Privacy Enhanced Personal Services for Smart Grids *

Zeki Erkin
Cyber Security Group
Department of Intelligent Systems
Delft University of Technology
Mekelweg 4, 2628CD, Delft, The Netherlands
Z.Erkin@tudelft.nl

Thijs Veugen
TNO Technical Sciences
2600 GB, Delft, The Netherlands
Thijs.Veugen@tno.nl

ABSTRACT

Millions of people are now increasingly using smart devices at home to improve the quality of their lives. Unfortunately, the smart devices that we use at home for comfort and simplicity make our lives more complicated in terms of management due to several issues like mismatching interfaces and complexity of the micro-management. One approach to manage smart homes is to enable the utility provider, which has direct access to electrical devices via smart meters. It is expected that the data collected for the management can also be utilized for other personalized services using other business partners. In this paper, we address these personalized services and argue that privacy is a serious consideration for the deployment of the new business ideas. We provide a scientific method to provide new services for smart homes while protecting the privacy-sensitive data. To the best of our knowledge, privacy enhanced new services based on the utilization of smart meter data have not been considered by the research community.

Categories and Subject Descriptors

K.4.1 [**Public Privacy Issues**]: Privacy

Keywords

Smart energy grid, privacy, cryptography, secret sharing, performance.

1. INTRODUCTION

One of the key advantages of smart grids is efficiency in term of the automation of services like remote maintenance, billing, load balancing, network monitoring and data analysis. This progress has been possible due to a setting where utility providers (UPs) install smart meters in households to measure user consumption in intervals ranging from hours to seconds [1]. The collected fine-granular meter readings are not only necessary for such grid operations but also very rich in terms of contained information. Daily activities of inhabitants can be monitored using non-intrusive appliance load monitoring (NALM), and even habits can be inferred in the long term [3]. This rich source of information can be utilized further to create new business cases like customized smart home management and personalized services. Use of smart meters will boost the economy in several ways [4].

Unfortunately, such use of smart-meter data is hindered throughout Europe due to privacy concerns, since it is possible to identify, monitor and track people based on their smart meter readings. Such privacy considerations led the Dutch parliament to decide in 2009 that smart-meter installation is possible only by consent. Nevertheless, the smart meter deployment is expected to reach 80% by 2020 in Europe. Therefore, it is pressing to address privacy considerations in a scientific manner. Without privacy solutions, the capabilities of the smart metering devices and new services offered by the UPs can be misunderstood by the society and hamper the developments in a big industry.

In this paper, we envision that there are multiple business partners (BPs) that are involved in commercial activities with the UP, which generates more business opportunities for all partners. The smart-meter readings collected by the UP are processed, and a profile for each customer is created using registration data and NALM. Typical profile data consist of customers demographic information, age and gender of the residents, the type and number of devices that could be detected using NALM, and usage statistics of these devices. In an informal way, we describe the profile in two parts: 1) personal information, and 2) identified devices with their power consumptions per time unit. In our vision, this profile will be shared with different BPs, which can use them for generating services for the households. For example, an ICT company can suggest to manage the smart devices by offering suggestions like turning on (or off) devices per time unit; another company can analyse the usage statistics and determine the efficiency of the devices and suggest to replace some of them with special offers. The type of services that can be built on such smart-meter data is limitless and is not the aim of this paper to identify such use cases. However, our argument is that such *personalized* services will be employable in the near future and there is a strong privacy consideration in each and every one of them. We present a scientific approach to protect the privacy-sensitive data without hampering such new business cases.

*This work is supported by the Dutch COMMIT programme.

We argue that companies offering personalized services have to take proper security and privacy precautions as directed by laws and regulations (e.g. European Data Protection Directive). However, it is also important for the companies to consider these issues from the user's perspective, since any business that cannot convince the users in terms of privacy is subject to fail, as has been seen in the case of Dutch ING Bank planning to sell customer data [5].

Considering that there is legal agreement between the user and the UP, we assume that the raw data collected from the smart meters are secured using well-known techniques like encrypted databases, access-control mechanisms and physical security measures. However, it is unlikely for the UP and the users to accept giving away raw data in plain text to the BPs. Therefore, we present a cryptographic approach in which personalized services can be performed by BPs without accessing the raw or profile data of the users. In particular, BPs are supposed to perform their services on the encrypted profiles.

