Wavelet-based Load Profile Representation for Smart Meter Privacy

Dominik Engel
Josef Ressel Center for
User-Centric Smart Grid Privacy, Security and Control
Salzburg University of Applied Sciences
Urstein Sued 1, A–5412 Urstein/Salzburg, Austria
Email: dominik.engel@en-trust.at

***Abstract*—A significant portion of (potential) end-users at this point in time are wary about possible disadvantages of smart grid technologies. A critical issue raised by end-users in various studies is the lack of trust in the level of privacy. Smart metering is the component in the end-user domain around which the most intense debate on privacy revolves, because load profiles are made available at high resolutions. Non-intrusive load monitoring (NILM) techniques allow the analysis of these load profiles to infer user behaviour, such as sleep-wake cycles. We investigate and compare the utility of different variants of the wavelet transform for creating a multi-resolution representation of load profiles. In combination with selective encryption, this multi-resolution representation allows end-users to grant or deny access to different resolutions on a "need-to-know" basis. Access to the different resolutions is thereby only granted to parties holding the needed keys. The whole datastream can be transmitted over the smart grid communications network. The lifting implementation of the wavelet transform has computationally low demands and can be run in embedded environments, e.g. on ARM-based architectures, in acceptable time. The proposed approach is evaluated based on the provided level of security, computational demands and feasibility in an economic sense.**

I. Introduction

The move towards smart grids has spawned a large number of industry initiatives, research programmes and standardization efforts, see e.g. [1] for a current overview. Many of the earlier contributions focused on the smart grid ecosystem at a larger scale, without exploring in detail the ramifications of the move towards smart grid technology for the end-user. More recent programmes increasingly accommodate the user perspective, cf. [1]. Addressing the topic of user acceptance is pointed out as a key issue by almost all authors.

Spreading Smart Grid technologies will be inherently difficult without addressing user concerns and actively managing user acceptance by providing secure methods and demonstrating safety of user data and privacy. Methods for privacy and security will be a critical in establishing end user *trust* and thereby enabling end user participation.

Smart meters form a core component of smart grids. Each of these devices contains a processor, as well as storage and communication facilities and is capable of transmitting detailed load profiles on a daily basis or even in real-time. The exact granularity of the transmitted load profiles is not finally specified, and may differ by country. The intervals between single measurements will lie between a few seconds and 30 minutes.

The availability of data at such fine granularities has raised privacy concerns: Apart from the data needed for regular operation, a number of other information items can be extracted from this data, some of them related to sensitive and personal information on the end user. Especially in the area of individual high resolution load profiles made available by smart meters, severe privacy concerns have been expressed in numerous contributions, e.g. [2]–[6]. In [5] results of a collaboration between researchers from law and engineering are reported. The authors argue that there "exist strong motivations for entities involved in law enforcement, advertising, and criminal enterprises to collect and repurpose power consumption data" [5, p. 1]. For example, burglars could use the data to determine occupancy patterns of houses to time break-ins. Marketing agencies could identify specific brands of appliances used, which could then be used for targeted advertising.

There are a number of approaches for matching appliance signatures to load profiles to determine which appliances were used at what time and for how long, e.g. [7]–[9]. This type of method is termed "non-intrusive load monitoring" (NILM) or "non-intrusive appliance load monitoring" (NALM). Detection based on NILM is remarkably accurate: In [5] over 90% accuracy are reported in detecting presence and sleep cycle intervals. The results show that "personal information can be estimated with a high degree of accuracy, even with relatively unsophisticated hardware and algorithms" [5, p. 2]. The authors of [10] use genetic algorithms for identification and report flawless identification for up to 10 types of appliances. In [11] successful identification of appliances in low resolution load profiles is reported, e.g. 30 minute intervals, with the use of data-mining techniques.

In summary, while there are many useful applications of smart meter data, such as energy saving and tailor-made energy rates, the privacy of this kind of data needs to be secured, even within communication environments secured against unauthorized external access. The authors of [1] make the case for a system in which insiders will access "data in an authorized manner and will only use this data in an *acceptable* manner" [1, p. 8].

