Privacy Preserving Smart Metering System Based Retail Level Electricity Market

Cory Thoma, Tao Cui, *Student Member, IEEE,* Franz Franchetti, *Member, IEEE*

***Abstract*—Smart metering systems in distribution networks provide near real-time, two-way information exchange between end users and utilities, enabling many advanced smart grid technologies. However, the fine grained real-time data as well as the various market functionalities also pose great risks to customer privacy. In this work we propose a secure multi-party computation (SMC) based privacy preserving smart metering system. Using the proposed SMC protocol, a utility is able to perform advanced market based demand management algorithms without knowing the actual values of private end user consumption and configuration data. Using homomorphic encryption, billing is secure and verifiable. We implemented a demonstration system that includes a graphical user interface and simulates real-world network communication of the proposed SMC-enabled smart meters. The demonstration shows the feasibility of our proposed privacy preserving protocol for advanced smart grid technologies which includes load management and retail level electricity market support.**

***Index Terms*—Cyber security, privacy preserving, retail electricity market, secure multiparty computation, smart metering.**

I. Introduction

Smart meter systems utilize two way communication enabling utilities to receive end user consumption data and send pricing or control signals back to end user at a near real time rate (i.e. 15 mins) [1]. The smart meter system can give network operators a much better view of the system state and allows for much better grid management. In addition, demand can be managed through variable energy pricing and market mechanisms to steer customers into behaviors good for the system. Having detailed customer profiles and the ability to steer customers with price signals provides ways to differentiate services and charge a premium for certain quality of service levels. Thus, the massive investment into smart meter infrastructure would be beneficial for the grid operator and the utilities. Smart meter systems have become an important enabling component for various smart grid technologies including real time pricing, demand response, etc.

However, the only participant without a strong benefit from smart meters is the customer. The effect of smart meter deployment is that the rates may become much more complicated, and the customers may have to change his/her behavior to acclimate to the grid, all the while the actual saving on his/her monthly bill is very limited. Most important, the installation of smart meters opens the door to detailed customer profiles to the utility and other parties. Researchers have shown that fine grained power consumption data at smart meter sampling rate can be used to extract detailed information on user activities [2] [3] [4] [5]. Moreover, most smart meter-based market functionalities require end user to submit sensitive information such as planned demand, usage preferences, responses to prices, etc. which may directly relate to user's private activities and life styles [6]. Given such a situation it is understandable that customers have no favorable view of smart meters and view them highly intrusive. Therefore, we believe that making privacy a first-class citizen in the smart meter development is absolutely necessary to increase customer acceptance and to achieve its ultimate success.

C. Thoma is with the Department of Computer Science, University of Pittsburgh, PA, USA. email: cmt69@pitt.edu. T. Cui and F. Franchetti are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. e-mail: {tcui,franzf}@ece.cmu.edu

Related work. In order to address the privacy issue, several privacy preserving smart metering schemes have been proposed. Based on homomorphic encryption techniques, a privacy friendly energy metering system has been proposed in [7]. A secured protocol for billing computation is presented in [8]. An approach to securely aggregate neighborhood data has been proposed in [9]. An anonymization process using a trusted third party to remove the user's identity is proposed in [10]. Another solution for future smart grid household uses batteries and other energy storage devices to make the load signature undetectable [11]. A Trust-Platform-Module based architecture aggregating the data of a user group over a certain time period is proposed in [2].

However, most of the previous works still target the traditional usage of smart meters for metering and billing purpose, without taking advanced smart grid applications such as real time load management and market functionalities into consideration. Some methods mathematically or physically obfuscate the real time data which unnecessarily sacrifices the data resolution and limits the usability of the smart meter data. Some methods lack a verifiable mechanism, or may still need a trusted third party. On the other hand, various proposed smart meter based load management methods such as real time pricing, retail level electricity market can have more complicated market or control algorithms and require very detailed user consumption or configuration data [6], which make the privacy preserving an even more difficult task.

In order to fully enable the advantages of smart meter system and address its privacy concern, we believe an ideal privacy preserving protocol should meet the following requirements: 1) fully protect the user's privacy, 2) without sacrificing the data for actual smart grid applications, 3) has a verification mechanism, and 4) without using a third party.

