Received: 16 November 2021 | Revised: 29 April 2022 | Accepted: 3 May 2022

DOI: 10.1002/widm.1469

FOCUS ARTICLE

WIREs DATA MINING AND KNOWLEDGE DISCOVERY WILEY

Privacy protection in smart meters using homomorphic encryption: An overview

Zita Abreu[1] | **Lucas Pereira**[2]

[1]Universidade do Minho, Braga, Portugal

[2]TI, LARSyS, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal

Correspondence
ITI, LARSyS, Instituto Superior Técnico, Universidade de Lisboa, Lisboa 1049-001, Portugal
Email: up202008740@up.pt; lucas.pereira@iti.larsys.pt

Funding information
Fundação para a Ciência e a Tecnologia, Grant/Award Numbers: CEECIND/01179/2017, UIDB/50009/2020; Madeira 14-20, Grant/Award Number: M1420-01-0145-FEDER-000002

Edited by: Witold Pedrycz, Editor-in-Chief

Abstract

This article presents an overview of the literature on privacy protection in smart meters with a particular focus on homomorphic encryption (HE). Firstly, we introduce the concept of smart meters, the context in which they are inserted the main concerns and oppositions inherent to its use. Later, an overview of privacy protection is presented, emphasizing the need to safeguard the privacy of smart-meter users by identifying, describing, and comparing the main approaches that seek to address this problem. Then, two privacy protection approaches based on HE are presented in more detail and additionally we present two possible application scenarios. Finally, the article concludes with a brief overview of the unsolved challenges in HE and the most promising future research directions.

This article is categorized under:

Commercial, Legal, and Ethical Issues > Security and Privacy

KEYWORDS

ElGamal cryptosystem, homomorphic encryption, privacy protection, smart-grid, smart-meter

1 | INTRODUCTION

A smart grid is an electricity grid/network that allows a bidirectional flow of electricity and data whereby smart-metering is often seen as a first step (Agarkar & Agrawal, 2019). A key aspect of the smart grid is that, unlike the traditional grid where consumers are passive actors, in the smart grid they become part of the process (Völker et al., 2021; Wang et al., 2019). This change will have a significant impact on the end-user, affecting their consumption habits and energy management routines. For example, if the end-user is ill-prepared for the changes that will come, it will have a bad impact and an increase in energy costs.

In high-level terms, a smart-grid consists of smart appliances, sensors, control systems, wireless communication devices, gateways, and smart meters (SMs). Information about electricity consumption from the SM is collected and accumulated at the gateways nodes. The data from a number of gateways are then put together in the so-called aggregator nodes, which are then made available to a control center. A high-level illustration of the smart grid is provided in Figure 1.

SMs are a cornerstone to the smart-grid realization since without them it is not possible to have accurate and timely (often near real-time) information on the energy flows (Zheng et al., 2013). In fact, in the traditional grid, energy metering is only possible for billing purposes since only the total consumption (in kWh) is measured (Snap Energy Latino, 2019).

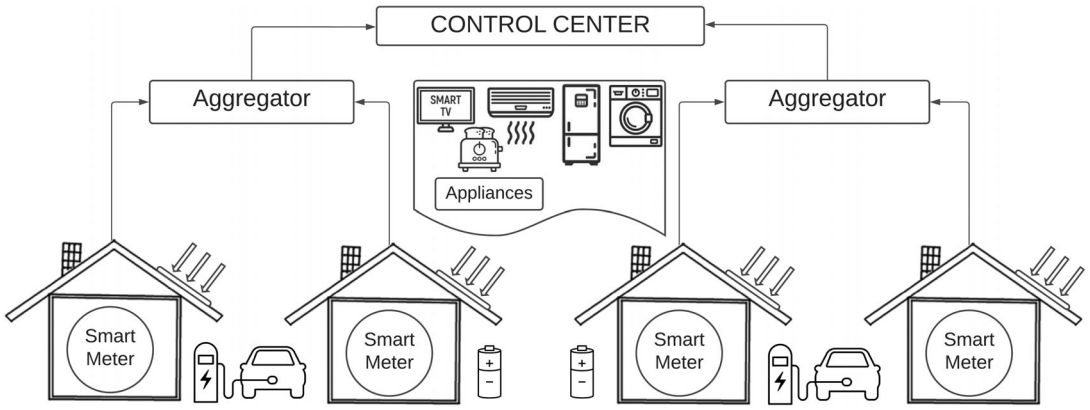

FIGURE 1 A simplified overview of a smart grid network

While the concept of a smart grid is about a decade old, the first smart-metering devices date back to 1972. Back then, Ted Paraskevakos created a system for digital monitoring. This system was intended for security, fire, and medical alarm systems, but was also able of reading utility meters. After receiving a US patent for this, in 1974, he created the company that was responsible for the first commercially available fully automated remote meter reading and load management system.

Ironically, despite their central role in the smart grid, SMs are the source of major concerns such as the proposition of value, public health, cyber-security, and user privacy (Hess & Coley, 2014).

The proposition of value refers to the extent SMs actually deliver the expected benefits. For example, having access to real-time consumption information is expected to lead to reductions in the energy bills (Zheng et al., 2013). However, the findings regarding the effectiveness of such solutions to date are not unanimous (Mogles et al., 2017), which may cause user resistance to smart-metering deployments.

Public health concerns are related to the belief that radio frequency emissions from wireless SMs are harmful to humans (Jeff Evans, 2012; Hess & Coley, 2014). Despite scientifically unfounded, (Exponent Inc., 2014; Richmond et al., 2011), this shows that the smart-grid infrastructure is not yet well understood (Jeff Evans, 2012).

As for cyber-security, SMs when not properly commissioned and installed can become vulnerable to cyber-attacks that can lead to power outages and network overloads (Anderson & Fuloria, 2010; Hahn & Govindarasu, 2011; Wang & Lu, 2013). Against this background, the National Institute of Standards and Technology (NIST) has developed a series of guidelines for smart-grid security (NIST, 2014). An extensive review of standards and technical countermeasures for smart grid cyber-attacks can be found in Hussain et al. (2018).

Regarding privacy, the main concerns are inherent to the possibility of inferring behavioral patterns from energy consumption data. Using electric load signature analysis tools such as non-intrusive load monitoring (NILM; Pereira & Nunes, 2018) that disaggregate the total consumption into individual devices, it is possible to have an attacker that can infer personal information about users, for example, if there are occupants in the house at a given time; whether the inhabitants maintain regular work schedules or daily routines; if they often go on vacation; have lunch or dinner regularly outside the home (Jin et al., 2017; Rubio et al., 2017). To make matters worse, the fact that occupancy alone is highly correlated with simple statistical metrics like average consumption and energy range, it is easier for an attacker to work even without very sophisticated algorithms (Barbosa, Brito, & Almeida, 2016).

The main ambition of this article is to present an overview of existing techniques to enhance the privacy of SM data, with a particular focus on homomorphic cryptography. In more detail, the contributions consist of a review of homomorphic cryptography, especially focused on ElGamal cryptosystem; the presentation of a possible proposal for efficient homomorphic smart measurement; the presentation of two application scenarios and the discussion of future directions with respect to cryptographic systems speaking briefly of the impact of quantum computing.

This article is organized as follows: Section 2 provides a concise overview of the literature in privacy protection techniques for SM data; Section 3 presents a detailed description of privacy protection techniques based on homomorphic cryptography; Section 4 presents two possible application scenarios of homomorphic cryptography in SMs; and Section 5 presents a discussion on the main challenges and future opportunities in HC and the conclusion.