In this paper we evaluate wavelet-based multi-resolution representations to secure load profiles and to provide a user-centric privacy approach. In previous work [12], the Haar wavelet was used in a preliminary proof of concept. In this paper, we detail the approach, show that aggregates are preserved and apply the approach in an embedded environment. Furthermore, we investigate the utility of integer-based wavelet filters and compare the filter variants. We provide a detailed evaluation regarding computational demands, and investigate the preservation of aggregates in real-world conditions, as well as the level of security provided and feasibility from an economic perspective.

The rest of this paper is organized as follows: Section II discusses the state of the art as well as prior and related work. The proposed scheme is detailed in Sections III and IV and evaluated in Section V. Section VI summarizes the most important findings and conludes.

II. Related Work

There are two kinds of privacy approaches: regulatory-based and technology-based [1]. An important source for regulatory scenarios and recommendations are the reports of the European Commission Smart Grid Expert Group Two for regulatory recommendations for data safety, data handling and data protection, e.g. [13]. Other sources include Common Criteria for Information Technology Security Evaluation (ISO/EIC 15408) and country-specific recommendations, such as the Federal Office for Information Security (BSI) in Germany, e.g. [14].

In the context of smart grid privacy, there is a number of contributions that deal with technological approaches to end-user privacy in general, for an overview see [15]. In [16] an anonymization scheme that is based on two different resolutions is proposed. This scheme employs a trusted third party escrow service. Two smart meter data sets are generated: One of low frequency that can be used for billing purposes, and one of high frequency that allows further investigation. The authors of [17] propose the anonymization of smart metering readings through the use of aggregation, i.e. high resolution smart meter readings are aggregated at the NAN level and only the aggregate is sent to the utility provider. They introduce two solutions both with and without involvement of trusted third parties. In [18] a scheme that allows to obfuscate smart meter data is proposed that does not affect the performance of overall state estimation. The authors of [19] propose a scheme that trades off interests of utility and users based on lossy source coding. In [20] the use of random sequences in compressed sensing of load profiles to provide privacy and integrity is proposed. The authors of [9] propose a zero-knowledge protocol for privacy enhanced-smart metering. The authors of [21] propose a privacy-preserving protocol for general calculations on meter readings on high resolutions. They use simple cryptography on the meters to certify readings and propose to off-load high-integrity calculations to other user devices. The authors show correctness through cryptographic verification.

Secure transmission of smart meter data is a key topic addressed by many contributions. A security protocol for smart meter aggregation that provides hop-by-hop security, while still providing end-to-end security, is proposed by [22]. In [23], a comprehensive proposal for securing smart grid infrastructure is given, including a proposal for a key infrastructure. The authors of [24] propose a scheme for authentication in the smart grid that is privacy aware. In [25] a secure transport protocol for smart grid data collection in general is presented. The authors of [26] propose a model-based access control system. In [27] a zero-configuration identity-based signcryption scheme for the smart grid is proposed.

Privacy-enabling encryption for smart meter data by the use of homomorphic encryption is suggested by both [28] and [29]. Specifically, a Paillier [30] cryptosystem is used in both contributions, which supports the additive homomorphic property, to enable aggregation of smart meter data in the encrypted domain. The approach suggested by [29] is evaluated in an honest-but-curious adversary model. The system proposed by [31] uses multi-party computation in combination with homomorphic encryption.

The need to deal with multiple resolutions of the available data has been widely acknowledged, e.g. [1], [16]. Furthermore multi-resolution representation can serve to protect privacy while at the same time preserving essential statistics of the underlying data [32]. We have previously proposed the use of the Haar wavelet to create a multi-resolution representation and to use selective encryption to grant conditional access to the individual resolutions on a "need-to-know" principle [12].

