PRIVACY PRESERVING AND COLLUSION RESISTANT ENERGY SHARING

Yuan Hong, Han Wang, Shangyu Xie, Bingyu Liu

Department of Computer Science
Illinois Institute of Technology
10 W 31st Street, Chicago, IL 60616
yuan.hong@iit.edu
{hwang185, sxie14, bliu40}@hawk.iit.edu

ABSTRACT

Energy has been increasingly generated or collected by different entities on the power grid (e.g., universities, hospitals and households) via solar panels, wind turbines or local generators in the past decade. With local energy, such electricity consumers can be considered as "microgrids" which can simultaneously generate and consume energy. Some microgrids may have excessive energy that can be shared to other power consumers on the grid. To this end, all the entities have to share their local private information (e.g., their local demand, local supply and power quality data) to each other or a third-party to find and implement the optimal energy sharing solution. However, such process is constrained by privacy concerns raised by the microgrids. In this paper, we propose a privacy preserving scheme for all the microgrids which can securely implement their energy sharing against both semi-honest and colluding adversaries. The proposed approach includes two secure communication protocols that can ensure quantified privacy leakage and handle collusions.

1. INTRODUCTION

Energy has been increasingly generated or collected by different entities on the power grid (e.g., universities, hospitals and households) via solar panels, wind turbines or local generators in the past decade. With local energy, such electricity consumers can be considered as "microgrids" which can simultaneously generate and consume energy [20, 1]. More recently, the research on cooperation among entities on the power grid (e.g., microgrids) has attracted great interests in both industry and academia [20]. For instance, microgrids can share their local energy to improve the efficiency and resilience of power supply [6].

Specifically, microgrids can transmit their excessive energy to the microgrids close to them. In the cooperation, all the participating microgrids jointly seek an energy transmission assignment that minimizes the global energy loss during transmission. However, to this end, all the microgrids should disclose their local information (e.g., local supply, local demand, and power quality for transmission) to each other or a third party. Then, the data recipient (which is a microgrid or a third party) formulates an optimization problem by denoting the amount of energy transmitted from M_i to M_j as x_{ij} and determining the objective function as well as the constraints.

Disclosing such local information to each other or a third party would compromise the corresponding microgrid's local information. To tackle the privacy concerns, the proposed approach in [6] efficiently transforms the shares of the optimization problem to a privacy-complaint format and enables any party to solve the problem. However, the algorithms in [6] pursue high efficiency but cannot quantify the privacy leakage in the protocol. In this paper, we extend the transformation and optimal solution reconstruction to two secure communication protocols in which privacy leakage can be quantified and bounded. In the meanwhile, we give formal security/privacy analysis for the protocols and identify that our proposed secure communication protocols can prevent additional information leakage against the potential collusion among microgrids while executing the protocols. Finally, we present some experimental results to demonstrate the effectiveness and efficiency of our approach.

2. RELATED WORK

In smart grid infrastructure, privacy concerns were recently raised in the fine-grained smart meter readings, which is frequently reported to the utility [21, 7, 3]. To prevent information leakage in smart metering, three different categories of privacy preserving schemes were proposed in the past few years. The first category of techniques built cryptographic protocols to directly aggregate or analyze such meter readings without sharing the raw data. For instance, Rottondi et al. [19] proposed a privacy preserving infrastructure based on cryptographic primitives to enable utilities and data consumers to collect and aggregate metering data. The second category of techniques obfuscate the meter readings to prevent adversaries from learning the status of the appliances at different times. For instance, Hong et al. [7] defined a pri-

vacy notion to quantitatively bound the information leakage in smart meter readings, and proposed streaming algorithms for converting the readings with guaranteed output utility. Finally, the third category of techniques utilize renewable energy sources like batteries to hide the actual load of different households, which can be found in [17], [22], etc.