2 | SMART METERS: PRIVACY PROTECTION OVERVIEW

Given the privacy exposure problem, it is necessary to build efficient infrastructures that adopt strategies that ensure the nondisclosure of private information. Overall, existing methods to mitigate privacy issues with SM data can be divided into two broad categories: changing the energy consumption profile (CEP) or changing the smart-meter data (CMD). Ultimately, all the techniques under these two categories attempt to minimize the loss of privacy by decreasing the chance of inferring sensitive information from the energy consumption data, for example, the consumption of individual appliances using NILM (Zhang et al., 2020).

2.1 | Change energy profile

As the name suggests, approaches under this category aim at changing the load demand profiles such that sensitive information cannot be inferred from SM data measurements (e.g., active power). There are three main approaches under the CEP category: (1) *battery energy storage systems (BESS)*, for example, (Farokhi & Sandberg, 2018; Sun et al., 2015; Zhang et al., 2017); (2) *renewable energy systems (RES)*, for example, (Giaconi, Gündüz, & Poor, 2018; Gündüz & Gómez-Vilardebó, 2013; Reinhardt et al., 2015; Tan et al., 2013); and (3) *flexible loads (FL)*, for example, (Baker & Garifi, 2018; Chen et al., 2015; Chin et al., 2021; Egarter et al., 2014).

Strategies based on *battery energy storage systems* tackle the issue of privacy protection by charging and discharging the storage device such that the SM data does not reveal any specific pattern about the residents. More precisely, whenever the house consumption exceeds a value that represents the level of stable and constant power consumption, the storage device is drained to provide the additional power to the house rather than pulling it from the grid. Similarly, when the house consumption is below the target value the battery is charged from the grid. Ideally, this process makes demand flat and equal to a target value, thereby hiding any patterns that can reveal user presence and/or absence (Chen et al., 2015). This strategy is also known as battery-based load hiding (BLH). The main drawback is privacy prevention schemes based on this approach is that they are always limited by battery capacity (kWh) and inverter size (kW). Furthermore, the battery charging and discharging may conflict with the users' economic interests, and lead to quicker degradation of the storage device.

Approaches based on *renewable energy sources* change the energy profile by controlling the output of local generation technologies such as solar photo-voltaic systems (solar PV). This can be done in several ways, but ultimately the objective is to either simulate or hide the presence of loads (e.g., [Reinhardt et al., 2015]). The former can be achieved by lowering the renewable generation such that the demand from the grid increases hence simulating an appliance activation. In contrast, the latter can be achieved by increasing the renewable generation output when specific appliances are in use. By increasing the generation, the demand from the grid will decrease, thus hiding the load consumption. Like with the approaches based on BESS, privacy protection strategies that rely on RES are also limited by the size of the renewable production facilities. For example, in the case of solar PV, this approach is limited by production capacity (kWp), and inverter size (kW). Likewise, the automatic control of the production units may conflict with the economic interests of the owners, for example, increasing the payback time if constantly producing below the rated capacity.

Contrasting the two previous alternatives, approaches based on *flexible loads* do not require the acquisition of additional hardware. Instead, they rely on flexible appliances, that is, appliances that can be used with different power levels or whose usage can be shifted in time. Privacy with flexible loads can be achieved in two main forms. First, by consuming energy demand, for example, turning the water heater ON, to simulate or hide the presence of appliances. Second, by shifting load usage in time (e.g., wet appliances) to mask individual appliance signatures (Chin et al., 2020; Kyri Baker and Kaitlyn Garifi, 2018). Of particular interest in this approach are electric vehicles (EVs) in the presence of smart-charging technology, which can be used at different power levels and for different periods of time. One limitation of approaches based on flexible loads is that at some stage energy can be consumed without need. For example, turning the water heater ON even if hot water is not required implies that extra electricity is used, and potentially a thermal loss if the hot water is not used in due time.

2.2 | Change meter data

In contrast to CEP, approaches under the change meter data category aim at changing the SM readings before they are used by third-party entities, for example, the utility. There are three main approaches under the CMD category: (1) *noise*

addition (NA), for example, (Barbosa et al., 2014; Fioretto et al., 2019; He et al., 2013); (2) *data-downsampling (DS)*, for example, (Cardenas et al., 2012; Reinhardt et al., 2013; Eibl & Engel, 2015); and (3) *data aggregation (DA)* (Ilic et al., 2013).

NA ensures the preservation of privacy by injecting tolerable noise into the SMs' original or aggregated readings, to obfuscate the real power consumption. Typical noise techniques, such as Gaussian, Laplace, or Gama noise, are employed as any of these enable that noise to cancel out once enough readings are put together (Barbosa et al., 2014). Thanks to the simplicity and low complexity of this approach, it can be easily deployed on low computing devices like most SMs. However, this solution suffers from a major drawback, which is the lack of formal methods for calculating the amount of noise that should be added to ensure the desired levels of privacy and also the utility needs (Barbosa, Brito, & Almeida, 2016). For example, the currently available techniques do not support dynamic power tariffs, which are quite common in smart-grid scenarios (Zhang et al., 2020).

Approaches via *data down-sampling* aim at protecting privacy by reducing the temporal frequency at which measurements are available to third-party entities. Typical approaches consist of decimation (consider only every M^{th} sample), filtering (e.g., average and median), and quantization (map the original measurement to a smaller set of discrete finite values; Reinhardt et al., 2013). Despite its simplicity, there is also an evident trade-off between privacy and utility needs when using this approach. For example, at very low data granularity dynamic tariffs and participation in demand response programs are no longer possible (Zhang et al., 2020).

Approaches that rely on DA reduce the privacy loss by constructing aggregators to collect the data from a few SMs together, so the utility is unable to detect the electricity events in a single meter. Techniques under this category are either with or without a trusted third party (TTP). In the former case, a data aggregator (DA) is responsible for gathering data from SMs and sending them to the utility. For example, in (Bohli et al., 2010) the data in each meter is encrypted (e.g., asymmetric encryption) before being sent to the DA, which in turn decrypts and averages the data from the different meters before sending it (encrypted) to the utility. As for the latter, encryption techniques like homomorphic encryption (HE) are used to encrypt the meter data before being sent to the utility, which is then able to manipulate the data without decrypting it (Li et al., 2010; Lu et al., 2012). Privacy protection techniques based on HE are discussed in detail in the remaining sections of this article.

2.3 | Comparison between techniques

To summarize, we perform a comparison of the above-mentioned approaches. The comparison is based on the following indicators: the financial cost, environmental impact, end-user impact, computational complexity, and independence between SMs. The comparison results are summarized in Table 1, where the number of checkmarks (✓) varies from zero (worst) to three (best).

The following observations are made:

- *Low cost and low environmental impact*: As mentioned, BESS helps to mitigate many privacy issues, but it is impossible to ignore its environmental effects and costs of using batteries (Dehghani-Sanij et al., 2019). Besides that, adding additional battery cycles for privacy protection may result in a lower calendar life of the devices. RES, on the other hand, is also not necessarily low cost. However, the prices have been consistently dropping, especially in the case of

TABLE 1 Comparison between the reviewed privacy protection techniques

	CEP			CMD		
	BESS	**RES**	**FL**	**NA**	**DS**	**DA**
Low cost		✓	✓✓	✓✓✓	✓✓✓	✓✓
Low environmental impact		✓	✓✓	✓✓✓	✓✓✓	✓✓✓
Low end-user impact			✓	✓✓	✓✓✓	✓✓✓
Low computational complexity	✓	✓	✓	✓✓	✓✓✓	
Independence between meters	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	

Note: The number of checkmarks (✓) varies from zero (worst) to three (best).

solar PV. These also have a lower environmental impact, especially when compared to Li-ion batteries (Dai et al., 2015). The remaining approaches do not have this limitation, despite DA (in particular HE) may require more expensive hardware.