III. Multi-resolution Representation of Load Profiles

The basis for both, regulatory-based and technology-based approaches to preserve privacy is detailed knowledge of what information can be extracted with which tools from the available user data. To date, there is little systematic research on this subject in the context of smart grids. In [33] an information theoretic approach to abstract privacy and utility requirements is used. The authors aim at providing a measure for the amount of information leaked, and also for the utility that is retained in the data at different levels of abstraction.

In [9] the information revealed from load profiles at different granularities is investigated. The authors show that with off-the shelf statistical methods detailed information on the behavior of users can be inferred from load profiles without prior knowledge or precomputed appliance signatures. They argue that "the information leaks directly correlate with the time granularity that a meter measures power consumption" [9, p.61] and list a number of privacy-relevant questions that can be answered using load profiles at granularities ranging from hours to seconds.

While a detailed empirical investigation of the exact amount of information that can be extracted from load profiles at each granularity is missing, current results, such as reported by [9], indicate that it is safe to assume an increase in the order of magnitude in detection accuracy each time the number of

available samples for a specific time are doubled. In other words, based on existing investigations it seems that classes of detection accuracy can be based on a resolution increases of powers of two.

A representation of load profiles in different resolutions corresponds to these classes of detecting accuracy. The classical wavelet transformation in the lifting implementation is the ideal tool to create integrated, dyadic multi-resolution representations of load profiles. Each resolution contained in the multi-resolution load profile can be tailored to correspond to a class of detection accuracy. Granting access to third party based on this multi-resolution representation allows informed, privacy-aware data exchange to the user.

A. Wavelet-based Representation

A suitable wavelet transform is applied to the original load profile. This leads to a low frequency and a high frequency band. To obtain a multi-resolution representation of the original signal, the wavelet analysis step is recursively applied to the low pass subband, up to a maximum level m. The low-frequency portion in each step presents the data at a resolution with half the number of samples of the next higher resolution. The resolution level corresponding to the highest decomposition depth m is referred to as R_0, and has a size of 2^{-m} samples.

The synthesis step of the inverse wavelet transform starts with R_0. Each next higher resolution can be obtained by applying the inverse wavelet transform to the low-pass subband (i.e., the lower resolution) and the corresponding high-pass subband. In this way, m further resolutions can be obtained. The resulting subbands are represented in a single bitstream.

To implement multi-resolution analysis in a manner that is suitable for smart metering devices, wavelet lifting [34] is the best approach. This view on the wavelet transform factors wavelet filters into lifting steps, which for many filters rely on simple operations only.

B. Haar Wavelet Filter

The Haar wavelet filter realizes low-pass filtering as averaging of the sample values. The high-pass step is realized by the corresponding differences to allow for lossless reconstruction. Let x_l be the input signal, and s_l and d_l be the low-pass and high-pass output signals, respectively. The lifting steps for the forward transform with the Haar wavelet can be written as follows [34]:

$$s_l^{(0)} = x_{2l} \quad (1)$$

$$d_l^{(0)} = x_{2l+1} \quad (2)$$

$$d_l = d_l^{(0)} - s_l^{(0)} \quad (3)$$

$$s_l = s_l^{(0)} + \frac{1}{2} d_l \quad (4)$$

with the inverse transform written as:

$$s_l^{(0)} = s_l - \frac{1}{2} d_l \quad (5)$$

$$d_l^{(0)} = d_l + s_l^{(0)} \quad (6)$$

$$x_{2l+1} = d_l^{(0)} \quad (7)$$

$$x_{2l} = s_l^{(0)}. \quad (8)$$

The Haar wavelet filter perfectly preserves[1]. the first moment, i.e. the average of the whole sequence is preserved in the lowpass signal with each transformation step:

$$\sum_l x_l = \frac{1}{2} \sum_k s_k. \quad (9)$$

This is an important property as it allows the use of lower resolutions for functions like accurate billing, as the sum of the original sequence can be derived from any of the lower resolutions.

Furthermore, the transformation is lossless, and the aggregation is equivalent to subsampling. In effect, the Haar wavelet in the proposed approach is equivalent to reducing the sampling rate.