Furthermore, energy sharing problem among microgrids [20, 24] has been recently studied – locally generated energy can be shared among homes due to the mismatch between generation harvesting and consumption time in microgrids. Zhu et al. [24] developed an energy sharing approach to determine which homes should share energy, and when to minimize system-wide efficiency loss. Zhu et al. [25] also proposed a secure energy routing approach to renewable energy sharing against security attacks such as spoofed routing signaling and fabricated routing messages. Also, some game theoretical models [20, 16, 2] were proposed to mitigate the risks of self-interested behaviors in the energy sharing/exchange. So far, Hong et al. [6] is the only work that resolves the privacy issues in energy sharing/exchange. The proposed scheme can provide some ad-hoc privacy guarantee based on matrix multiplication. Instead, we extend the approach in [6] to ensure provable security.

3. PRELIMINARIES

In this section, we briefly summarize the problem formulation, transformation and solution reconstruction in [6]. Note that the formulations of three optimization problems in [6] are similar, which can be securely transformed and solved using the same secure communication problem. Thus, we only focus on the basic formulation.

3.1. Problem Formulation

Given n microgrids $M_1, \ldots, M_i$, the demand and supply of M_i at time t is denoted as $D_i(t)$ and $S_i(t)$, respectively. Then, given x_{ij} as the amount of energy transmitted from M_i to M_j, the optimization (LP) problem to minimize the overall energy delivery loss in the sharing is formulated as follows.

$$\min : \sum_{i=1}^{n}\sum_{j=1}^{n}\theta_{ij}x_{ij}$$
$$s.t.\begin{cases}\forall i \in [1,n], \sum_{j=1}^{n}(1-\theta_{ji})x_{ji} - \sum_{j=1}^{n} x_{ij} + S_i(t) \geq D_i(t)\\ \forall i \in [1,n], \sum_{j=1}^{n} x_{ij} \leq S_i(t)\\ \forall i \in [1,n], \forall j \in [1,n], x_{ij} \geq 0\end{cases} \tag{1}$$

where θ_{ij} represents the energy loss rate for transmission between M_i and M_j, which is determined by the distance between them on the power transmission network and the power quality data, such as voltage and current. $D_i(t)$, $S_i(t)$ and θ_{ij} are privately held by microgrid M_i. The general form of Equation 1 can be derived as below:

$$\min \quad \vec{c_1}^T\vec{x_1} + \vec{c_2}^T\vec{x_2} + \cdots + \vec{c_n}^T\vec{x_n}$$
$$s.t.\begin{cases} A_1\vec{x_1} + & \ldots & +A_n\vec{x_n} & \leq & \vec{b_0}\\ B_1\vec{x_1} & & & \leq & \vec{b_1}\\ & \ddots & & \vdots & \vdots\\ & & B_n\vec{x_n} & \leq & \vec{b_n}\end{cases} \tag{2}$$

where $\vec{x_i}$ represents M_i's variables $(x_{i1}, \ldots, x_{in})$, which is privately held by M_i. Matrices/vectors A_i, B_i, $\vec{c_i}^T$ and $\vec{b_i}$ are M_i's private inputs in the LP problem.

3.2. Transformation

The above LP problem is heterogeneously partitioned into n shares – global constraints are co-held by all the parties (vertically partitioned [10, 12, 5]) while each constraint belongs to only one party (horizontally partitioned [8, 13, 11]). To ensure privacy protection in solving and realizing the above problem, a transformation-based approach [6] was proposed:

$$\begin{aligned}\forall i \in [1,n], A_i &\longrightarrow A_iQ_i\\ \forall i \in [1,n], B_i &\longrightarrow B_iQ_i\\ \forall i \in [1,n], \vec{c_i}^T &\longrightarrow \vec{c_i}^TQ_i\\ \forall i \in [1,n], \vec{x_i} &\longrightarrow \vec{y_i}\end{aligned} \tag{3}$$

where each party M_i locally post-multiplies its shares (i.e., A_i, B_i and $\vec{c_i}^T$) in the LP problem by an $n \times n$ random nonnegative monomial matrix Q_i [10] which is privately generated by itself, and variables in the new problem $\forall\vec{y_i}$ correspond to $\forall\vec{x_i}$. Then, $\forall i \in [1,n], A_iQ_i, B_iQ_i, \vec{c_i}^TQ_i$ can be disclosed to other parties.