Contribution. In this work, we build upon our previous work in [12], we propose a secure multiparty computation based privacy preserving framework for more advanced smart metering system applications including real time pricing, retail level marketing, and verifiable billing. Secure multiparty computation (SMC) is a computation framework which enables

multiple parties to secretly compute some joint function value using a secured protocol without revealing the private data to anyone. Built upon several SMC primitives, more complicated function can be constructed and evaluated within SMC framework and satisfying the above ideal privacy requirement. We take the smart grid retail level electricity market in [6] as an example and implemented an SMC based privacy preserving retail level electricity market. We further developed a demonstration system which includes a graphical user interface and runs on the campus network. The demonstration shows the feasibility of the proposed scheme on commodity IT systems.

Synopsis. This paper is organized as follows: the concepts of SMC are reviewed in Section II. An SMC based retail level electricity market is detailed in Section III. The demonstration is described in Section IV. Section V concludes the paper.

II. Secure Multiparty Computation

In this section, we review the concept of secure multiparty computation (SMC). We also show some SMC related properties and primitives that can be used to build the proposed privacy preserving framework.

A. Secure Multiparty Computation

Secure multi-party computation (SMC) is a cryptographic problem in which multiple parties jointly compute a value based on individually held private data, without sharing the data. The concept is closely related to the idea of *zero-knowledgeness* used in public key cryptosystems (for instance, RSA) and zero-knowledge authentication (for instance, Feige-Fiat-Shamir Identification Scheme) [13]. Security is often derived from one-way functions like integer multiplication/factorization that is easy in one way (polynomial time algorithm to multiply two prime numbers) but hard to invert (exponential time to find the original integers from the product). Historically, the first example of SMC was the *millionaire problem*: millionaires Alice and Bob are interested in knowing which of them is richer without revealing their actual wealth [14]. A more general formulation of SMC is: for a number of players $P_1, \ldots, P_n$, each has initial inputs $x_1, \ldots, x_n$, and SMC securely computes some function f on these inputs, where $f(x_1, ...x_n) = (y_1, ..., y_n)$. Each player P_i only obtains the output y_i. During the computation process, the actually value of each player P_i's input x_i is kept privately without being revealed to anyone.

B. Homomorphic Encryption and SMC

One standard approach to SMC is homomorphic encryption, which enables direct arithmetic operations on encrypted values. A prominent example is the Paillier cryptosystem [15], [16]. One simple illustrative example would be: Let $n = pq$, and p and q be distinctive prime numbers of sufficient size (1,024–2,048 bits). n is the public key and (p, q) is the private key. Also let $g = n + 1$. To encrypt a value $m \in \mathbb{Z}_m$, select a random value $r \in \mathbb{Z}_m$ and compute $[m] = (mn + 1)r^n = g^m r^n \bmod n^2$. [.] denotes an encrypted value; the public key is usually omitted since it is constant. For encrypted messages $[a]$ and $[b]$, and constants c, one can easily compute $[a+b] = [a][b]$ and $[ca] = [a]^c$. The computation of $[ab]$ usually requires a cryptographic protocol, since the Paillier cryptosystem is not homomorphic with respect to multiplication.

C. SMC Primitive Example: Secure Summation

Secure summation computes the summation of multiple numbers privately held by multiple parties without revealing the actual value to anyone and can be built upon the Paillier cryptosystem. As mentioned above, Paillier is an additive homomorphic cryptosystem. The following steps describe the details of Paillier scheme.

1) **Key generation**: Choose two large prime p and q randomly and independently. Let $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$. Choose random $g \in \mathbb{Z}^*_{n^2}$, ensure n divides the order of g by checking the existence of $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$ where $L(x) = (x-1)/n$. The public key is (n, g). The private key is (λ, μ).
2) **Encryption**: Given the public key (n, g) and a random number $r \in \mathbb{Z}^*_n$. A plaintext M can be encrypted to ciphertext $[M]$, $[M] = g^M \cdot r^n \bmod n^2$. The encryption process is denoted as: $[M] = E(M)$.
3) **Decryption**: Given the public key (n, g) and private key (λ, μ), a ciphertext $[M]$ can be decrypted to plaintext M by $M = L([M]^\lambda \bmod n^2) \cdot \mu \bmod n$. The decryption process is denoted as: $M = D([M])$.