- *Low user impact*: Approaches under the CEP have a significant impact on the end-users. This is particularly true in the case of BESS and RES given the trade-offs between device operation for privacy protection and economic benefits. Likewise, FL can also have a significant user impact if the operation of such devices has undesirable effects on the daily life of the end-users. NA, on the other hand, does not affect routines, however, it currently suffers from the limitation that it does not support the application of dynamic tariffs, which may end up impacting end-users choices. The same issue can happen with DS, depending on the data down-sampling factor. For example, reducing the sampling to one sample per hour would imply that dynamic energy prices can only change every hour.
- *Computational complexity*: Low computational complexity is mainly desired because most installed SMs have low-cost micro-controllers with very limited computing resources. In this respect, DA approaches are the most complex, especially those based on HE. In contrast, NA and DS are the least complex solutions. As for the approaches under the CEP category they all have similar levels of complexity since the working principle is very similar. The main difference is the enabling technology, which adds its own constraints in terms of load-leveling capacity.
- *Independence between meters*: The only approach studied here that does not have independence between SMs is DA (considering HE) because to exchange randomly generated keys, and secret shares, HE protocols require communication between the meters. Additionally, if a meter fails any message exchange, aggregation can become impossible if it requires pending calculations using all distributed keys or secret shares. This, in turn, can create scalability problems when DA is applied in areas with a large number of meters.

2.4 | Relation to other review articles

Having received the attention of a large body of work, there are already some interesting published literature reviews on the field. A listing of such review articles is presented in Table 2, where "Focus" indicates the categories reviewed (CEP, CMD, or Both), and "HE" indicates if HE is addressed (Y—Yes, N—No).

In their article, (Barbosa, Freitas, et al., 2016), the authors explore the technical details of five different privacy-preserving approaches, namely, NA, BESS, and three HE alternatives. In (Finster & Baumgart, 2015), privacy protection of SM data is reviewed from two perspectives, billing, and operations. This article also reviews approaches under CEP and CMD categories, including BESS and HE, but unlike (Barbosa, Freitas, et al., 2016) it does not go deep with regard to HE based approaches. In (Asghar et al., 2017), the authors cover several techniques under the CEP and CMD categories, considering three uses of SM data: billing, operations, and value-added services. Ultimately, this review does not provide in-depth technical details about any of the techniques but rather explores whether each technique can be applied and still enable the different use cases. Similarly, (Farokhi, 2020) and (Win & Tonyalı, 2021) provide high-level overviews of SM data privacy using both CEP and CMD based techniques.

While these five review articles cover techniques under the two categories, the works presented in (Giaconi, Gunduz, & Poor, 2018) and (Agarkar & Agrawal, 2019) focus only on one of the categories. More precisely, (Giaconi,

TABLE 2 List of review articles in privacy protection of smart-meter data

Title	References	Focus	HE
Privacy-aware smart metering: A survey	(Finster & Baumgart, 2015)	Both	Y
Privacy-preserving techniques in smart metering: An overview	(Barbosa, Freitas, et al., 2016)	Both	Y
Smart meter data privacy: A survey	(Asghar et al., 2017)	Both	Y
Privacy-aware smart metering: Progress and challenges	(Giaconi, Gunduz, & Poor, 2018)	CEP	N
A review and vision on authentication and privacy preservation schemes in smart grid network	(Agarkar & Agrawal, 2019)	CMD	Y
Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling	(Farokhi, 2020)	Both	N
Security and privacy challenges, solutions, and open issues in smart metering: A review	(Win & Tonyalı, 2021)	Both	Y

Gunduz, & Poor, 2018) focuses on techniques under the CEP category; namely, BESS, RES, and DS. Conversely, (Agarkar & Agrawal, 2019) reviews cryprographic approaches for privacy preservation, which fall in the CMD category; it addresses HE, elliptic curve cryptography (ECC), and lattice cryptography (LC) based schemes, showing how they have been employed by other researchers. This review article provides an overview and comparison of techniques under CEP and CMD categories, before focusing on the details of HE. Unlike the existing reviews, this article attempts to provide a comprehensive overview of the technical details of HE approaches, in particular of ElGamal cryptosystems. Two possible application scenarios using that cryptosystem and based on different types of aggregation are also presented.

3 | HOMOMORPHIC ENCRYPTION

Smart metering systems need a secure way to regularly transmit consumption information through the Internet such that the privacy of consumers is preserved. Privacy protection approaches based on cryptography have already proven their usefulness in this field. These are particularly interesting approaches because, on the one hand, they prevent attackers from obtaining confidential data without the private key and, on the other hand, they avoid falsifying signatures to request arbitrary readings (Rouf et al., 2012). One such approach is HE. This is especially useful when solutions are aggregated and meters are organized into groups. At the level of smart metering, HE turns out to be very important because it allows the supplier to obtain only the aggregate consumption values from the meters in each group.

There are essentially two proposals related to cryptography and smart grid networks that can be found in the literature: *HE* and *ECC* (Agarkar & Agrawal, 2019). The first proposal includes several possible cryptosystems, the best known being Paillier cryptosystem and ElGamal cryptosystem.

HE is a standard approach to secure multi-party computation (SMC) that allows direct arithmetic operations on encrypted values. SMC is a cryptographic problem in which multiple parties jointly compute a value based on individually held private data, without sharing the data. In this problem, security is often derived from one-way functions like integer factorization or discrete logarithm problem. The best-known example of SMC is the millionaire problem: Alice and Bob are interested in knowing which of them is richer without revealing their true wealth. More formally, for several individuals $I_1,...,I_n$, each has initial inputs $x_1,...,x_n$. The output y_i is calculated using a function f, such that: $f(x_1,...,x_n) = (y_1...,y_n)$. That is, each individual I_i only obtains the output y_i. During the computation process, the actual value of each I_i's input x_i is kept privately without being revealed to anyone but y_i's values are public. This process is achieved by applying HE over the integers $x_1,...,x_n$.

In (Domingo-Ferrer, 2002), HE schemes are defined as "encryption transformations mapping a set of operations on cleartext to another set of operations on ciphertext." In other words, this means that it is possible to perform operations on the ciphertext without decrypting it first. Homomorphic cryptographic systems are a security protocol option, thanks to their additive and multiplicative homomorphic properties. A *fully homomorphic* encryption (FHE) scheme allows the multiplication and addition of ciphertext. However, such schemes are relatively new and complex. It was only in 2009 that Craig Gentry developed the first fully homomorphic algorithm (Gentry, 2009). Therefore, it is preferable to use *partially* HE schemes, which allows only one of these operations (Zirm & Niedermeier, 2012).

In (Knirsch et al., 2020), the authors present a direct comparison between the ElGamal and Paillier cryptosystems for smart grid aggregation protocols, considering both runtime for encryption and decryption. Ultimately, the ElGamal outperformed the Pailier cryptosystem, with a faster encryption-decryption execution time, as well as other features. Therefore, in this article we focus on the study of ElGamal's cryptosystem.

Before moving on, remember from Section 2.3 that HE has some disadvantages. The two main disadvantages for smart grid are: (1) the complexity of the mathematical operations which make homomorphic schemes computationally expensive; and (2) the fact that the meters are not independent, since cooperation between them is required to avoid the need for a third-party entity to handle the generation and consequent distribution/sharing of the private key (Barbosa, Brito, & Almeida, 2016).

Such disadvantages suggest the need for another ElGamal scheme using elliptic curves, hence renewing the presence of a reliable entity. Using cryptography based on elliptic curves the resulting system requires only one message sent from each SM without the need for communication between the meters. *ECC* is based on the properties of algebraic curves over fields and the security of *ECC* is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP).