Note that the righthand side values $\vec{b_0}, \vec{b_1}, \ldots, \vec{b_n}$ are also transformed to random numbers in [6], and we still keep such transformation. Thus, we will focus on the security/privacy improvement on the transformation in Equation 3.

3.3. Reconstruction

In [6], after solving the transformed problem to obtain the optimal solution $\forall\vec{y_i}^*$, the solver (any party or an external party, e.g., the cloud) distributes the solution shares to the corresponding parties. Then, the optimal solution of the original problem $\forall i \in [1,n], \vec{x_i}^*$ can be locally reconstructed as: $\vec{x_i}^* = Q_i\vec{y_i}^*$ [6, 9, 10]. The solver and other parties cannot learn the details of $\vec{x_i}^*$, A_i, B_i since Q_i is unknown to them.

4. EXTENDED TRANSFORMATION

With the transformation in [6], each party's share of problem cannot be learnt by other untrusted parties, even if the transformed shares are disclosed to them. However, the informa-

tion leakage in the communication protocol cannot be quantified. We now extend it to a more secured transformation based on Homomorphic cryptosystem (e.g., Paillier [18]).[1]

4.1. Overview

The basic idea of the extended transformation is described as follows. For any party M_i's shares in the LP problem A_i, B_i and $\vec{c_i}^T$, we let all the parties jointly transform such shares (via Homomorphic Encryption) in sequence – while transforming M_i's shares, party M_j locally generates a new random nonnegative monomial matrix $\forall j \in [1, n], Q_{ij}$, and post-multiplies it to each of the three transformed shares (by the previous party). In case that $j = i$ holds, M_i post-multiplies its own shares by its own matrix Q_{ii}. Similarly, all the parties jointly reconstruct every share of the optimal solution $\vec{y}$ by pre-multiplying their matrices in a reverse order (also via Homomorphic Encryption).

4.2. Extended Secure Transformation

Without loss of generality, we let an external party P (e.g., the cloud) solve the transformed problem. In the extended secure transformation protocol, P generates the public/private key pair (pk, sk), and distributes the public key pk to $M_1, \ldots, M_n$. Since the transformation for A_i, B_i and $\vec{c_i}^T$ are identical [6], we can take A_i as an example to illustrate our secure transformation protocol in Algorithm 1.

Algorithm 1 Extended Secure Transformation

1: **for** $i \in [1, n]$ **do**
2: M_i randomly generates Q_{ii}
3: M_i encrypts A_iQ_{ii} with pk to generate $E = Enc_{pk}(A_iQ_{ii})$, and sends E to the next party M_j in Line 4
4: **for** $\forall j \in [1, n], j \neq i, M_j$ **do**
5: M_j randomly generates Q_{ij}
6: M_j updates E with Q_{ij} (Line 7-9: E_{ab} denotes the entry at row a and column b in E, and $(Q_{ij})_{kb}$ denotes the entry at row k and column b in Q_{ij})
7: **for** each row a of E and each column b of Q_{ij} **do**
8: M_j computes $E_{ab} \leftarrow \prod_{k=1}^{n} E_{ak}^{(Q_{ij})_{kb}}$
9: **end for**
10: M_j sends the updated E to the next party
11: **end for**
12: the last party sends E to the solver P
13: P decrypts E to obtain: $A_iQ_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}$
14: **end for**

After decrypting all the ciphertexts, solver P can formulate a new LP problem with the transformed shares:

$$\forall i \in [1, n], A_i \longrightarrow A_iQ_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}$$
$$\forall i \in [1, n], B_i \longrightarrow B_iQ_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}$$
$$\forall i \in [1, n], \vec{c_i}^T \longrightarrow \vec{c_i}^T Q_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}$$
$$\forall i \in [1, n], \vec{x_i} \longrightarrow \vec{y_i} \quad (4)$$

Then, P can solve the new LP problem and distribute the solution share $\vec{y_i}^*$ to M_i, which securely reconstructs its solution share in the original problem with all the other parties.