The two homomorphic encryption properties of Paillier cryptosystem can be written as follows.

$$D(E(m_1) \cdot E(m_2) \bmod n^2) = m_1 + m_2 \bmod n. \quad (1)$$

$$D(E(m_1)^k \bmod n^2) = km_1 \bmod n. \quad (2)$$

Based on the additive homomorphic encryption property of Paillier cryptosystem in (1), a *Secure Summation* process to compute the summation of User 1 to User n's private data is described below and showed in Fig. 1.

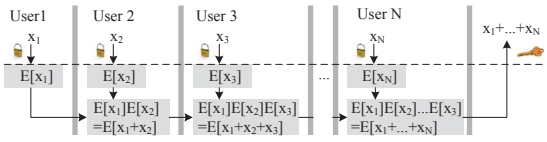


Fig. 1. Steps of Secure Summation, the equations are modulo equations

1) **Set-up**: Using Paillier system, the public key (n, g) is given to all users and the utility. The private key (λ, μ) is only given to utility.
2) **Start**: User 1 encrypts his/her private data x_1 to ciphertext $E[x_1]$, and send $[M_1] = E[x_1]$ to next User 2.
3) **Encrypted Addition**: When User i received message $[M_{i-1}]$ from User $i-1$, User i encrypts his/her private data x_i to $E[x_i]$, and send the new message $[M_i] = E[x_i] \cdot [M_{i-1}] \bmod n^2$ to next User $i+1$.
4) **Stop**: When the message $[M_N]$ from the last User N finally send to the utility. The utility decrypt the message $M_N = D([M_N])$ using the private key.
   Then $M_N = \sum_{i=1}^{n} x_i$.

In this way, the summation can be obtained without knowing the actual value of any user's private data. Therefore, the privacy preserving *secure summation* primitive can be achieved.

D. SMC Software Framework

In general, the theoretical and algorithmic foundations for SMC are well-researched and it has been shown that SMC has the potential to solve hard problems in application areas that require strong privacy. Various approaches based on compilers and domain-specific languages exist: The Fairplay system [17] implements two-party SMC, and the FairplayMP extension [18] implements multiparty SMC. SMCL [19] is a domain-specific language for SMC. One large scale real-world application of SMC was a sugar beet auction system in Denmark [20]. From its definition, SMC framework can not only protects multiple users' privacy, but also enable complicated arithmetic and logic operations. SMC shows great potential in building privacy preserving smart meter systems with advanced smart grid applications.

III. SMC Based Local Electricity Retail Market

In this section, we first introduce an example of retail level electricity market with real time local marginal pricing based on market clearing described in [6]. Based on SMC, we then describe our privacy preserving solution for this type of electricity market which satisfies the proposed ideal privacy preserving requirements in Section I. We also describe a verifiable billing method based on homomorphic encryption.

A. Market Clearing Based Retail Level Electricity Market

The real time price can be determined by the real time demand-supply relations between suppliers and customers using the market clearing price (MCP). MCP is the price at which the quantity supplied is equal to the quantity demanded. The MCP mechanism has been widely used to model and explain various competitive electricity market activities in the wholesale level [21]. Also various forms of real time pricing such as time-of-use price, tiered-price at retail level can be viewed as simplified versions of the demand-supply based MCP. Recently in [6] the real time price based on MCP has been fully implemented into an actual retail level electricity market with real utility and customers involved.

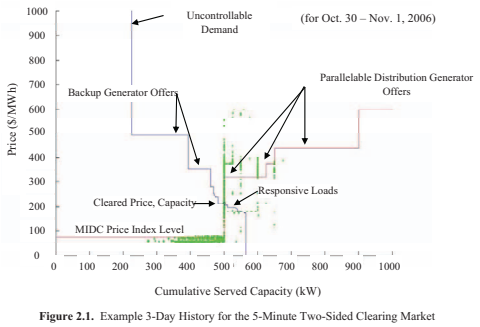


Figure 2.1. Example 3-Day History for the 5-Minute Two-Sided Clearing Market

Fig. 2. Real time market clearing pricing [6]

Fig. 2 from [6] shows a snapshot of MCP based real time pricing. The decreasing demand curve shows for a certain price, how much energy the customers are willing to consume considering uncontrollable demand, customer-owned backup generators, and responsive loads. The increasing supply curve shows for certain amount of energy, at what price the utility is willing to sell, considering the wholesale price and cost of utility owned distribution generators. The intersection of the demand and supply curves determines the MCP. The dots on Fig. 2 shows the historical MCP points at the interval of every 5 minutes during a 3-day operation.