C. LeGall $5/3$ Wavelet Filter

The LeGall 5/3 wavelet filter [35] is a biorthogonal wavelet filter, frequently used in image coding. An interesting property of this filter is that its lifting implementation can be realized using integer operations only. With the background of an advanced metering infrastructure with limited computational capacity this can be seen as an advantage.

On the other hand, the LeGall 5/3 filter uses more samples for prediction in the lifting implementation than the Haar wavelet. This may result in longer processing times. Furthermore, and also due to this fact, the LeGall 5/3 filter always requires zero-padding.

The LeGall 5/3 also preserves the first moment. However, due to the necessary border handling, the sum is not perfectly preserved. It depends on the intended application if the loss in accuracy is acceptable. Empirical results on this issue are discussed in Section V.

IV. Conditional Access of Multi-resolution Load Profiles

The idea of conditional access stems from the context of multimedia entertainment data. Entertainment content usually exists in various resolutions (e.g. mobile content, standard definition, high definition), which may be priced differently. A multi-resolution representation of the multimedia data allows the efficient representation of the resolutions in a single bitstream. This is an advantage as only one version of the bitstream needs to be handled and transmitted. Conditional access allows users to pay only for the resolutions they are interesting in. For example, the owner of a standard definition

[1]There may be small discrepancies due to border handling, depending on the length of the input signal. However, this can be resolved by using zero-padding.

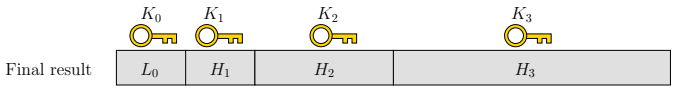

Fig. 1. Final Bitstream Produced by Smart Meter

	$l=1$	$l=2$	$l=3$	$l=4$	$l=5$
Haar	0%	0%	0%	0%	0%
LeGall 5/3	0.44%	1.16%	2.24%	6.26%	11.6%

TABLE I
RELATIVE DIFFERENCE IN AGGREGATION OVER 400 LOAD PROFILES

television has no need to pay for the high-definition version of the content. Through conditional access only the bitstream portion relevant for the desired resolution is decrypted, the rest of the bitstream is ignored.

We propose to use the conditional access paradigm for smart-metering data in multi-resolution representation. Each high-pass subband is encrypted with a different key. If desired, the lowest resolution can remain unencrypted to be accessible for each party, e.g. for billing purposes. The whole datastream can be transmitted over Smart Grid communications infrastructure. Access to the different resolutions is thereby only granted to parties that hold the needed keys, as illustrated by Figure 1.

The lowest resolution remains accessible to the energy provider at all times to enable billing. In the example above this is done by leaving R_0 unencrypted (which in principle mirrors the situation in current energy networks). Alternatively, R_0 could also be encrypted with an appropriate key that allows access to the energy provider.

This scheme allows flexible control by the end-user how access is granted to smart meter data. For example, a particular energy provider may be granted access to the lowest resolution for billing purposes, but the end-user may not be willing to provide any detailed usage statistics. A third-party service providing energy saving advice by employing NILM methods may be granted access to the highest resolution by the user. Thereby, a hierarchical keying scheme (e.g., MIKEy – Multimedia Internet KEYing [36]) needs to be employed, allowing parties who hold K_n to access data encrypted with K_i for $i \leq n$.

The proposed scheme also enables relaying of data. For example, the data needed by a third party analysis lab can be forwarded in encrypted form by an aggregator, or even the utility provider. The parties forwarding the data on route to the destination can only access data in the resolution for which they have been cleared by the owner of the data. This may also mean no access at all, i.e. only forwarding is permitted.

Of course, the proposed scheme requires the smart meter hardware to provide functionality for wavelet lifting and encryption, and to support the manual or automatic setting of encryption keys for the higher resolutions. Furthermore solutions for key management, revocation and a key infrastructure need to be provided.