The approach of processing encrypted data has been used before in several domains including biometric data matching [6], medical healthcare [7], social networks [8] and data mining [9]. It relies on cryptographic protocols that are built using tools like fully/somewhat homomorphic encryption (FHE/SHE) [10], secret sharing [11] and garbled circuits [12], to compute a function with private data. Within the context of smart grids, cryptography has been considered but so far only for data aggregation and billing. Bohli et al. [13] and Wang et al. [14] applied data perturbation for live monitoring by adding random noise to raw meter readings. Acs̀ et al. [15] and Lin et al. [16] added Laplacian noise to the smart meter readings and applied additive blinding to conceal them. For data aggregation, solutions based on secret sharing [17] and homomorphic encryption [18] have been proposed. Billing protocols that delegate the computation to the users are presented in [19].

Generating recommendations based on user data have been investigated in depth as a vital tool in e-commerce. The privacy aspects of recommender systems, particularly those using collaborative filtering techniques, consequently triggered research efforts in the past years [20]. Polat and Du [21] suggested hiding the personal data statistically. Shokri et al. [22] presented a recommender system that is built on distributed aggregation of user profiles, containing a trade-off between privacy and accuracy. McSherry and Mironov [23] proposed a method using differential privacy, which has a similar trade-off between accuracy and privacy. Cissée and Albayrak [24] presented an agent system where trusted software and secure environment are required. Atallah et al. [25] proposed privacy-preserving collaborative forecasting and benchmarking to increase the reliability of local forecasts and data correlations using cryptographic techniques. Erkin et al. [26] also proposed protocols based on cryptographic techniques, which are computationally more efficient than their counterparts.

There are initial works to hide the consumption data from the UP for protecting the the privacy of users' daily activities using a cooperative state estimation technique [27] and a third party escrow mechanism for authenticated anonymous meter readings which are difficult to associate with a particular smart meter or customer [28]. However, to the best our knowledge, generating personalized recommendations based on smart metering data have not been addressed before, let alone their privacy aspects. Therefore, in this paper we lay out a path for a new research field with some initial ideas.

The rest of the paper is structured as follows. We present the recommendation system as a personalized service and the required privacy tools in Section 2. We describe the privacy enhanced recommender system in detail in Section 3. We present the details about the implementation in Section 4. We analyse our proposal in terms of complexity and security in Section 5. We also discuss some ideas and future work in this new research domain in that section. Finally, we draw conclusions in Section 6.

2. PERSONALIZED SERVICES AND TOOLS FOR PRIVACY

2.1 Personalized Services

The number and the type of personalized services built on smart metering data is a subject for creating new business cases. We assume that using NALM and registration data, a UP creates a profile that contains information on the number of devices like TVs, oven, fridge, light bulbs, electrical car, heating pump, and so on. Note that these device usage profiles can also be generated locally and submitted to the UP, given that smart meters have resources and can also communicate with smart devices using protocols like ZigBee within the household. Each device $\mathcal{D}$ has its own energy consumption data. We assume there are n users, and their energy consumption is measured during m time intervals. So for each device we have usage data $C_{\mathcal{D}}(i, j)$, an integer value representing the energy consumption by device $\mathcal{D}$ of user i, $1 \leq i \leq n$, during time interval j, $1 \leq j \leq m$.

Based on these usage data, we envision three main scenarios where a BP generates a personalized service for a single household:

1. Based on the usage data of a set of devices, the BP finds out similar other households in the system (in the same neighborhood, district or city). Then, the BP provides usage statistics of those similar households, for example to improve the energy usage since it is shown in [29] that this information is sufficient to increase the energy efficiency by 15%. These clustered households can later be used for generating recommendations.
2. The BP can also monitor all of the devices in the household, and remotely manage the devices more efficiently. For example, during the different weather conditions, the heating systems and the fridge can be controlled and based on the usage patterns, the washing machine can be programmed, and the electrical car can be charged.
3. Using a binary decision tree, the BP determines whether a certain device satisfies a set of requirements. For example, whether the TV is energy efficient or not. Based on the device characteristics and usage information, the decision tree suggests services and/or new devices with better energy consumption.