4.3. Secure Reconstruction

Following the proof in [6, 10], the optimal solution in the original problem $\forall i \in [1, n], \vec{x_i}^*$ can be reconstructed as below:

$$\forall i \in [1, n], \vec{x_i}^* = Q_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}\vec{y_i}^* \quad (5)$$

As a result, all the parties $M_1, \ldots, M_n$ should jointly reconstruct each solution share. Then, we present the secure communication protocol for the optimal solution reconstruction in Algorithm 2.

Algorithm 2 Secure Reconstruction

1: **for** $i \in [1, n]$ **do**
2: M_i generates a public/private key pair (pk_i, sk_i) and sends the public key pk_i to all the other parties $M_1, \ldots, M_n$
3: M_i encrypts $\vec{y_i}^*$ with pk_i to generate $Y = Enc_{pk}(\vec{y_i}^*)$, and sends Y to the next party M_j in Line 4
4: **for** $\forall j \in [n, 1], j \neq i, M_j$ **do**
5: M_j updates Y with Q_{ij} (Line 6-8: Y_a denotes the ath entry in Y)
6: **for** each row a of Q_{ij} **do**
7: M_j computes $Y_a \leftarrow \prod_{k=1}^{n} Y_k^{(Q_{ij})_{ak}}$
8: **end for**
9: M_j sends the updated Y to the next party
10: **end for**
11: the last party sends Y to M_i
12: M_i decrypts Y to obtain: $\prod_{j=1,j\neq i}^{n} Q_{ij}\vec{y_i}^*$
13: M_i reconstructs its share in the original optimal solution $\vec{x_i}^* = Q_{ii}\prod_{j=1,j\neq i}^{n} Q_{ij}\vec{y_i}^*$ (pre-multiplying by Q_{ii})
14: **end for**

Finally, in the optimal energy sharing, each party M_i can locally route the energy amount $x_{ij}^* \in \vec{x_i}^*$ to the recipient M_j (note that $x_{ij} = 0$ if $i = j$ holds).

4.4. Privacy Preservation and Collusion Resistance

Privacy. We now analyze the privacy leakage of the two protocols. For both extended secure transformation and secure

[1] Homomorphic cryptosystem is a semantically-secure public key encryption with an additional property to generate the ciphertext of an arithemetic operation between two plaintexts by other operations between their individual ciphertexts. For instance, two encryptions $E(A)$ and $E(B)$, there exists operations *, such that $E(A * B) = E(A) * E(B)$ where * is either addition or multiplication (in some abelian group).

reconstruction, there is no privacy leakage while executing the protocol under the definition of secure multiparty computation [23, 4] (all the messages received by all the parties can be simulated in polynomial time by repeating the protocols). Therefore, private inputs (e.g., demand, supply, and power quality of each party) can be protected.

On the other hand, the information leakage in the outputs can be quantified:

- The solver only learns the transformed optimization problem (the obfuscated shares of each party and the corresponding optimal solution).
- Each party only knows its share in the optimal solution, e.g., how much energy transmitted from itself to the energy recipient in the global optimal sharing.

Handling Collusions. The two protocols can also effectively handle potential collusions (on learning private information) while solving the problem. None of those parties knows the actual overall transformation (aka. a combination of transformations), since each of $\{\forall i, \forall j, Q_{ij}\}$ is privately generated as a random nonnegative monomial matrix by M_j (for transforming M_i's shares). As a consequence, the solution reconstruction cannot be completed if any party M_j is absent (missing $\forall i, M_{ij}$). Therefore, any number of microgrids (less than n) cannot collude with each other to infer private information from other honest microgrids while executing the protocol. The collusion resistant feature provided by the two protocols is equivalent to a trusted-third party.