In this article, we present the technical details for two homomorphic cryptography schemes. The first scheme is based on the discrete logarithm problem (DLP) and requires communication between meters. The second scheme relies on elliptical curves to remove the need for communication between meters. These two approaches are described in the

following sub-sections. For each system, we describe the cryptographic procedures and present the homomorphic property and an application example.

3.1 | Modified ElGamal cryptosystem

This first HE system presented here is based on the DLP which was proposed in (Barbosa, Freitas, et al., 2016). The DLP consists of the following: given a prime p, a generator g of $\mathbb{Z}_p^*$, and a nonzero element $y \in \mathbb{Z}_p$, find the unique integer x, $0 \leq x \leq p-2$, such that $y \equiv g^x \pmod{p}$.

3.1.1 | Cryptographic system description

Set up and key generation

1. Choose two large prime numbers p and q such that $q|p-1$;
2. Select a generator g of the order q multiplicative subgroup G of $\mathbb{Z}_p^*$;
3. The private key x is randomly generated such that $x \in \mathbb{Z}_q^*$ and the public key is $y = g^x$.

Encryption

1. The message $m \in G$ is encrypted with the public key y, obtaining a random number $r \in \mathbb{Z}_q^*$ and calculating:

$$c = g^r \text{ and } d = m.y^r.$$

2. The m cryptogram under the y public key is:

$$E_y(m) = (c, d).$$

Decryption

1. $E_y(m)$ is decrypted calculating: $m = d.c^{-x}$.

3.1.2 | Homomorphic property

This is a multiplicative homomorphic cryptographic system, since given messages m_1 and m_2, it is possible to obtain $m_1 \cdot m_2$ as follows:

$$E_y(m_1) \cdot E_y(m_2) = (c_1 \cdot c_2, d_1 \cdot d_2) = (g^{r_1} \cdot g^{r_2}, m_1 \cdot y^{r_1} \cdot m_2 \cdot y^{r_2}) = (g^{r_1+r_2}, m_1 \cdot m_2 \cdot y^{r_1+r_2}) = (c_1 \cdot c_2, d_1 \cdot d_2) = E_y(m_1 \cdot m_2).$$

3.1.3 | Application in SMs

The ElGamal cryptosystem can be used in such a way that it is additively homomorphic. Suppose we want to calculate the total consumption in a region. For that, (Busom et al., 2016) proposed an ElGamal cryptosystem similar to the previous one but additive, such that:

$$E_y(g^{m_1}) \cdot E_y(g^{m_2}) = E_y(g^{m_1} \cdot g^{m_2}) = E_y(g^{m_1+m_2}).$$

First, each SM has a large prime number q and its generator g, a private key x_i and a public key $y_i = g^{x_i}$.

To encrypt measurements, a global public key $y = \prod_{i=1}^{N} y_i$ is necessary. So let m_i be the measurement of a SM. The total consumption will consist of the following procedure:

1. Each meter generates a random value $z_i \in \mathbb{Z}_q^*$ and computes the ciphertext by doing:

$$C_i = E_y(g^{m_i+z_i}) = (c_i, d_i).$$

2. C_i is sent to the aggregator.
3. The aggregator combines all messages by doing:

$$C = \left(\prod_{i=1}^{N} c_i, \prod_{i=1}^{N} d_i\right) = (c, d)$$

and send c for each SM.

4. Each meter calculates $T_i = c^{x_i} \cdot g^{z_i}$ and send the result to the aggregator.

5. At the end, the aggregator calculates $D = d \cdot \left(\prod_{i=1}^{N} T_i\right)^{-1}$ and $\log_g D = M = \sum_{i=1}^{N} m_i$, where M is the total consumption.

In order to illustrate the cryptosystem that we have just presented, follow the scheme below. Let ESS denote electricity supply substation which here represents the aggregating entity that receives periodic measurements from the SMs (Figure 2).

This example works because the ESS calculates:

$$C = \left(\prod_{i=1}^{N} c_i, \prod_{i=1}^{N} d_i\right) = \left(\prod_{i=1}^{N} g^{r_i}, \prod_{i=1}^{N} g^{m_i+z_i} \cdot y^{r_i}\right) = \left(g^r, g^{M+z} \cdot y^r\right) = (c, d)$$

and each SM computes:

$$T_i = c^{x_i} \cdot g^{z_i} = g^{r \cdot x_i} \cdot g^{z_i} = g^{x_i \cdot r} \cdot g^{z_i} = y_i^r \cdot g^{z_i}.$$

So, the ESS calculates:

$$D = d \cdot \left(\prod_{i=1}^{N} T_i\right)^{-1} = \frac{g^{M+z} \cdot y^r}{\prod_{i=1}^{N} (y_i^r \cdot g^{z_i})} = \frac{g^{M+z} \cdot y^r}{\prod_{i=1}^{N} (y_i^r) \cdot g^z} = \frac{g^{M+z} \cdot y^r}{g^z \cdot y^r} = g^M$$

In practice, when a SM is installed in a house, it establishes a connection with the ESS and before transmitting electricity measurements, the ESS needs to indicate to all SMs the start of a key establishment operation. This can be done as follows:

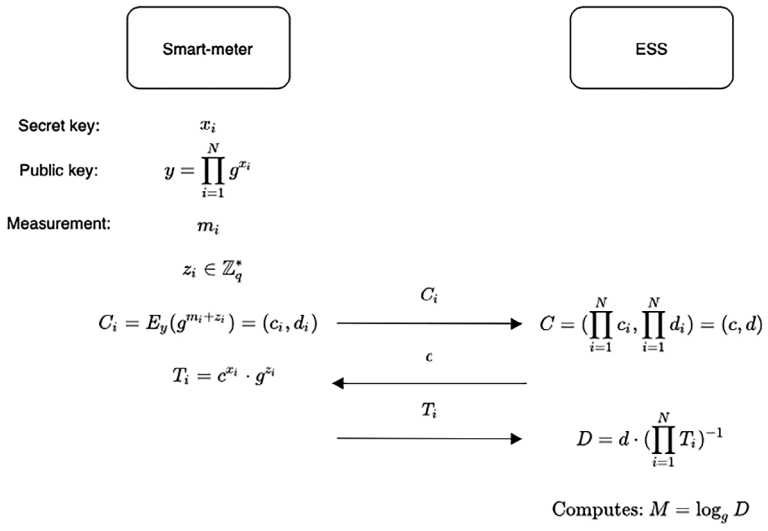

FIGURE 2 Schema of the ElGamal cryptosystem

1. ESS sends a message to each SM indicating that a key establishment will be carried out.
2. Each SM sends g^{x_i} and $Cert_i$ to ESS.
3. ESS verifies the validity of $Cert_i$. If it is correct, y_i and $Cert_i$ are sent to all the other SMs that will perform the same check.
4. Each SM computes the group public key as $y = \prod_{i=1}^{N} g^{x_i}$.

This validation process for the construction of the public key allows us to obtain the following scheme (Figure 3):

3.2 | ElGamal cryptosystem using elliptic curves

An elliptic curve is represented by an equation of the form:

$$y^2 = x^3 + ax + b,$$

with $\Delta = -16(4a^3 + 27b^2) \neq 0$. ECC is based on the ECDLP, that is, given two points A and B on the curve such that one is a scalar multiple of the other, $A = k \cdot B$, it is computationally difficult to calculate k.