V. EVALUATION

In the following we evaluate the discussed wavelet filters for use in the proposed approach. We use smart meter data from an Austrian energy provider, which was generated by real households over a period of 18 months. In our tests, we use 400 load profiles. The load profiles originate from Siemens smart meter hardware, model TD3510 (3 phase, 100 Amp.). The sampling interval is 15 minutes, i.e. 96 readings a day. This allows a maximum wavelet decomposition depth of 5. With maximum decomposition, the lowest resolution consists of 3 values per day.

A. Aggregation Preservation

For real-world applicability, the lower resolutions need to be created in a way that preserves the original sum. Both investigated wavelet filters preserve the first moment and the original sum can be derived from wavelet decompositions of arbitrary depth. However, due to the necessary border handling, for the LeGall Filter a loss in accuracy is incurred. Table V-A shows the average relative difference for the sum of the lowpass subband compared to the sum of the original data for the 400 load profiles in the test set for different decomposition levels l.

B. Security

There are no methods to infer the higher resolutions by using the information from lower resolutions. Therefore, the higher resolutions are secure, provided that state-of-the art cryptographic ciphers are used.

The proposed scheme does not prevent tampering of smart meter data at the point of origin, i.e. if a tampered smart meter produces fake data, this is not recognized. To prevent this kind of tampering, the proposed scheme needs to be combined with trusted computing (e.g. [23]).

Regarding successful privacy protection of the higher resolutions, the proposed scheme has an advantage over the scheme proposed by [16]. As stated by [37], the privacy afforded by the scheme proposed by [16] may be compromised by data aggregation through an eavesdropper: The eavesdropper could link the tow IDs for low and high frequency data (LFID and HFID, respectively) by summing up high frequency data that he observes. Such an attack is not possible in the scheme proposed here, as all high frequency data is transmitted in encrypted form.

C. Complexity

As discussed above, implementing the wavelet transform as lifting steps is computationally inexpensive. Generally, the discrete wavelet transform has a complexity of $\mathcal{O}(n)$. Due to the simple operations used in the lifting implementation, the transformation part can be realized by inexpensive smart meter hardware.

The computational demands for encryption depends on the used encryption scheme. For standard encryption schemes,

	WAV	AES	RSA	HYB
Average Execution Time (ms)	0.3092	2.36	89.27	92.12
Standard Deviation	0.0356	0.42	4.92	6.59

TABLE II
EXECUTION TIMES FOR HAAR WAVELET ON A BEAGLEBOARD: AVERAGE FOR 400 LOAD PROFILES WITH 1000 EXECUTIONS EACH

	WAV	AES	RSA	HYB
Average Execution Time (ms)	0.2684	2.34	89.15	91.69
Standard Deviation	0.0495	0.42	3.26	1.53

TABLE III
EXECUTION TIMES FOR LEGALL 5/3 WAVELET ON A BEAGLEBOARD: AVERAGE FOR 400 LOAD PROFILES WITH 1000 EXECUTIONS EACH

efficient implementations exist that can even be integrated into smart meter hardware. Depending on the desired scenario, symmetric encryption alone can be used, or in combination with asymmetric encryption. The latter case is computationally more demanding but benefits from the support for public key infrastructures, such as proposed by [23]. Some overhead is introduced for key management, and potentially for the creation of session keys.

Three scenarios are investigated for each wavelet filter: (i) Symmetric encryption: AES with 128 bit keys, (ii) Asymmetric encryption only: RSA with 2048 bit keys, (iii) Hybrid encryption: 128 bit AES session keys encrypted with 2048 bit RSA keys. In each scenario the following steps are executed: (i) Level 5 wavelet transform of the load profile, (ii) Generation of different keys to encrypt resolutions R_1 through R_5 (R_0 is left unencrypted), (iii) Encryption of R_1 through R_5, each with a different key.

The implementation was done in Java (OpenJDK 1.6). The Java standard implementation of the cryptographic routines were used. Lifting implementations were used for both, the Haar wavelet and the LeGall 5/3 wavelet transforms. No special optimization was performed. The tests were run on an low cost embedded environment (Beagleboard BB-XM-00 with a TI DM3730 ARM processor and 512MB of RAM) running Ubuntu Linux 12.04. An ARM-based environment can be envisioned to be used as the central unit for processing and communication in a AMI Home Area Network or even as part of the smart meter.