Due to space issues, we provide in this paper a privacy-preserving solution for the first scenario only, in which similar households are found and recommendations are generated. In all of the above scenarios, we assume that the BP (or different BPs in each scenario) is directly linked to every household via some communication channel. The profile data are privacy-sensitive and subject to protection. Therefore, all functions should be realized on *obscured* data of the household with the help of the UP. Anonymization techniques will not be sufficient, as the goal for the households is to get personalized services. There can be cases where the UP is not trusted either. However, we leave this more sophisticated setting for future work.

2.2 Tools for Privacy

Before we describe the tools we use for designing our protocol, it is worth mentioning our security assumptions. We assume that everyone is motivated to use this system and therefore follows the protocol description. However, they are also curious to extract more information than they are entitled to by storing past messages. This assumption is known as the honest-but-curious model. We also assume that communication between parties are secured using traditional mechanisms.

For our application scenario of finding similar households and generating recommendations based on the device profile data, we use additive secret-sharing [11], where the consumption data is split by the user into two secret shares. One share is sent to the BP, and the other is given to the UP. The BP and UP, who jointly hold secret sharings of the consumption data, can compute any function on these shares, in our case finding similar households, comparison and generating averages. In additive sharing, addition of shares can be done locally, while multiplication requires preparation of some computations, and interaction by the two parties.

Secret sharing is preferable to public-key cryptography, because the numbers involved are much smaller, which leads to reduced computational and communication complexities. This has, for example, been shown in a recent comparative study by Blom on implementations of the secure comparison protocol [30].

Let p be a prime, large enough to incorporate all input, intermediate, and output values, as jointly computed and accumulated by the BP and the UP. All values are presented as elements of the field $\mathbb{F}_p$, which informally means that we are computing modulo p. By $[x]$ we denote a secret-sharing of a value $x \in \mathbb{F}_p$, which means that BP has a value $x_{BP} \in \mathbb{F}_p$, UP has a value $x_{UP} \in \mathbb{F}_p$, and both add up to $x = (x_{BP} + x_{UP}) \bmod p$. Although UP and BP know their share, they learn nothing about the secret value x.

In the following, we show how two secret-shared values can be multiplied, the multiplication result being again secret-shared. Let $[x]$ and $[y]$ be sharings of secret values $x, y \in \mathbb{F}_p$. Assume that sharings $[a], [b]$ and $[c]$ have been computed in advance for secret random values $a, b, c \in \mathbb{F}_p$ such that $a \cdot b = c \bmod p$. Then, BP and UP engage in the following protocol:

1. BP and UP locally compute $[e] = [x] - [a]$, and open $e = (x - a) \bmod p$.
2. BP and UP locally compute $[d] = [y] - [b]$, and open $d = (y - b) \bmod p$.
3. BP and UP locally compute $[z] = [c] + d[a] + e[b] + de$, which satisfies $z = xy \bmod p$ because $xy = (a + e)(b + d) = (c + ad + eb + de) \bmod p$.

Opening a secret-shared value means that BP and UP send each other their share, and locally compute the secret value by adding the two shares. A secret-shared value is multiplied by a known constant by locally multiplying each share with this constant. Only when the constant is secret-shared, the above multiplication protocol has to be executed.

3. PRIVACY ENHANCED PERSONALIZED SERVICES

In this section, we present a privacy enhanced version of a recommender system for smart grids. Based on the energy consumption data per user per device, a recommendation is computed as follows:

1. UP and BP compute all necessary multiplication triplets.
2. All users upload the power consumption data of their devices to the UP and the BP using additive sharing.
3. UP and BP compute the similarity values in terms of energy consumption, of all users with respect to user A.
4. UP and BP choose the users most similar to user A, by comparing the similarity values with a certain threshold.
5. UP and BP compute the average usage of these similar users, and give it to user A as a recommendation.

All computations are done on secret-shared values, so UP and BP do not learn private power consumption data. We now describe each of these steps in more detail.