5. EXPERIMENTS

We have estimated the performance of our protocols using two different key length (512/1024-bit) and varying number of parties (20 to 500). [2] The computational costs of two protocols are plotted in Figure 1. To significantly improve the security/privacy, the protocols take longer time compare to [6], and such computational costs are still tolerable with a polynomially increasing trend as the number of parties increases.

In addition, we present the communication overheads of the two protocols per party in Table 1. As the number of parties increase, the average bandwidth consumption (size of the transmitted messages) of the extended secure communication protocol and secure reconstruction protocol also grow polynomially. Therefore, the two protocols can be implemented in most of the current networking environment.

6. CONCLUSION AND FUTURE WORK

In this paper, we have extended the secure transformation and solution reconstruction in [6] to ensure provable security for solving the energy sharing optimization problem and implementing the optimal solution on the power grid. Novel secure communication protocols were proposed for all the parties to jointly transform their individual shares of the optimization problem, and jointly reconstruct their own shares in the optimal solution of the original problem. In the meanwhile, collusions can be handled with the secure communication protocols. In case that some parties disclose information to each other so as to learn other parties' private information, they cannot learn the actual transformation and reconstruction as long as at least one party is not colluding with them.

In the future, we will investigate other privacy preserving cooperative models among entities with local energy (viz. microgrids) on the power grid. For instance, global and local load balancing can be manipulated and further optimized via the cooperation among microgrids (e.g., scheduling [14, 15]). We intend to propose a privacy preserving cooperative model for them to jointly improve the global and local performance of the power generation, supply, storage and consumption.

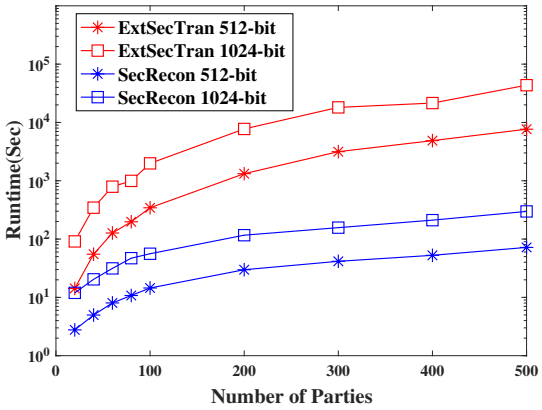

Fig. 1. Computational Costs

Table 1. Communication Overheads

Number of Parties	ExtSecTransform	SecReconstruction
20	0.00904 MB	0.0004 MB
40	0.0761 MB	0.0019 MB
60	0.261 MB	0.0045 MB
80	0.624 MB	0.0078 MB
100	1.23 MB	0.014 MB
200	9.96 MB	0.051 MB
300	33.5 MB	0.112 MB
400	79.6 MB	0.119 MB
500	155.6 MB	0.312 MB

Acknowledgments

This work is partially supported by the National Science Foundation under Grants No. CNS-1618221/1745894.

[2] We are currently implementing the simulation system for the main grid and numerous microgrids by integrating communication and power distribution networks, and will evaluate our proposed protocols in the system soon.

7. REFERENCES

[1] P. Arboleya, C. Gonzalez-Moran, M. Coto, M. C. Falvo, L. Martirano, D. Sbordone, I. Bertini, and B. D. Pietra. Efficient energy management in smart microgrids: ZERO grid impact buildings. *IEEE Trans. Smart Grid*, 6(2):1055–1063, 2015.

[2] R. Duan and G. Deconinck. Multi-agent coordination in market environment for future electricity infrastructure based on microgrids. In *SMC*, pages 3959–3964, 2009.

[3] S. Goel and Y. Hong. Security challenges in smart grid implementation. *SpringerBriefs in Cybersecurity*, pages 1–39, 2015.

[4] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game - a completeness theorem for protocols with honest majority. In *Proceedings of the 19th ACM Symposium on the Theory of Computing*, pages 218–229, New York, NY, 1987. ACM.

[5] Y. Hong. *Privacy-preserving Collaborative Optimization*. PhD thesis, Rutgers University, Newark, NJ, 2013.