Tables II and III show the results for the Haar Wavelet and the LeGall Wavelet, respectively. The timing results are given in milliseconds comparing wavelet transform only (WAV) with AES, pure RSA and hybrid encryption (HYB) using an AES session key encrypted with RSA. In each category, 400 load profiles were investigated, each of which was transformed and encrypted 1000 times. The results present the average time needed for processing one load profile.

It can be seen that compared to the computational demands of the encryption stage, the computational demands for the wavelet transform are almost negligible. On average, the transformation of a load profile takes 0.31 ms for the Haar wavelet and 0.27 ms for the LeGall wavelet. The fact that the LeGall uses integer lifting operations accounts for the slightly faster performance.

As expected, symmetric encryption outperforms asymmetric and hybrid encryption by a factor of nearly 40. In application scenarios, that do not require public key management, this advantage will make symmetric encryption a prime candidate.

Due to the limited size of the subbands, public key cryptography can be used directly on the load data. For our test setup, all subbands can be encrypted using 2048 bit RSA keys. It can be observed that the hybrid approach in our scenario is slower than the pure asymmetric approach. This is due to the fact that the load profile subbands are limited in size. Of course, for larger data sets using pure asymmetric encryption is not feasible and the hybrid approach would have to be used. However, it can be rated an advantage that the multi-resolution representation of the load profiles allows the direct application of public key cryptography.

VI. CONCLUSION

Multi-resolution wavelet representation of smart-meter data is a way to balance the need for privacy with the additional functionality introduced by the smart meter load profiles. By using multiple keys to encrypt each resolution separately, the proposed scheme provides end-user control of access to different granularities of the data. Apart from providing user-centric privacy, due to encrypting the higher resolutions the proposed scheme also implements secure transmission of the load profiles and prevents unauthorized access by eavesdroppers.

In terms of choice of wavelet filter, the Haar filter offers the advantage of preserving the aggregate exactly over the different resolutions, which makes functions like billing possible. The fact that the LeGall 5/3 wavelet offers slightly faster computation cannot counterbalance this advantage.

The scheme fits neatly into the larger frameworks proposed to date, such as [23], as it is compatible with other approaches for securing smart grid communication, including authentication, integrity checking, and the integration into smart grid public key infrastructure.

Regarding computational complexity, some overhead is introduced. However, both employed wavelet transforms have very low demands, when implemented as lifting steps. The computational demands for encryption of the higher resolution subbands are higher, especially if an asymmetric or hybrid approach is chosen.

In terms of economic feasibility, it has been shown that the proposed privacy-aware encryption scheme can be employed on inexpensive ARM-based hardware, even running a non-optimized Java implementation on Linux. In dedicated chipsets that offer hardware acceleration for the cryptographic routines the scheme can easily be integrated into smart meters or the corresponding communication gateways.

ACKNOWLEDGEMENT

The financial support by the Austrian Federal Ministry of Economy, Family and Youth and the Austrian National Foundation for Research, Technology and Development is gratefully acknowledged.

The author would like to thank Salzburg AG for providing extensive test data.

REFERENCES

[1] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Communications Surveys & Tutorials*, vol. PP Issue:99, no. 99, pp. 1–18, 2012.

[2] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network (SSRN)*, Feb. 2009.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009.

[4] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[5] M. A. Lisovich and S. B. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," *IEEE Proceedings on Power Systems*, vol. 1, no. 1, 2008.

[6] M. Lisovich, D. Mulligan, and S. Wicker, "Inferring personal information from demand-response systems," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 11–20, 2010.

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

[8] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy of appliances based on load signatures," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 2, pp. 653–660, 2007.

[9] 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*, ser. BuildSys '10. New York, NY, USA: ACM, 2010, pp. 61–66. [Online]. Available: http://doi.acm.org/10.1145/1878431.1878446

[10] S. K. J. Leung, S. H. K. Ng, and W. M. J. Cheng, "Identifying appliances using load signatures and genetic algorithms," in *Proceedings International Conference on Electrical Engineering (ICEE)*, Hong Kong, Jul. 2007.