3.1 Computing multiplication triplets

All necessary multiplication triplets have to be (pre)computed jointly by UP and BP, one for each multiplication. This could be achieved by using any additively homomorphic encryption system such as Paillier [31], denoted by $[\![.]\!]$, which has the property that $[\![x]\!] \cdot [\![y]\!] = [\![x + y]\!] \bmod N^2$, where $x, y \in \mathbb{Z}_N$. We assume the BP holds the private decryption key. The following protocol generates a shared triplet $([a], [b], [c])$ of random values such that $c = (a \cdot b) \bmod p$.

1. BP generates random $a_{BP}, b_{BP} \in \mathbb{Z}_p$, encrypts them, and sends $[\![a_{BP}]\!]$ and $[\![b_{BP}]\!]$ to UP.
2. UP generates random $a_{UP}, b_{UP} \in \mathbb{Z}_p$, chooses a large random number r, computes $[\![a_{BP} \cdot b_{UP} + b_{BP} \cdot a_{UP} + r]\!] = [\![a_{BP}]\!]^{b_{UP}} \cdot [\![b_{BP}]\!]^{a_{UP}} \cdot [\![r]\!] \bmod N^2$, and sends it to the BP.
3. BP decrypts it, and computes its share $c_{BP} = (a_{BP} \cdot b_{BP} + (a_{BP} \cdot b_{UP} + b_{BP} \cdot a_{UP} + r)) \bmod p$.
4. UP computes its share $c_{UP} = (a_{UP} \cdot b_{UP} - r) \bmod p$.

The random value r should be large enough such that the value $a_{BP} \cdot b_{UP} + b_{BP} \cdot a_{UP}$, obtained by BP, is additively blinded. Since p is much smaller than the Paillier modulus N, this will not lead to a carry-over in step 2. Correctness of the multiplication triplet is easily verified: $c_{BP} + c_{UP} =$

$(a_{BP} + a_{UP})(b_{BP} + b_{UP}) \bmod p$. Since the multiplication triplets are data independent, they could be precomputed at any moment that suits both UP and BP.

3.2 Uploading shares

User i uploads the energy consumption of all his devices to the UP and the BP as follows. Given integer $x = C_{\mathcal{D}}(i, j)$, for a certain device $\mathcal{D}$ and time period j, user i generates a random number r_x in $\mathbb{F}_p$, and sends each party one of the shares r_x and $(x - r_x) \bmod p$.

3.3 Computing similarity scores

The similarity values could be computed in various ways, see also Section 5. As an example, we compute similarity based on the energy consumption of a specific subset D of devices, distributed over different time periods.

So for each user i and time period j, BP and UP locally compute the secret-shared consumption data $[s_{ij}] = \sum_{\mathcal{D} \in D} [C_{\mathcal{D}}(i, j)]$, and consequently the similarity score with user A

$$[\mathrm{Sim}(A, i)] = \sum_{j=1}^{m} [s_{Aj}] \cdot [s_{ij}].$$

This computation involves m executions of the secure multiplication protocol, and $m - 1$ local additions of shares. At the end, UP and BP will have the shared similarity scores $[\mathrm{Sim}(A, i)]$, for all users i other than A. Although the similarity scores can be computed for all users, the most similar households will be the households that actually own (at least some of) the devices from D, so households that contain neither of them can be discarded beforehand.

3.4 Finding the most similar households

In this step, UP and BP compare each similarity score with a certain public threshold. This comparison protocol outputs a secret-shared binary value $[\delta_i]$, which is one if $\mathrm{Sim}(A, i)$ is larger than the threshold, and zero, otherwise. Any secure comparison protocol can be used for securely computing the δ_i, e.g. the constant-round protocol of Nishide and Ohta [32], or the linear-round solution by Garay, Schoenmakers and Villegas [33] that uses less secure multiplications. The households that pass the threshold will be considered as 'similar' households. Because BP and UP only hold secret-shared values, they do not know which households actually are similar.

