


Article

# A New Secure and Anonymous Metering Scheme for Smart Grid Communications

Shaohao Xie <sup>1,2,\*</sup> , Fangguo Zhang <sup>1,2,\*</sup>, Huizhi Lin <sup>1,2</sup> and Yangtong Tian <sup>1,2</sup>

<sup>1</sup> School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China; linhzh9@mail2.sysu.edu.cn (H.L.); tianyt6@mail2.sysu.edu.cn (Y.T.)

<sup>2</sup> Guangdong Key Laboratory of Information Security, Guangzhou 510006, China

\* Correspondence: xieshh6@mail2.sysu.edu.cn (S.X.); isszhfg@mail.sysu.edu.cn (F.Z.)

Received: 3 November 2019; Accepted: 7 December 2019; Published: 12 December 2019



**Abstract:** The smart meter is one of the most important components of the smart grid, which enables bi-directional communication between electric power providers and in-home appliances. However, the fine-grained metering mechanism that reports real-time electricity usage to the provider may result in some privacy and security issues for the owner of the smart meter. In this paper, we propose a new secure and anonymous smart metering scheme based on the technique of direct anonymous attestation and identity-based signatures. We utilize the trusted platform module to realize the tamper resistance of the smart meter. Moreover, our scheme is able to detect malfunctioning meters in which data is reported more than once in a time period. Finally, the performance and security results show that our proposed scheme is efficient and satisfies the security requirements of the smart grid communication system.

**Keywords:** privacy; security; direct anonymous attestation; identity-based signature; smart metering; smart grid

## 1. Introduction

Electrical energy is one of the most important factors for the advancement of industrial development, urbanization, and economic globalization of any country [1]. Nowadays, the problems of climate change and electrical energy consumption are becoming more and more serious. The globe is facing an energy crisis because of the steadily increasing demand for electrical energy as well as high emissions of carbon dioxide (CO<sub>2</sub>) [2]. Many countries in the world are seeking new technologies to develop renewable energies (derived from wind, sunlight, waters, etc) and to reduce CO<sub>2</sub> emissions and air pollution. Nevertheless, there also exists problems in dealing with the integration, system stability, and storage of different kinds of energy sources [3]. Fortunately, the emergence of smart grid techniques has provided solutions for such problems.

Smart grid, according to the studies [4–6], is a new generation of electric power grid infrastructure for improved efficiency, reliability, and safety, with smooth integration of renewable and alternative energy sources, through automated control and modern communications technologies. With the high development of industry 4.0 and the emergence of 5G mobile communications technology, the smart grid, which is concerned as an important part of Internet of Things and smart cities, has been playing an important role in people's daily lives.

In order to efficiently use the electric power resources and utilize different kinds of renewable energies, in recent years, many different kinds of distributed energy management systems have been proposed by researchers [7–10]. Such kinds of energy management systems can be applied in facilities that need two or more kinds of energy usage, such as airports, hospitals, and hotel buildings [11,12].

However, in the smart grid communication network, the smart meter's fine-grained metering mechanism, which reports real-time electricity usage to the utilities (the electricity providers or service providers), may result in privacy issues for the owner of the smart meter [13]. The inhabitants' behavioral patterns (e.g., the appliances they use, the time they wake up, take a shower, or leave home, etc.) can be deduced from the fine-grained meter readings [14,15]. Moreover, it is essential to guarantee data security and integrity any time that the meter data is stored in the smart meter or transmitted in the channel of the smart grid network.

Over the past decade, in order to preserve privacy and security in the smart grid network, many privacy-preserving smart metering schemes have been proposed by researchers [16–19]. The schemes can be classified into two large categories. The first category involves concealing fine-grained metering data using symmetric/public encryption [20,21], homomorphic encryption [22–25], identity-based signcryption [26], secure multiparty computation [27], and other data masking techniques such as noise addition [15,28] and using rechargeable batteries [29–31]. The other category involves hiding the identity of the smart meter utilizing anonymity techniques, such as group signatures [32,33], ring signatures [34], zero knowledge signatures [35,36], and other pseudonym techniques [37–39]. In order to prevent the meter data from being manipulated or altered by the meter owner, a tamper-resistant trusted platform module (TPM chip) is adopted by the smart meter [40]. However, in most of the solutions, although they claimed that the smart meter was embedded with a TPM chip [32,35], they did not split the smart meter into two entities: A TPM and a host platform (the meter). Since the TPM has limited bandwidth and computational capability, most of the operations should be calculated in the computing module of the meter. Later, Zhao et al. [34] realized this problem, and in their solution, the TPM and the smart meter work together to generate a signature. However, they use ring signatures, where the computational complexity of smart meters will increase linearly with the total number of members in a ring; thus, their scheme will be inefficient for large-scale smart meter scenarios.

To solve this problem, in this paper, we design a new privacy-preserving scheme for the smart grid communication network. We use a pairing-based direct anonymous attestation (DAA) signature [41] to realize a tamper-resistant anonymous signature for smart meters. The DAA signature is adopted in the TPM version 2.0 [42]. To alleviate the computational burden on the TPM chip, the host (the computation module of the smart meter) and the TPM chip will jointly generate the anonymous signature of the meter data. Moreover, the computational efficiency of smart meters will not be affected by the group members in the assigned domain in a data aggregator. Meanwhile, an efficient and provably secure identity-based signature (IBS) [43] is used by the data aggregator to guarantee the data integrity and secure transmission of aggregated metering data.