[11] G. Kalogridis and S. Z. Denic, "Data mining and privacy of personal behaviour types in smart grid," in *Proc. IEEE 11th Int Data Mining Workshops (ICDMW) Conf*, 2011, pp. 636–642.

[12] D. Engel, "Conditional access smart meter privacy based on multiresolution wavelet analysis," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. New York, NY, USA: ACM, 2011, pp. 45:1–45:5.

[13] European Commission Task Force Smart Grids, Expert Group 2: Regulatory Recommendations for Data Safety, Sata Handling and Data Protection, "Report," http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf, Feb. 2011, online.

[14] Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security), "Protection profile for the gateway of a smart metering system," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf, Aug. 2011, final Draft Version 01.01.01. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf

[15] G. Iachello and J. Hong, "End-user privacy in human-computer interaction," *Found. Trends Hum.-Comput. Interact.*, vol. 1, pp. 1–137, January 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1324103.1324104

[16] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 238–243.

[17] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Proc. IEEE Int Communications Workshops (ICC) Conf*, 2010, pp. 1–5.

[18] Y. Kim, E. C.-H. Ngai, and M. B. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Proc. IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2011, pp. 178–183.

[19] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Proc. IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2011, pp. 220–225.

[20] H. Li, R. Mao, L. Lai, and R. C. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Proc. First IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2010, pp. 114–119.

[21] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on privacy in the electronic society*, ser. WPES '11. New York, NY, USA: ACM, 2011, pp. 49–60. [Online]. Available: http://doi.acm.org/10.1145/2046556.2046564

[22] A. Bartoli, J. Hernández-Serrano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid M2M networks," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 333–338.

[23] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[24] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Pass: Privacy-preserving authentication scheme for smart grid network," in *Proc. IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2011, pp. 196–201.

[25] Y.-J. Kim, V. Kolesnikov, H. Kim, and M. Thottan, "SSTP: A scalable and secure transport protocol for smart grid data collection," in *Proc. IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2011, pp. 161–166.

[26] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Proc. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–7.

[27] H. K.-H. So, S. H. Kwok, E. Y. Lam, and K.-S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 321–326.

[28] F. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Security and Trust Management*, ser. Lecture Notes in Computer Science, J. Cuellar, J. Lopez, G. Barthe, and A. Pretschner, Eds. Springer Berlin / Heidelberg, 2011, vol. 6710, pp. 226–238. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-22444-7_15

[29] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 327–332.

[30] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of Eurocrypt '99, Advances in Cryptology*, ser. Lecture Notes in Computer Science, J. Stern, Ed., vol. 1592. Prague, Czech Republic: Springer, May 1999, pp. 223–238.

[31] C. Thoma, T. Cui, and F. Franchetti, "Secure multiparty computation based privacy preserving smart metering system," in *44th North American Power Symposium (NAPS)*, 2012. to appear.

[32] L. Liu, J. Wang, and J. Zhang, "Wavelet-based data perturbation for simultaneous privacy-preserving and statistics-preserving," in *Proc. IEEE Int. Conf. Data Mining Workshops ICDMW '08*, 2008, pp. 27–35.

[33] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Proc. IEEE Int Smart Grid Communications (SmartGridComm) Conf*, 2011, pp. 190–195.

[34] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *J. Fourier Anal. Appl.*, vol. 4, no. 3, pp. 247–269, 1998.

[35] D. Le Gall and A. Tabatabai, "Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques," in *Proc. Int Acoustics, Speech, and Signal Processing ICASSP-88. Conf*, 1988, pp. 761–764.

[36] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing," RFC 3830 (Proposed Standard), Internet Engineering Task Force, Aug. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3830.txt

[37] T. Baumeister, "Literature review on smart grid cyber security," University of Hawaii at Manoa, Tech. Rep., Dec. 2010.