3.5 Generating the recommendation

In this stage, only households that have a similar usage pattern will be considered. Our aim is to show the feasibility of utilizing energy consumption data among similar households in a privacy preserving manner. The actual recommendation could have various forms, see also Section 5. As an example we consider a recommendation to user A, consisting of the energy consumption of a specific device, not in set D, accumulated over all similar households. So user A will learn for example the average energy consumption spent on a TV, given households with a similar (to A) energy consumption on fridge and micro-wave.

The total power consumption of similar households for a certain device $\mathcal{D}$, is computed by $[C_{\mathcal{D}}] = \sum_{i=1}^{n} [\delta_i] \cdot \sum_{j=1}^{m} [C_{\mathcal{D}}(i, j)]$. This will take UP and BP n secure multiplications, and $(m-1)n$ local additions of shares. To obtain an average over all similar users, this value has to be divided by $\sum_{i=1}^{n} [\delta_i]$, the number of similar users. An example of a secure integer division protocol based on long tail division, is presented by Paul Bunn and Rafael Ostrovsky [9].

The average energy consumption of device $\mathcal{D}$ over all similar users is opened to user A, by sending A both shares, which can be added modulo p. User A could divide this integer by m to get an impression of the average consumption per time period.

4. IMPLEMENTATION

Suppose we would implement the privacy-preserving smart grid system based on secret sharing, as described earlier. As an example we suggest time intervals of one hour, and cumulative energy consumption per day for computing similarities, so $m = 24$. Because we chose [33] for securely comparing similarity values with the threshold, it's important that we choose a prime p larger than twice the maximal similarity value to reduce the computational effort [32]. For each device, the energy consumption per time unit can be scaled to an arbitrary integer. Suppose the energy consumption per device per hour, $C_{\mathcal{D}}(i, j)$, is expressed by an integer of maximal size 55, which is sufficient for generating sufficiently discriminating similarity values [34]. When the subset D of devices contains not more than 10 elements, then the maximal size of a similarity value, $\mathrm{Sim}(A, i)$, would be $m \cdot (55 \cdot 10)^2 = 7260000 < 2^{23}$. When we choose a prime p of 25 bits, we are assured that $\mathrm{Sim}(A, i) < p/2$ for each i.

To get an idea of its complexity, we used the secure comparison implementation of Blom [30], which is the most complex operation within our system. When using [33] with a 25 bits prime, it took 0.0378 seconds, and 1.4 KB of communication to perform one secure comparison. The pre-computation effort for this secure comparison, which includes generating the triplets, came at 0.5322 seconds, and 60.78KB of communication. Since we need to perform one secure comparison per user, this results in 6 minutes and 14 MB of data transfer for the online phase with $10,000$ as the overall complexity.

Security of the system depends on the cryptographic tools used. Secret sharing and homomorphic encryption are proven secure under certain assumptions. Therefore, we consider the formal security proof unnecessary for the purpose of this paper. It is important, however, to note that the input and the output of our protocol does not hamper the privacy of the users. As long as the UP and BP do not collude, the shared data is safe: it is impossible for one party to learn the original data. As the output of the protocol is also shared, including the intermediate values like comparison results, the protocol is secure.

It is only left to discuss about the practicality of our proposal. As our aim is to show the feasibility of smart metering data utilization in a privacy preserving manner, we do believe that the protocol presented achieves this goal: similar usage patterns can be found and based on this information, different business cases can be created. The most importantly, this can be achieved in a privacy preserving manner.

Note that processing smart metering data to analyse device usages, creating profiles, suggesting new devices, and even managing smart devices by sending control signals are possible to be realized. The cryptographic tools such as secret sharing and homomorphic encryption seem to be very useful to realize such function however, efficiency of cryptographic protocols heavily depends on a number of factors, namely business model, application scenario, the complexity of the functions and the time interval to compute the function. While it is promising to use cryptography for privacy protection, it is still a challenge to deploy cryptographic tools for functions that has to be performed *almost* in real time such as load balancing.

5. DISCUSSION

In the previous section we presented a privacy preserving way of offering new services to users based on their energy consumption. All users upload detailed energy consumption of their devices, which enables UP and BP to compute various values that are worthwhile to individual users. As an example we showed how a user can obtain the energy consumption of a device averaged over all similar users. The linear secret-sharing system allows all kind of similarity definitions. To determine 'similarity', one could even have all users upload more personal information like the number of household members, or even personal hobbies. The BP could provide recommendation services, give advertisements, warn users about technical failures of devices, etc.