B. SMC Based Privacy Preserving Design

Market clearing computation. In order to compute the MCP, each producer and each customer defines a cost function that describes for each price level the amount of energy the participant would sell or buy. In practice, a k-dimensional vector (p_j) of possible prices is agreed upon in advance by the m participants. For each market clearing interval, participant i defines a k-dimensional supply vector (s_j^i) stating the amount of energy he or she would sell at price p_j and a k-dimensional demand vector (d_j^i) stating the amount of energy he or she would buy at price p_j. Consumers such as end users would set up various cost functions in advance, depending on their needs of energy throughout the day. Producers such as the utility and users who own distributed generation compute their current supply function based on the wholesale electricity price and the cost functions of operating their distributed generators.

During the market clearing process, The MCP for the next interval is computed as follows. Each participant has his/her own demand curve and/or supply curve defined as above. Based on all individual curves, for each price, the total supply or demand curve in the market can be computed by aggregating all individual supply of demand curve. For growing supply curve and decreasing demand curve with increasing price, there is a price where total supply equals total demand which is the market equilibrium point, and the price is the MCP. Mathematically, one can compute for each price $j = 1, \ldots, k$ the total supply and demand:

$$s_j = \sum_{i=1}^{m} s_j^i \quad \text{and} \quad d_j = \sum_{i=1}^{m} d_j^i, \tag{3}$$

and finds the market clearing index ℓ for which $s_\ell = d_\ell$, and the corresponding MCP p_ℓ. The actual MCP may be between two p_i since we use vectors and not continuous functions. Based on the index ℓ, participant i get the right to consume d_ℓ^i kWh and/or to sell d_ℓ^i kWh at price p_ℓ.

SMC algorithm. The MCP computation among multiple participants can be decomposed into two parts: *Summation* among multi-party to compute the total demand and supply curves in (3), and comparison of the total supply and demand curve to find the intersection point and obtain the MCP. As introduced in Section II, the SMC primitive: *Secure Summation* can be the main building block of our proposed privacy preserving market. In this market case, the user's individual demand or supply curve comprise the critical private data that needs to be kept private. Therefore, the algorithm and structure is shown as in following Fig 3:

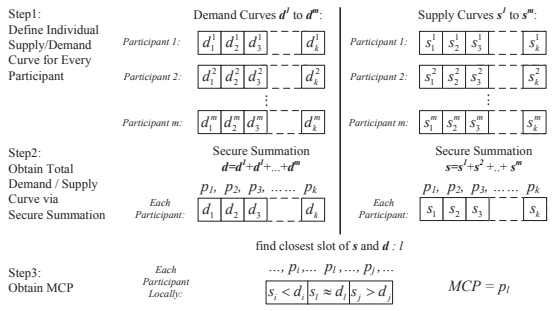


Fig. 3. Secure market clearing process

In Fig. 3, step 1, each participant can be both consumer and producer, with his/her own demand and supply curves. All the curves are defined on a mutually agreed price grid p_1 to p_k. In step 2, all participants together compute the total demand curve and total supply curve using *secure summation*. Every participant obtains the total demand curve and total supply curve after the secure summation. The *secure summation* guarantees that these two total curves are obtained without revealing any individual demand or supply information to anyone. In step 3, the total demand curve and total supply curve are compared on the price grid to find the slot ℓ where $s_\ell = d_\ell$ or where the comparison result change from $s_{\ell-1} < d_{\ell-1}$ to $s_\ell > d_\ell$. Then ℓ is the intersection of the demand and supply curves and $MCP = p_\ell$. Since every participant has the total demand and supply curves, the MCP can be obtained locally without revealing market information to anyone, and without using a trusted third party. In practice, finding the ℓ can be done via binary search. Also, since the total demand and supply curves have already removed individual participant's identity, these two curves can also be used in public for verification purpose.

