Secure and Privacy-preserving Local Electricity Trading Market – an MPC Application

www.esat.kuleuven.be/cosic/secure-and-privacy-preserving-local-electricity-trading-market-an-mpc-application/

September 1, 2016

Smart Grid (SG) has been widely tipped as the tool that will help us revolutionise the way we generate, trade and consume electricity. But what is SG? SG is the next generation electrical grid that can support bi-directional electricity and communication flows between different entities of the grid (e.g., grid operators, suppliers, users, third parties, etc.), so that the grid can be managed more efficiently and reliably [1].

One of the long-term goals of governments is to shift from having few large centralised electricity sources to having many decentralised local electricity sources. To achieve this goal, many governments encourage people to install solar panels in their homes by offering them various incentives [2], usually at the expenses of other users. However, this approach has two limitations: (i) it leads to the increase of the average electricity bill of users, as well as, (ii) it is financially beneficial only to users with solar panels.

One proposed solution to overcome these limitations is to create a local electricity market where users can trade electricity among themselves in an open and competitive market, i.e., to let users sell their excess electricity at a price they are willing to sell it for, and others to buy electricity at the price they are willing to pay for it. Is this possible? Yes, with the help of SG, this is possible seeing that trading electricity between two entities is just a virtual transaction. What needs to be done is: (i) sellers and buyers of electricity agree on the amount and price of the electricity to be traded at a given time period, (ii) they inform their respective suppliers about their agreements, and (iii) they inject/consume electricity at the particular time slot according to their agreement. Such a local electricity market would allow (i) users with excess electricity to sell this electricity for a higher price than the one they are currently getting from their suppliers and (ii) users with an electricity demand to buy electricity for a cheaper price than the one offered by their respective suppliers.

The trading could be done using the well-known double action mechanism where users submit their supply or demand bids as well as their asking price to a local authority, which could use this information to determine the winners of the auction (users), the amount of electricity traded at the market as well as the clearance price, and inform the users and their respective suppliers about the outcome of the market. However, is this solution secure and user privacy-friendly? Well-known cryptographic primitives such as encryption and authentication could be used to protect users against curious and malicious third parties, but what about the local authority which would see every user’s bid for every single time period (assuming all users send either supply or demand bid for each time period). Such information could be highly sensitive and reveal various private information about users such as who sells/buys how much electricity at any given time period, who earns most, whose house is empty, who is on holiday, etc. [3].

To address these issues we have proposed a local electricity trading market based on secure MPC [4]. In short, as shown in the Fig. 1, users provide their private inputs in a shared form to a virtualised third party composed of three computational parties (one representing the users, another the suppliers and a third one a local control agency) so that the need for a trusted third party is eliminated, while still guaranteeing security and correctness. Upon reception of the shares, each of the computational parties randomly permutes the users' shares by multiplying them with a beforehand-computed randomized permutation matrix. Then, using the secure comparison and sorting algorithms based on MPC, computational parties jointly compute the clearance price, traded volume, and identify the accepted/rejected bids in a data-oblivious fashion using the shares of the users' bids. Finally, the computational parties open the shares of the market output and send them to the corresponding users and supplier. Then, the users and suppliers, using the received shares, construct their desired outputs. As a result, not a single party learns more than it is supposed to learn. Moreover, none of the computational parties learn anything about the market output.