In terms of efficiency, the overall protocol is feasible. Additions in secret-sharing systems are costless compared to multiplications. We only need pre-computation and interaction for multiplying secret-shared values. Creating triplets is the most computationally intensive part of our protocol, which can be precomputed, for example in the idle-time of the UP and the BP. Considering that the numbers in secret-sharing are very small, for example p can be in the order of 25 bits, the overall computation time is considerably less than any counterparts using homomorphic encryption. Techniques based on homomorphic encryption use much larger integers (at least 1024 bits) due to security reasons leading to larger execution times. E.g. the recent recommendation system by Erkin et al [8] needs 50 minutes for computing a recommendation with only 10.000 users, and it does not include the secure integer division (the number of similar users is leaked).

Since UP and BP only compute with secret-shared values, all input, intermediate, and output values remain secret. Only when shares are interchanged, so values are opened, personal information could be revealed. As long as UP and BP do not collude and follow the rules of the protocol, users can be absolutely sure that their personal information is safe. The BP could assist the UP in the accounting of energy delivery. They can jointly compute the total energy consumption for each user, multiply it with the tariffs only the UP knows, and open only the financial costs per period to the UP, so he is able to bill the users and nothing more. On the other hand, the UP can help the BP in delivering new services based on detailed energy consumption of its users, without learning any personal information. Given their opposed incentives, UP and BP are not likely to collude. One could even incorporate a third, privacy preserving authority party, which would be able to control UP and BP, as the secret-sharing system is easily extended to multiple parties.

6. CONCLUSION

Smart grids are essential parts of our future for achieving highly efficient, green and sustainable energy distribution. These networks are also connected to other type of networks consisting of smart devices like TV's, electric cars, and even mobile phones. The intelligence deployed in smart grids opens up new possibilities that were not possible with traditional power networks before.

Unfortunately, highly connected network consisting of numerous type of devices, the need for fine-granular data for network operations and new business cases also have potential security and privacy risks. There are a number of efforts to mitigate security and privacy threats in smart grids, mostly focussing on the essential functions of the grid such as data aggregation. However, there is no research, to the best of our knowledge, on data utilization and its security and privacy aspects in smart grids.

In this paper, we present the idea of personalized services for people based on *readings* data to improve their life quality and reduce their (energy) costs, which is beneficial both for the society and the environment. As we consider the privacy aspects of these new cases the biggest obstacle, we propose a scientific approach based on cryptography. We aim to show that personalized services, while we only present a simple scenario, can be realized in a privacy preserving manner. It is obvious that this new research domain is very new and there are numerous research challenges in terms of efficiency and realistic application settings.

7. REFERENCES

[1] S. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34–41, Sept 2005.

[2] A. Bleicher, "Privacy on the smart grid," IEEE Spectrum, 2010, http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

[3] R. Anderson and S. Fuloria, "On the security economics of electricity metering," in *The 9th Workshop on the Economics of Information Security*, 2010.

[4] NA, "The executive summary of the smartregions project," http://www.smartregions.net/default.asp?SivuID=26875.

[5] C. Hensen, "AFM waarschuwt ING voor gebruik van klantgegevens," http://www.nrc.nl/nieuws/2014/03/14/afm-waarschuwt-ing-voor-gebruik-van-klantgegevens/, March 14 2014.

[6] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in *European Symposium on Research in Computer Security*, Leuven, Belgium, September 2011.

[7] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ecg classification with branching programs and neural networks," *IEEE Transactions on Information Forensics and Security*,

vol. 6, no. 2, pp. 452–468, 2011.

[8] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1053–1066, 2012.

[9] P. Bunn and R. Ostrovsky, "Secure two-party k-means clustering," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM New York, NY, USA, 2007, pp. 486–497.

[10] C. Gentry, S. Halevi, and N. P. Smart, "Fully homomorphic encryption with polylog overhead," in *EUROCRYPT*, 2012, pp. 465–482.

[11] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, November 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[12] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 1987, pp. 218–229.

