pp. 15–15.

[30] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols," in *STOC*. ACM, 1988, pp. 11–19.

[31] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[32] G. Asharov and Y. Lindell, "A full proof of the BGW protocol for perfectly secure multiparty computation," *Journal of Cryptology*, pp. 1–94, 2015.

[33] I. Damgård, M. Keller, E. Larraia, V. Pastro, P. Scholl, and N. P. Smart, "Practical covertly secure MPC for dishonest majority or: Breaking the SPDZ limits," in *ESORICS*. Springer, 2013, vol. 8134, pp. 1–18.

[34] ELEXON, "The electricity trading arrangements a beginners guide," Nov. 2015, available online: https://www.elexon.co.uk/wp-content/uploads/2015/10/beginners_guide_to_trading_arrangements_v5.0.pdf.

[35] DECC, "Smart meters, smart data, smart growth," 2015, available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/397291/2903086_DECC_cad_leaflet.pdf.

[36] ofgem, "Electricity supply market shares by company: Domestic (GB)," June 2016, available online: https://www.ofgem.gov.uk/chart/electricity-supply-market-shares-company-domestic-gb.

[37] R. Gennaro, M. O. Rabin, and T. Rabin, "Simplified VSS and fast-track multiparty computations with applications to threshold cryptography," in *PODC '98*. ACM, 1998, pp. 101–111.

[38] A. Aly, "Network flow problems with secure multiparty computation," Ph.D. dissertation, Universté catholique de Louvain, IMMAQ, 2015.

[39] O. Catrina and S. de Hoogh, "Improved primitives for secure multiparty integer computation," in *SCN*, 2010, pp. 182–199.