An ElGamal cryptosystem with additive homomorphism can be also defined using ECC, represented in (Deepak & Chandrasekaran, 2020), as follows:

3.2.1 | Cryptographic system description

Set up and key generation

1. Choose a base point P of order N on an elliptic curve E over a finite field;
2. Choose f: $x \mapsto P_x$, which converts plaintexts x into points P_x on E. The function f is defined as $f(x) = x \cdot P$, where $\cdot$ represents the scalar multiplication of the point P with x;
3. Select a random private key $k \in \mathbb{Z}_N$.
4. The public key is the pair of points $(P, Y = k \cdot P)$.

Encryption

1. Choose a random number $a \in \mathbb{Z}_N$.

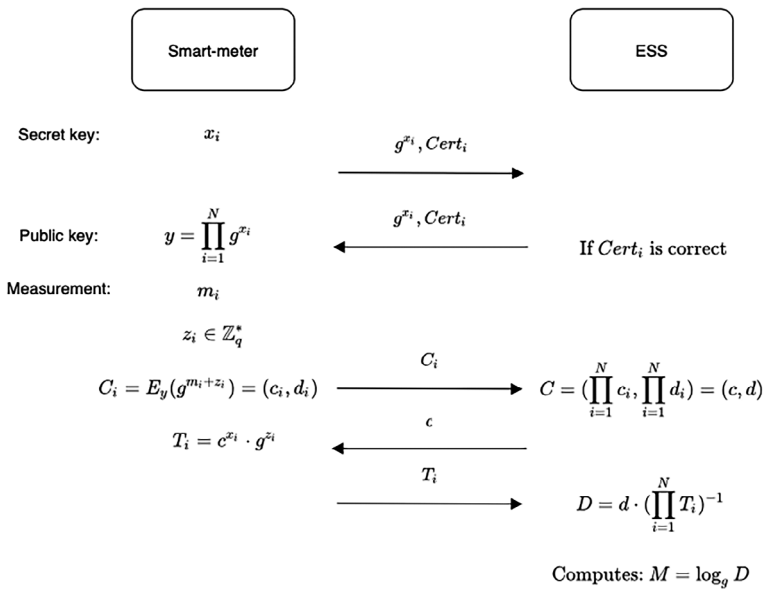

FIGURE 3 Schema of the ElGamal cryptosystem applied to a neighborhood of smart-meters

2. Calculate $P_x = f(x)$, where x is the plaintext;
3. The ciphertext is the pair of points $(a \cdot P, a \cdot Y + P_x)$.

Decryption
1. From a received ciphertext (B_1, B_2), calculate $B_1{}' = k \cdot B_1$ using the private key k;
2. Compute $P_x = B_2 - B_1{}'$;
3. The original plaintext x is $f^{-1}(P_x)$.

3.2.2 | Homomorphic property

Let us consider two ciphertexts $c = (c_1, c_2)$, $d = (d_1, d_2)$, where c and d are the encryptions of messages x and y, respectively under the same key k. For a random a and b, let $c = (a \cdot P, a \cdot Y + x \cdot P)$, $d = (b \cdot P, b \cdot Y + y \cdot P)$. The ciphertext corresponding to the encryption of the message $(x + y)$ under key k is:

$$c + d = ((a+b) \cdot P, (a+b) \cdot Y + (x+y) \cdot P)$$

3.2.3 | Application in SMs

ECC is based on the properties of algebraic curves over fields. Let us exemplify here, without going into too much detail, how this cryptosystem could be applied to SMs.

First, each SM has a base point P of order N on an elliptic curve E over a finite field, a private key $k \in \mathbb{Z}_N$ and a public key is the pair of points $(P, Y = k \cdot P)$. Let m_i be the measurement of a SM. The total consumption will be denoted by M and consist of the following procedure:

1. Each meter generates a random value $a \in \mathbb{Z}_N$ and computes the ciphertext by doing:

$$(B_i, B_{i+1}) = (a \cdot P, a \cdot Y + P_{m_i}),$$

where $P_{m_i} = f(m_i)$ and f is a function defined as $f(m_i) = m_i \cdot P$.

2. (B_i, B_{i+1}) is sent to the aggregator.
3. The aggregator combines all messages by doing:

$$C = (C_1, C_2) = \sum_{j=1}^{N} (B_j, B_{j+1})$$

and send C_1 for each SM.

4. Each meter calculates $C_1' = k \cdot C_1$ and send the result to the aggregator.
5. Finally the aggregator calculates $P_M = C_2 - C_1'$ and computes $M = f^{-1}(P_M)$.

In order to illustrate the idea of the cryptosystem that we have just presented, follow the scheme below (Figure 4).

Similar to the previous scheme and so that the ESS indicates to all SMs the start of a key establishment operation, we have the following more complete scheme:

4 | POSSIBLE APPLICATION SCENARIOS USING ElGamal CRYPTOSYSTEM

In this section, we present two possible scenarios on how to use the ElGamal cryptosystem, introduced in the last section, in the context of SM privacy preservation. The two scenarios presented are based on the ones presented in (Zirm & Niedermeier, 2012) to demonstrate the application of the Paillier cryptosystem. More precisely, SMs are

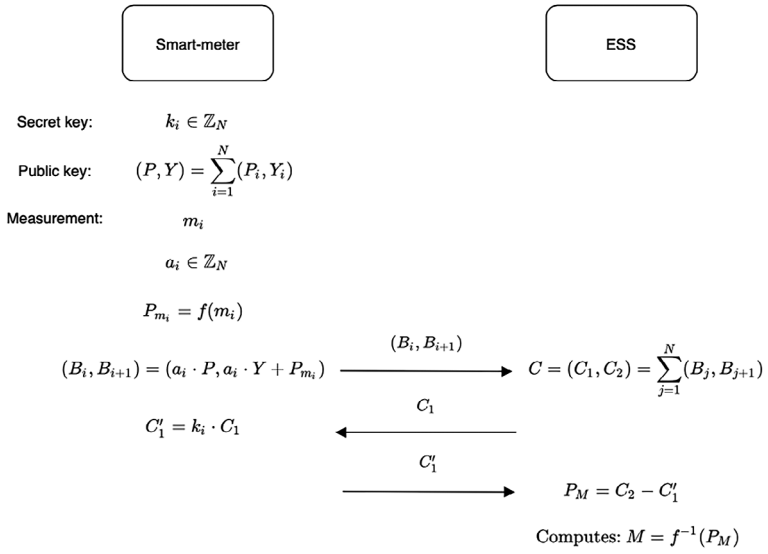

FIGURE 4 Schema of the ElGamal cryptosystem

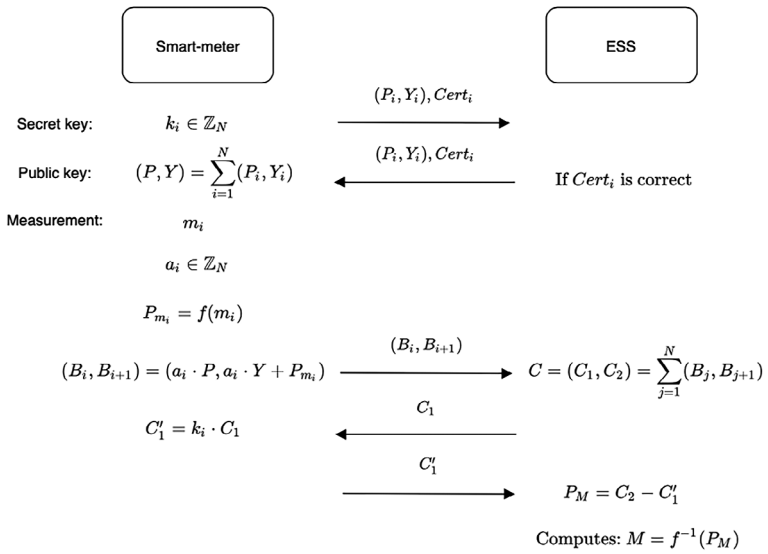

FIGURE 5 Schema of the ElGamal cryptosystem applied to a neighborhood of smart-meters

grouped into clusters and the objective is to send the aggregated load profiles of each cluster to the utility, without revealing the individual profile of each SM. For the sake of simplicity, it is assumed that the communication channels are already protected (Figure 5).