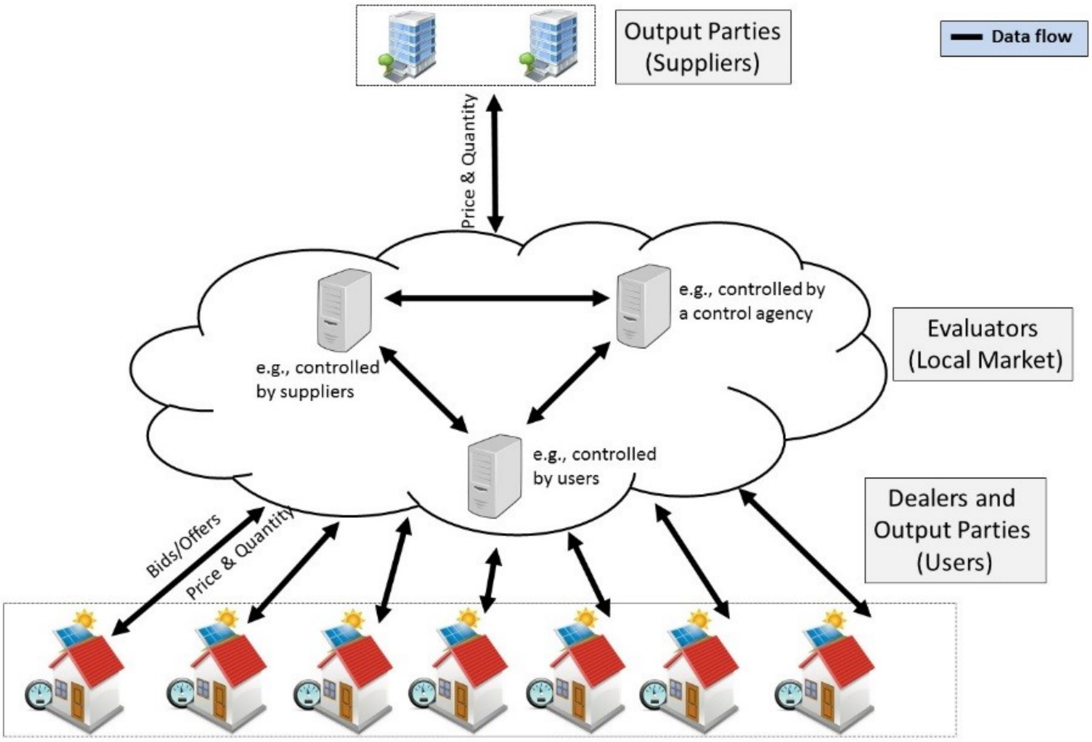
Output Parties (Suppliers)
Data flow
Price & Quantity
e.g., controlled by a control agency
Evaluators (Local Market)
e.g., controlled by suppliers
e.g., controlled by users
Dealers and Output Parties (Users)
Bids/Offers
Price & Quantity

Figure 1: A privacy-preserving local market based on MPC for trading electricity.

Furthermore, we have implemented the proposed market in C++ and tested its performance with realistic data sets [5]. Our simulation results show that the market tasks can be performed for 2500 bids in less than five minutes in the online phase, showing its feasibility for a typical electricity trading period, e.g., 30 minutes.

Future work would include designing a users/suppliers billing system based on the private volumes of the locally traded electricity, as well as incorporating personalised rewards and electrical network fee reductions into the billing system, without violating users' privacy.

[1] Farhangi, H., "The path of the smart grid," *IEEE Power and Energy Magazine,* 8(1) (2010) 18-28 [2] Legal sources on renewable energy, http://www.res-legal.eu/search-by-

country/ [3] Mustafa, M.A., Cleemput, S., Abidin, A., “A local electricity trading market: Security analysis,” In *IEEE PES ISGT-Europe*, 2016 [4] Abidin, A., Aly, A., Cleemput, S., Mustafa, M.A., “Towards a local electricity trading market based on secure multiparty computation,” *COSIC internal report*, http://securewww.esat.kuleuven.be/cosic/publications/article-2664.pdf, 2016 [5] Abidin, A., Aly, A., Cleemput, S., Mustafa, M.A., “An MPC-based Privacy-Preserving Protocol for a Local Electricity Trading Market,” In *Cryptology ePrint Archive*, Report 2016/797. http://eprint.iacr.org/2016/797, 2016

Thanks to Mustafa A. Mustafa for writing this blog post.