Remarks. In our paper, the main purpose to use this MCP based retail level electricity market model is to demonstrate that even for such complicated market mechanism, the SMC based privacy preserving approach can be fully integrated to fully protect the user's privacy. It demonstrates the potential feasibility of SMC for privacy preserving in various other smart meter-based demand response systems.

C. Billing and Verification

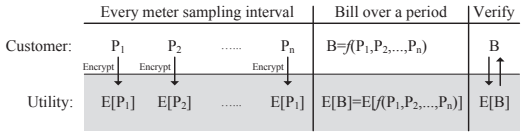


Fig. 4. Steps of verifiable bill

The billing and verification is achieved by *homomorphic encryption*. In (1) and (2) we can see the Paillier cryptosystem allows secure computation of the dot-product of a encrypted usage vector with its corresponding price vector. Therefore the encrypted bill can be computed without knowing the actual value of usage. The billing process is showed in Fig. 4. The customer locally calculates his/her own bill in plaintext using real-time consumption P_i and corresponding price in each time slot i. The customer also sends his/her encrypted real-time consumption $E[P_i]$ to utility. The utility computes the bill using these encrypted consumption data in each time slot. At the end of each billing period, the utility will have an encrypted bill $E[B]$ and the user will have plaintext bill B. Then, both utility and user will be able to verify whether the bill is correct or not by check if $E[B]$ matches B. e.g. The end user send his/her own unencrypted bill B to the utility and the utility encrypts it with the public key and compares the result to the recorded encrypted values $E[B]$.

IV. System Implementation

We have implemented the proposed SMC based privacy preserving retail electricity market load management as a proof-of-concept demonstration.

A. Network

The network structure consists of smart meters and the SMC servers. The network topology of the proposed privacy preserving load management is shown in Fig. 5. There are two structures for different security primitives:

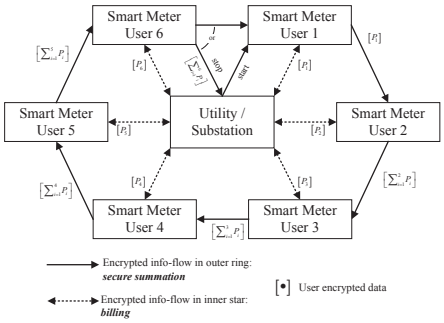


Fig. 5. Network structure

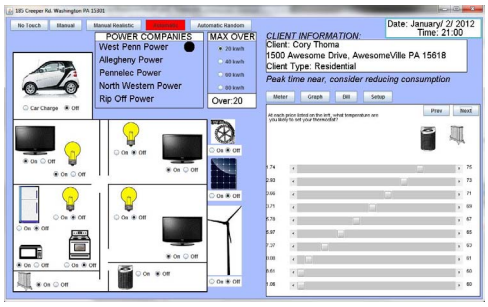
1) The outer ring structure is used for *secure summation*. It is a re-arrange of Fig. 1. Note in Fig. 5, all data in [.] are locally encrypted by each user. The P_i could be a scalar (real time consumption) or a vector (demand/supply curve).

2) The inner star structure used for *billing* and other information flow between individual user and utility.

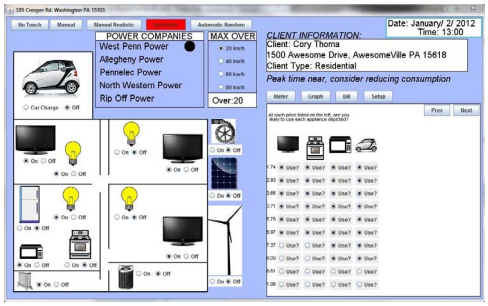
B. User interface

Fig. 6 shows the user control panel to set different price responses for different appliances. Fig. 6(a) shows price response setting for the appliance that has continuous (or multi-stage) working status such as a thermostat: at a certain price, what room temperature should be set. Fig. 6(b) shows price response setting for appliance with only on/off working status: at what price, certain appliance is allowed to be turned on. From the user's multiple responsive appliance settings, the user's demand curve can be obtained.

The total demand curve and supply curve of all users and utility can be obtained by our proposed SMC protocol. The utility and all users have the same total supply and demand curves locally to obtain the MCP as shown in Fig. 7. In this example, both curves are plotted in the market display as shown in Fig. 7. The intersection of demand and supply curves determines the real time price for next time interval.