4.1 | Scenario 1: direct aggregation

In this scenario, the ElGamal cryptosystem with additive homomorphic property is used to aggregate user data in a separate aggregator, as illustrated in Figure 6.

In this scenario, each participating entity owns a set of keys (private and public). All the SMs send their data to the respective cluster aggregator, encrypted with the Power Company public key. There, individual data is not deciphered but aggregated using the homomorphic properties of the ElGamal cryptosystem. The Aggregator is therefore in possession of the cluster's overall encrypted consumption without knowing the individual SM measurements. The encrypted

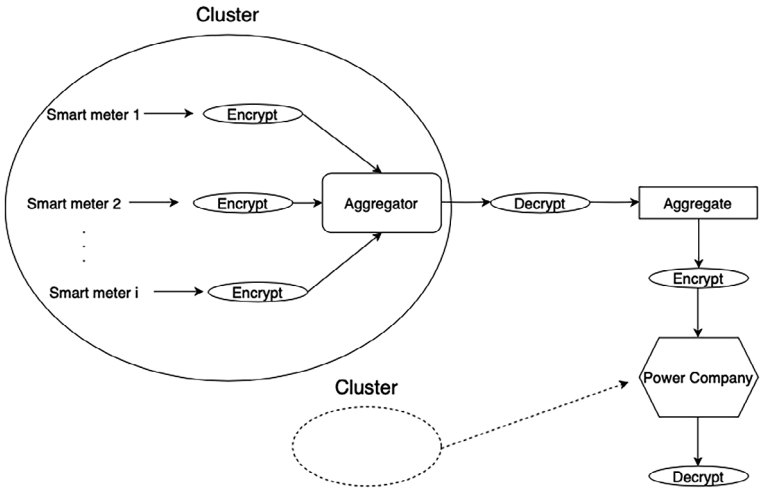

FIGURE 6 Scenario 1: direct aggregation

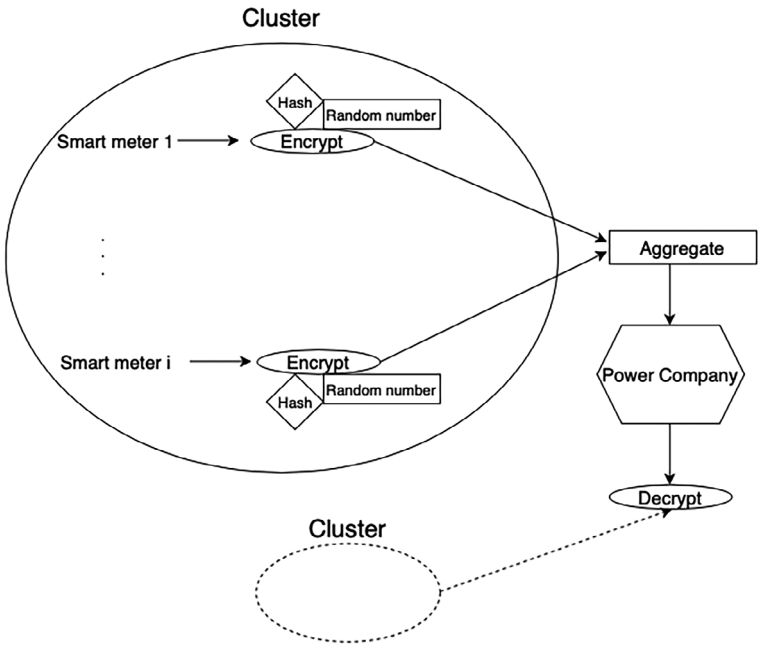

FIGURE 7 Scenario 2: spatial and temporal aggregation

data are then sent to the Power Company which is able to decrypt it using its private key. Upon decryption of the data, the Power Company is in possession of the aggregated load profile, without knowing its individual components.

4.2 | Scenario 2: spatial and temporal aggregation

In this second scenario, all SMs in a cluster have the same public key and the private key is known to all entities. Moreover, a separate Aggregator is not needed, because each SM can act as an aggregator itself. The procedure is illustrated in Figure 7.

In this approach, each SM whit-in a cluster is responsible for encrypting its data (p). Each SM is also in possession of a secret hash $H(p)$, and a random number $r \in \mathbb{N}$. Note that even though the private keys are known within a particular cluster, individual consumption data cannot be decrypted because the $H(p)$ and r are only known by each SM. In

fact, it is only when all the values are aggregated, using the homomorphic property, that they can be decrypted by the Power Company.

4.3 | Summary

In summary, when comparing the two scenarios, the second is more flexible than the first one because it allows adaptation to various smart-grid scenarios and privacy requirements. For example, the second scenario can be easily adapted to transfer the consumption data of individual appliances to the Power Company, whereas in the first scenario, only the aggregated data can be transmitted to the Power Company. Furthermore, since it is not necessary to keep private keys, this does no longer present a potential security breach.

5 | CONCLUSION

Ultimately, HE seems to be the only option where there is no trade-off between privacy and the benefits of the smart grid. For example, CLP approaches have a significant effect on how the load is managed to assure privacy, which may not be the best option for smart-grid operators. As for CMD, all these operations considerably reduce the quality of the data available to the grid operator. In contrast, in HE, the actual measurements are available although in an indirect format, which ensures privacy and at the same time adequate smart-grid operations.

However, one of the major problems of HE is the high computational cost of performing operations on top of encrypted data that are several orders of magnitude slower than operations on unencrypted data.[1] Against this background, recent times have seems some efforts toward improving the computational performance of HE by introducing hardware acceleration using GPU, FPGA, and possibly ASICs, for example, (Morshed et al., 2020; Roy et al., 2017; Yang et al., 2020). Furthermore, some efforts have also been developed toward producing custom hardware for HE. For example, in March 2021, Intel announced a partnership with Defense Advanced Research Projects Agency (DARPA) to perform in its Data Protection in Virtual Environments (DPRIVE) program, which aims to develop an accelerator for FHE[2].

Currently, homomorphic cryptography has reached an inflection point and much of its future development will consist of standardization. An important part of standardization is broad agreement on security levels for various parameter sets. There is currently a document approved by the Homomorphicencryption.org community in 2018 with recommendations of security parameters to be used for HE at various security levels (Albrecht et al., 2019; Chase et al., 2017). Future versions of the standard should also describe a standard API (Brenner et al., 2017) and a programming model for HE (Archer et al., 2017).

Ironically, despite the fact HE solutions are still very hard to implement in practice, one of the main challenges in HE research lies whit-in the fact that HE needs to be adapted to the post-quantum era. In fact, it has already been shown that a quantum computer with a sufficiently large number of qubits and depth of circuits can solve some of the hard mathematical problems that form the basis of state-of-the-art homomorphic cryptography schemes (Agarkar & Agrawal, 2019) and it is certain that the future and application of homomorphic cryptography will have to include and rely on quantum computing (Alloghani et al., 2019). It is not yet known when there will be a stable quantum computer capable of overthrowing current classical primitives, but the rapid development in this area means that it is important to start preparing for what will be the future of cryptography. One of the approaches that have been considered is LC.[3] Still, as mentioned by the authors (Agarkar & Agrawal, 2019), Lattice-based cryptography has not seen much development in the context of the smart grid.