[6] Y. Hong, S. Goel, and W. M. Liu. An efficient and privacy-preserving scheme for p2p energy exchange among smart microgrids. *International Journal of Energy Research*, 40(3):313–331, 2016.

[7] Y. Hong, W. M. Liu, and L. Wang. Privacy preserving smart meter streaming against information leakage of appliance status. *IEEE Trans. Information Forensics and Security*, 12(9):2227–2241, 2017.

[8] Y. Hong and J. Vaidya. An inference-proof approach to privacy-preserving horizontally partitioned linear programs. *Optimization Letters*, 8(1):267–277, 2014.

[9] Y. Hong, J. Vaidya, and H. Lu. Efficient distributed linear programming with limited disclosure. In *DBSec*, pages 170–185, 2011.

[10] Y. Hong, J. Vaidya, and H. Lu. Secure and efficient distributed linear programming. *Journal of Computer Security*, 20(5):583–634, 2012.

[11] Y. Hong, J. Vaidya, H. Lu, P. Karras, and S. Goel. Collaborative search log sanitization: Toward differential privacy and boosted utility. *IEEE Trans. Dependable Sec. Comput.*, 12(5):504–518, 2015.

[12] Y. Hong, J. Vaidya, H. Lu, and L. Wang. Collaboratively solving the traveling salesman problem with limited disclosure. In *DBSec*, pages 179–194, 2014.

[13] Y. Hong, J. Vaidya, and S. Wang. A survey of privacy-aware supply chain collaboration: From theory to applications. *Journal of Information Systems*, 28(1):243–268, 2014.

[14] Y. Hong, S. Wang, and Z. Huang. Efficient energy consumption scheduling: Towards effective load leveling. *Energies*, 10(1), 2017.

[15] F. Liu, S. Wang, Y. Hong, and X. Yue. On the robust and stable flowshop scheduling under stochastic and dynamic disruptions. *IEEE Transactions on Engineering Management*, PP(99):1–15, 2017.

[16] I. Maity and S. Rao. Simulation and pricing mechanism analysis of a solar-powered electrical microgrid. *IEEE Systems Journal*, 4(3):275–284, 2010.

[17] S. E. McLaughlin, P. McDaniel, and W. Aiello. Protecting consumer privacy from electric load monitoring. In *ACM Conference on Computer and Communications Security*, pages 87–98, 2011.

[18] P. Paillier. Public key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - Eurocrypt '99 Proceedings, LNCS 1592*, pages 223–238, 1999.

[19] C. Rottondi, G. Verticale, and A. Capone. Privacy-preserving smart metering with multiple data consumers. *Computer Networks*, 57(7):1699–1713, 2013.

[20] W. Saad, Z. Han, H. V. Poor, and T. Basar. Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications. *IEEE Signal Process. Mag.*, 29(5):86–105, 2012.

[21] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor. Smart meter privacy: A theoretical framework. *IEEE Trans. Smart Grid*, 4(2):837–846, 2013.

[22] W. Yang, N. Li, Y. Qi, W. H. Qardaji, S. E. McLaughlin, and P. McDaniel. Minimizing private data disclosures in the smart grid. In *ACM Conference on Computer and Communications Security*, pages 415–427, 2012.

[23] A. C. Yao. How to generate and exchange secrets. In *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, pages 162–167, Los Alamitos, CA, USA, 1986. IEEE, IEEE Computer Society.

[24] T. Zhu, Z. Huang, A. Sharma, J. Su, D. E. Irwin, A. K. Mishra, D. S. Menasché, and P. J. Shenoy. Sharing renewable energy in smart microgrids. In *ACM/IEEE 4th International Conference on Cyber-Physical Systems*, pages 219–228, 2013.

[25] T. Zhu, S. Xiao, Y. Ping, D. Towsley, and W. Gong. A secure energy routing mechanism for sharing renewable energy in smart microgrid. In *SmartGridComm*, pages 143–148, 2011.