(a) Continuous setting according to price. e.g. thermostat



(b) On/Off setting according to price

Fig. 6. User control panels for different price responsive appliances

Fig. 7. Market display: price by demand and supply curves

C. Hardware and Software Platform

The demonstration is implemented as a Java program running on multiple laptops with Core 2 CPU. The computational power necessary for the simulation shows that an embedded system in a smart meter could meet the performance requirements for a real-world deployment of the proposed approach.

V. Conclusion

In this work, we propose a secure multi-party computation (SMC) based privacy preserving smart metering system. Using proposed protocol, the utility is able to monitor and manage real time demand without knowing the end user's private consumption data. More advanced smart grid technologies such as real time pricing and retail electricity market can also be enabled without any privacy issues. Using homomorphic encryption, the billing is secure and verifiable. We have further implemented a demonstration system which include a graphical user interface and simulates the real-world network communications of the smart meters. The demonstration shows the feasibility of the proposed privacy preserving protocol for various smart grid technologies including load management and retail level electricity market.

Acknowledgments

The authors acknowledge the support of the Smart Grid Research Center, under the Energy Research Initiative of Semiconductor Research Corporation and the support from National Science Foundation through award 0931978.

References

[1] "Assessment of Demand Response and Advanced Metering," Federal Energy Regulatory Commission, Tech. Rep., 2008.

[2] S. Wicker and R. Thomas, "A privacy-aware architecture for demand response systems," *Hawaii International Conference on System Sciences*, 2011.

[3] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, New York, NY, USA: ACM, 2010, pp. 61–66.

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

[5] Y. Kim, T. Schmid, Z. Charbiwala, and M. Srivastava, "ViridiScope: design and implementation of a fine grained power monitoring system for homes," in *Proceedings of the 11th international conference on Ubiquitous computing*. ACM, 2009, pp. 245–254.

[6] D. Hammerstrom, R. Ambrosio, T. Carlon, J. DeSteese, G. Horst, P. N. N. L. (US), and U. S. D. of Energy, *Pacific Northwest GridWise Testbed Demonstration Projects: Olympic Peninsula Project*. Pacific Northwest National Laboratory, 2007.

[7] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *In 6th Workshop on Security and Trust Management (STM 2010)*, ser. Lecture Notes in Computer Science, J. C. et al., Ed. Springer Verlag, 2010.

[8] A. Rial and G. Danezis, "Privacy-preserving smart metering," Microsoft technical report MSR-TR-2010-150, Tech. Rep., 2010.

[9] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010.

[10] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010.

[11] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010.

[12] C. Thoma, T. Cui, and F. Franchetti, "Secure multiparty computation based privacy preserving smart metering system," in *North American Power Symposium (NAPS), 2012*. IEEE, 2012, pp. 1–6.

[13] L. C. Washington and W. Trappe, *Introduction to Cryptography: With Coding Theory*: Prentice Hall PTR, 2002.

[14] A. C. Yao, "Protocols for secure computations," in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1982, pp. 160–164.

[15] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *EUROCRYPT*, 1999, pp. 223–238.

[16] M. Franz, B. Deiseroth, K. Hamacher, S. Jha, S. Katzenbeisser, and H. Schroeder, "Secure computations on non-integer values," Cryptology ePrint Archive, Report 2010/499, 2010.

[17] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, "Fairplay—a secure two-party computation system," in *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. Berkeley, CA, USA: USENIX Association, 2004, pp. 20–20. [Online]. Available: http://portal.acm.org/citation.cfm?id=1251375.1251395

[18] A. Ben-David, N. Nisan, and B. Pinkas, "Fairplaymp: a system for secure multi-party computation," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2008, pp. 257–266.

[19] J. D. Nielsen and M. I. Schwartzbach, "A domain-specific programming language for secure multiparty computation," in *Proceedings of the 2007 workshop on Programming languages and analysis for security*, ser. PLAS '07. New York, NY, USA: ACM, 2007, pp. 21–30.

[20] P. Bogetoft, D. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. Nielsen, J. Nielsen, K. Nielsen, J. Pagter *et al.*, "Secure multiparty computation goes live," *Financial Cryptography and Data Security*, pp. 325–343, 2009.

[21] D. Kirschen and G. Strbac, *Fundamentals of Power System Economics*. Wiley, 2004.