To sum up, it is clear that HE can contribute significantly to advancing the smart grid without compromising end-user privacy. Nevertheless, besides the need for additional research toward making HE computationally efficient and safeguard from future quantum computers, it is also crucial to develop an applied and multi-disciplinary research agenda aiming at understanding and demonstrating how HE can be applied to different smart-grid use cases.

AUTHOR CONTRIBUTIONS

Zita Abreu: Conceptualization (supporting); formal analysis (equal); investigation (lead); methodology (equal); validation (equal); visualization (equal); writing – original draft (equal); writing – review and editing (equal). **Lucas Pereira:** Conceptualization (lead); formal analysis (equal); funding acquisition (lead); investigation (supporting); methodology

(equal); project administration (lead); supervision (equal); validation (equal); writing – original draft (equal); writing – review and editing (equal).

CONFLICT OF INTEREST

The authors have declared no conflicts of interest for this article.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Lucas Pereira https://orcid.org/0000-0002-9110-8775

RELATED WIREs ARTICLES

Data privacy
Data mining privacy preserving: Research agenda
Privacy preserving classification over differentially private data

ENDNOTES

[1] https://pureai.com/articles/2020/07/13/homomorphic-encryption.aspx?m=1.

[2] https://www.intel.com/content/www/us/en/newsroom/news/intel-collaborate-microsoft-darpa-program.html.

[3] https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717.

REFERENCES

Agarkar, A., & Agrawal, H. (2019). A review and vision on authentication and privacy preservation schemes in smart grid network. *Security and Privacy*, *2*, e62. https://doi.org/10.1002/spy2.62

Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., & Vaikuntanathan, V. (2019) *Homomorphic encryption standard*. Cryptology ePrint Archive, Report 2019/939. https://ia.cr/2019/939.

Alloghani, M. A., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. *Journal of Information Security and Applications*, *48*, 102362.

Anderson, R., & Fuloria, S. (2010). Who controls the off switch? In *2010 First IEEE International Conference on Smart Grid Communications*, pp. 96–101.

Archer, D., Chen, L., Cheon, J. H., Gilad-Bachrach, R., Hallman, R. A., Huang, Z., Jiang, X., Kumaresan, R., Malin, B. A., Sofia, H., Song, Y., & Wang, S. (2017) Applications of homomorphic encryption. *Technical Report*, HomomorphicEncryption.org, Redmond, WA.

Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys & Tutorials*, *19*, 2820–2835.

Baker, K., & Garifi, K. (2018). Power signature obfuscation using flexible building loads. In *4th International NILM Workshop*. Austin, TX. http://nilmworkshop.org/2018/proceedings/Paper_ID02.pdf.

Barbosa, P., Brito, A., & Almeida, H. (2016). A technique to provide differential privacy for appliance usage in smart metering. *Information Sciences*, *370-371*, 355–367 http://www.sciencedirect.com/science/article/pii/S0020025516305862

Barbosa, P., Brito, A., Almeida, H., & Clauß, S. (2014). Lightweight privacy for smart metering data by adding noise. *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, SAC'14, pp. 531–538. Association for Computing Machinery, New York, NY. https://doi.org/10.1145/2554850.2554982.

Barbosa, P., Freitas, L., Brito, A., & Silva, L. (2016). Privacy-preserving techniques in smart metering: An overview. *XVI Brazilian Symposium on Information and Computational Systems Security*. Rio de Janeiro, Brazil.

Bohli, J., Sorge, C., & Ugus, O. (2010). A privacy model for smart metering. *2010 IEEE International Conference on Communications Workshops*, pp. 1–5.

Brenner, M., Dai, W., Halevi, S., Han, K., Jalali, A., Kim, M., Laine, K., Malozemoff, A., Paillier, P., Polyakov, Y., Rohloff, K., Savaş, E., & Sunar, B. (2017). A standard API for RLWE-based homomorphic encryption. *Technical Report*. HomomorphicEncryption.org. Redmond, WA.

Busom, N., Petrlic, R., Sebé, F., Sorge, C., & Valls, M. (2016). Efficient smart metering based on homomorphic encryption. *Computer Communications*, *82*, 95–101 https://linkinghub.elsevier.com/retrieve/pii/S0140366415003151.00026

Cardenas, A., Amin, S., & Schwartz, G. A. (2012). Privacy-aware sampling for residential demand response programs. *Proceedings of the 1st International ACM Conference on High Confidence Networked Systems (HiCoNS)*. ACM, Beijing, China. http://www.truststc.org/pubs/903.html.

Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Hoffstein, J., Lauter, K., Lokam, S., Moody, D., Morrison, T., Sahai, A., & Vaikuntanathan, V. (2017) Security of homomorphic encryption. *Technical report*. HomomorphicEncryption.org. Redmond, WA.

Chen, D., Kalra, S., Irwin, D., Shenoy, P., & Albrecht, J. (2015). Preventing occupancy detection from smart meters. *IEEE Transactions on Smart Grid*, *6*, 2426–2434.

Chin, J.-X., Baker, K. and Hug, G. (2020) Consumer privacy protection using flexible thermal loads. *arXiv:2002.05408 [cs, eess, math]*. http://arxiv.org/abs/2002.05408.

Chin, J.-X., Baker, K., & Hug, G. (2021). Consumer privacy protection using flexible thermal loads: Theoretical limits and practical considerations. *Applied Energy*, *281*, 116075.

Dai, K., Bergot, A., Liang, C., Xiang, W.-N., & Huang, Z. (2015). Environmental issues associated with wind energy—A review. *Renewable Energy*, *75*, 911–921 http://www.sciencedirect.com/science/article/pii/S0960148114007149

Deepak, K. & Chandrasekaran, K. (2020). Investigating elliptic curve cryptography for securing smart grid environments. *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, pp. 1–7.

Dehghani-Sanij, A. R., Tharumalingam, E., Dusseault, M. B., & Fraser, R. (2019). Study of energy storage systems and environmental challenges of batteries. *Renewable and Sustainable Energy Reviews*, *104*, 192–208 http://www.sciencedirect.com/science/article/pii/S1364032119300334

Domingo-Ferrer, J. (2002). A provably secure additive and multiplicative privacy homomorphism. *Proceedings of the 5th International Conference on Information Security*, ISC'02, pp. 471–483. Springer-Verlag, Berlin, Heidelberg.

Egarter, D., Prokop, C., & Elmenreich, W. (2014). Load hiding of household's power demand. *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 854–859.

Eibl, G., & Engel, D. (2015). Influence of data granularity on smart meter privacy. *IEEE Transactions on Smart Grid*, *6*, 930–939.

Evans, J. (2012). *The opt-out challenge. Electric Light & Power*. https://senate.texas.gov/cmtes/82/c510/1009-WaltBaum06.pdf.

Exponent Inc. (2014) Scientific and Public Health Agency perspectives on radio frequency fields related to smart meters. *Technical Report. 1300283.000-2940*, Vermont Department of Health, Montpelier, VT.

Farokhi, F. (2020). Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. *IET Smart Grid*, *3*, 605–613.

Farokhi, F., & Sandberg, H. (2018). Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries. *IEEE Transactions on Smart Grid*, *9*, 4726–4734.

Finster, S., & Baumgart, I. (2015). Privacy-aware smart metering: A survey. *IEEE Communications Surveys Tutorials*, *17*, 1088–1101.

Fioretto, F., Mak, T. W. K., & Van Hentenryck, P. (2019). Differential privacy for power grid obfuscation. *IEEE Transactions on Smart Grid*, *11*, 1356–1366 https://ieeexplore.ieee.org/document/8809257

Gentry, C. (2009) *A fully homomorphic encryption scheme*. (PhD thesis). Stanford University. crypto.stanford.edu/craig.