[13] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, May 2010, pp. 1–5.

[14] S. Wang, L. Cui, J. Que, D.-H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering." *IEEE Trans Smart Grid*, vol. 3, pp. 1317–1324, 2012 Sep 2012.

[15] G. Acs and C. Castelluccia, "I have a DREAM! (Differentially PrivatE smart Metering)," in *Information Hiding Conference*, ser. LNCS. Springer, May 18-20 2011, pp. –.

[16] H.-Y. Lin, W.-G. Tzeng, S.-T. Shen, and B.-S. Lin, "A practical smart metering system supporting privacy preserving billing and load monitoring," in *Applied Cryptography and Network Security*, ser. Lecture Notes in Computer Science, F. Bao, P. Samarati, and J. Zhou, Eds. Springer Berlin Heidelberg, 2012, vol. 7341, pp. 544–560.

[17] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *PETS*, 2011, pp. 175–191.

[18] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *6th Workshop on Security and Trust Management (STM 2010)*, ser. Lecture Notes in Computer Science, J. C. et al., Ed., vol. 6710. Springer Verlag, 2010, pp. 226–238.

[19] G. Danezis, C. Fournet, M. Kohlweiss, and S. Z. Béguelin, "Smart meter aggregation via secret-sharing," in *SEGS@CCS*, 2013, pp. 75–80.

[20] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *SIGMOD '00: Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, vol. 29(2). ACM Press New York, NY, USA, 2000, pp. 439–450.

[21] H. Polat and W. Du, "SVD-based collaborative filtering with privacy," in *SAC '05: Proceedings of the 2005 ACM symposium on Applied computing*. New York, NY, USA: ACM Press, 2005, pp. 791–795.

[22] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J.-P. Hubaux, "Preserving privacy in collaborative filtering through distributed aggregation of offline profiles," in *RecSys '09: Proceedings of the third ACM conference on Recommender systems*. New York, NY, USA: ACM, 2009, pp. 157–164.

[23] F. McSherry and I. Mironov, "Differentially private recommender systems: building privacy into the net," in *KDD '09: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*. New York, NY, USA: ACM, 2009, pp. 627–636.

[24] R. Cissée and S. Albayrak, "An agent-based approach for privacy-preserving recommender systems," in *AAMAS '07: Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems*. New York, NY, USA: ACM, 2007, pp. 1–8.

[25] M. Atallah, M. Bykova, J. Li, K. Frikken, and M. Topkara, "Private collaborative forecasting and benchmarking," in *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. New York, NY, USA: ACM, 2004, pp. 103–114.

[26] D. Kononchuk, Z. Erkin, J. C. A. van der Lubbe, and R. L. Lagendijk, "Privacy-preserving user data oriented services for groups with dynamic participation," in *ESORICS*, 2013, pp. 418–442.

[27] Y. Kim, E. Ngai, and M. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, Oct 2011, pp. 178–183.

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

[29] J. Chinnow, K. Bsufka, A.-D. Schmidt, R. Bye, A. Camtepe, and S. Albayrak, "A simulation framework for smart meter security evaluation," in *Smart Measurements for Future Grids (SMFG), 2011 IEEE International Conference on*, Nov 2011, pp. 1–9.

[30] F. Blom, "A performance evaluation of secure comparison protocols in the two-party semi-honest model," MSc. Thesis VU University Amsterdam, March 2014.

[31] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99*, ser. Lecture Notes in Computer Science, vol. 1592. Springer, 1999, pp. 223–238.

[32] T. Nishide and K. Ohta, "Multiparty computation for interval, equality, and comparison without bit-decomposition protocol," in *PKC 2007*, ser. LNCS, T. Okamoto and X. Wang, Eds., vol. 4450. Springer, 2007, pp. 343–360.

[33] B. S. Juan Garay and J. Villegas, "Practical and secure solutions for integer comparison," in *Public Key Cryptography - PKC'07*, vol. 4450. Springer-Verlag, 2007, pp. 330–342.

[34] F. Ricci, L. Rokach, B. Shapira, and P. Kantor, *Recommender Systems Handbook*. Springer, 2011, iSBN 978-0-387-85820-3.