Giaconi, G., Gündüz, D., & Poor, H. V. (2018). Smart meter privacy with renewable energy and an energy storage device. *IEEE Transactions on Information Forensics and Security*, *13*, 129–142.

Giaconi, G., Gunduz, D., & Poor, H. V. (2018). Privacy-aware smart metering: Progress and challenges. *IEEE Signal Processing Magazine*, *35*, 59–78.

Gündüz, D. & Gómez-Vilardebó, J. (2013). Smart meter privacy in the presence of an alternative energy source. *2013 IEEE International Conference on Communications (ICC)*, pp. 2027–2031.

Hahn, A. & Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2. IEEE Transactions on Smart Grid.

He, X., Zhang, X., & Kuo, C.-C. J. (2013). A distortion-based approach to privacy-preserving metering in smart grids. *IEEE Access*, *1*, 67–78.

Hess, D. J., & Coley, J. S. (2014). Wireless smart meters and public acceptance: The environment, limited choices, and precautionary politics. *Public Understanding of Science*, *23*, 688–702. https://doi.org/10.1177/0963662512464936

Hussain, S., Meraj, M., Abughalwa, M., & Shikfa, A. (2018). Smart grid cybersecurity: Standards and technical countermeasures. *2018 International Conference on Computer and Applications (ICCA)*, pp. 136–140.

Ilic, D., Karnouskos, S., & Wilhelm, M. (2013). A comparative analysis of smart metering data aggregation performance. *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 434–439. IEEE, Bochum, Germany. http://ieeexplore.ieee.org/document/6622924/.

Jin, M., Jia, R., & Spanos, C. J. (2017). Virtual occupancy sensing: Using smart meters to indicate your presence. *IEEE Transactions on Mobile Computing*, *16*, 3264–3277.

Knirsch, F., Unterweger, A., Unterrainer, M., & Engel, D. (2020). Comparison of the Paillier and ElGamal cryptosystems for smart grid aggregation protocols. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, pp. 232–239. SCITEPRESS—Science and Technology Publications, Valletta, Malta. https://doi.org/10.5220/0008770902320239.

Li, F., Luo, B., & Liu, P. (2010). Secure information aggregation for smart grids using homomorphic encryption. *2010 First IEEE International Conference on Smart Grid Communications*, pp. 327–332.

Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. S. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, *23*, 1621–1631. https://doi.org/10.1109/TPDS.2012.86

Mogles, N., Walker, I., Ramallo-González, A. P., Lee, J., Natarajan, S., Padget, J., Gabe-Thomas, E., Lovett, T., Ren, G., Hyniewska, S., O'Neill, E., Hourizi, R., & Coley, D. (2017). How smart do smart meters need to be? *Building and Environment*, *125*, 439–450 http://www.sciencedirect.com/science/article/pii/S0360132317304225

Morshed, T., Aziz, M. M. A., & Mohammed, N. (2020). CPU and GPU accelerated fully homomorphic encryption. *arXiv:2005.01945 [cs]*.

NIST (2014) Guidelines for smart grid cybersecurity. *Tech. Rep. NIST IR 7628r1*, National Institute of Standards and Technology, Gaithersburg, MD, USA. URL: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

Pereira, L., & Nunes, N. (2018). Performance evaluation in non-intrusive load monitoring: Datasets, metrics, and tools—A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *8*, e1265. https://doi.org/10.1002/widm.1265

Reinhardt, A., Egarter, D., Konstantinou, G., & Christin, D. (2015). Worried about privacy? Let your PV converter cover your electricity consumption fingerprints. *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 25–30.

Reinhardt, A., Englert, F., & Christin, D. (2013). Enhancing user privacy by preprocessing distributed smart meter data. *2013 Sustainable Internet and ICT for Sustainability (SustainIT)*, pp. 1–7.

Richmond, R., Macari, E., Mantey, P., Wright, P., McCarthy, R., Long, J. C. S., Winickoff, D., & Papay, L. (2011) Health impacts of radio frequency from smart meters. *Technical Report*. CCST, Sacramento, CA. https://ccst.us/reports/health-impacts-of-radio-frequency-from-smart-meters/.

Rouf, I., Mustafa, H., Xu, M., Xu, W., Miller, R., & Gruteser, M. (2012). Neighborhood watch: Security and privacy analysis of automatic meter Reading systems. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS'12, pp. 462–473. Raleigh, NC, ACM. https://doi.org/10.1145/2382196.2382246.

Roy, S. S., Vercauteren, F., Vliegen, J., & Verbauwhede, I. (2017). Hardware assisted fully homomorphic function evaluation and encrypted search. *IEEE Transactions on Computers*, *66*, 1562–1572.

Rubio, J. E., Alcaraz, C., & Lopez, J. (2017). Recommender system for privacy-preserving solutions in smart metering. *Pervasive and Mobile Computing*, *41*, 205–218 http://www.sciencedirect.com/science/article/pii/S1574119217301645

Snap Energy Latino. (2019). *History of smart meters*. https://snapenergylatino.com/history-of-smart-meters/.

Sun, Y., Lampe, L., & Wong, V. W. S. (2015). Combining electric vehicle and rechargeable battery for household load hiding. *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 611–616.

Tan, O., Gunduz, D., & Poor, H. V. (2013). Increasing smart meter privacy through energy harvesting and storage devices. *IEEE Journal on Selected Areas in Communications*, *31*, 1331–1341.

Völker, B., Reinhardt, A., Faustine, A., & Pereira, L. (2021). Watt's up at home? Smart meter data analytics from a consumer-centric perspective. *Energies*, *14*, 719.

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*, 1344–1371 http://www.sciencedirect.com/science/article/pii/S1389128613000042

Wang, Y., Chen, Q., Hong, T., & Kang, C. (2019). Review of smart meter data analytics: Applications, methodologies, and challenges. *IEEE Transactions on Smart Grid*, *10*, 3125–3148.

Win, L. L. & Tonyalı, S. (2021) Security and privacy challenges, solutions, and open issues in smart metering: A review. In *2021 6th International Conference on Computer Science and Engineering (UBMK)*, 800–805.

Yang, Z., Hu, S. & Chen, K. (2020) FPGA-based hardware accelerator of homomorphic encryption for efficient federated learning. *arXiv: 2007.10560 [cs]*.

Zhang, X.-Y., Kuenzel, S., Córdoba-Pachón, J.-R., & Watkins, C. (2020). Privacy-functionality trade-off: A privacy-preserving multi-channel smart metering system. *Energies*, *13*, 3221 https://www.mdpi.com/1996-1073/13/12/3221

Zhang, Z., Qin, Z., Zhu, L., Weng, J., & Ren, K. (2017). Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise. *IEEE Transactions on Smart Grid*, *8*, 619–626.

Zheng, J., Gao, D. W., & Lin, L. (2013). Smart meters in smart grid: An overview. In *2013 IEEE Green Technologies Conference (GreenTech)*, pp. 57–64.

Zirm, M. & Niedermeier, M. (2012) The future of homomorphic cryptography in smart grid applications. *Proceedings of the 3rd IEEE German Student Conference*. IEEE, Passau, Germany. https://pdfs.semanticscholar.org/b911/2a4d3aa84de19550c2acf6a107b79bb46838.pdf.

How to cite this article: Abreu, Z., & Pereira, L. (2022). Privacy protection in smart meters using homomorphic encryption: An overview. *WIREs Data Mining and Knowledge Discovery*, e1469. https://doi.org/10.1002/widm.1469