**Contributions:** We propose a scheme which utilizes an efficient pairing-based DAA to realize the tamper resistance and anonymous signatures in smart meters. Moreover, in order to avoid accidents caused by smart meters, our scheme is able to detect malfunctioning meters that report twice during a time period, and to revoke such kinds of smart meters. In addition, we use identity-based signatures to ensure the secure communication between the data aggregator and operation center. Finally, the security results show that our scheme satisfies the security requirements of smart grid communications, namely, correctness, data integrity, authenticity, anonymity, and traceability of malfunctioning meters. The experimental results show that our scheme is efficient and practical, especially in the signing of smart meters.

**Organization:** The rest of this paper is organized as follows. The next section introduces the methodology of our paper. In Section 3, we present the security and performance results of our scheme. Finally, the discussion and conclusions are respectively presented in Section 4 and Section 5.

## 2. Methodology

In this section, we introduce our methodology, which includes the cryptographic primitive, mathematical hard problem, system model, and detailed constructions of our proposed scheme. The notations used in our paper are described in Table 1.

**Table 1.** The notations used in the paper.

Notations	Descriptions
DAA	Direct anonymous attestation
IBS	Identity-based signature
SM	Smart meter
DA	Data aggregator
OC	Operation center
TPM	Trusted platform module
$SM_i$	The $i$ -th smart meter
$DA_j$	The $j$ -th data aggregator
$TPM_i$	The TPM chip embedded in $SM_i$
$ID_j$	The identity of $DA_j$
ms	millisecond
$n$	The total number of SMs in a domain
$m$	The total number of DAs
$\hat{e}$	Bilinear map
$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$	Multiplicative cyclic groups
$k$	The security parameter
$q$	Prime order of $\mathbb{G}_1$ and $\mathbb{G}_2$
$g_1$	A generator of $\mathbb{G}_1$
$g_2$	A generator of $\mathbb{G}_2$
$\psi$	A computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$
gsk	The system master key
gpk	The system public key
$f$	The secret key of the SM
$F$	The public key of the SM
$cre$	The credential of the SM
$H_1$	A secure hash function that $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$
$H_2$	A secure hash function that $H_2 : \{0, 1\}^* \rightarrow \mathbb{G}_1$
$H_3$	A secure hash function that $H_3 : \{0, 1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$
RL	The list of rogue/malfunctioning smart meters
TS	The current timestamp
$msg_i$	Metering data of $SM_i$
$M_j$	Aggregated meter data of $DA_j$
$SID_j$	Identity-based private key of $DA_j$
$M_{OC}$	The entire meter consumption of the OC
$J$	A base point of elliptic curve
$K$	Pseudonym of the SM
$T$	The blind credential of the SM
$\parallel$	Concatenation operation
$\{0, 1\}^l$	The set of all binary strings of length $l$
RSA	The public-key encryption algorithm
AES-256	The symmetric encryption–decryption algorithm
SHA-256	The hash function

### 2.1. Bilinear Maps

The DAA signature and IBS signature used in our scheme are based on an bilinear pairings. Let  $\mathbb{G}_1$  and  $\mathbb{G}_2$  be two multiplicative cyclic groups of prime order  $q$  with the generator  $g_1$  and  $g_2$ , respectively. We claim that  $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  is a bilinear map if it satisfies the following properties [43–45]:

- Bilinearity:  $\forall (g, h) \in \mathbb{G}_1 \times \mathbb{G}_2$ , and  $\forall a, b \in \mathbb{Z}_q^*$ ,  $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$ .
- Non-degeneracy:  $\forall g \in \mathbb{G}_1$ ,  $\hat{e}(g, h) = 1$  for all  $h \in \mathbb{G}_2$  iff  $g = 1_{\mathbb{G}_1}$ .
- Computability:  $\forall (g, h) \in \mathbb{G}_1 \times \mathbb{G}_2$ ,  $\hat{e}(g, h)$  is efficiently computable.
- There exists an efficient and publicly computable isomorphism  $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$  such that  $\psi(g_2) = g_1$ .

Then, the two groups  $(\mathbb{G}_1, \mathbb{G}_2)$  in the above are considered as a bilinear map pair.

## 2.2. Mathematical Problem

Our scheme is based on the  $q$ -Strong Diffie–Hellman Problem. To introduce this problem, we follow the description given by Boneh and Boyen [46]. Let  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  be the bilinear map groups of prime order  $q$  with two generators,  $g_1 \in \mathbb{G}_1$  and  $g_2 \in \mathbb{G}_2$ . The  $q$ -Strong Diffie–Hellman ( $q$ -SDH) problem in  $(\mathbb{G}_1, \mathbb{G}_2)$  is defined as follows: Given a  $(q+2)$ -tuple  $(g_1, g_2, g_2^x, g_2^{x^2}, \dots, g_2^{x^q})$  as input, the output is a pair  $(g_1^{1/(x+\alpha)}, \alpha)$  where  $\alpha \in \mathbb{Z}_q^*$ . An algorithm  $\mathcal{A}$  has advantage  $\epsilon$  in solving the  $q$ -SDH in  $(\mathbb{G}_1, \mathbb{G}_2)$  if

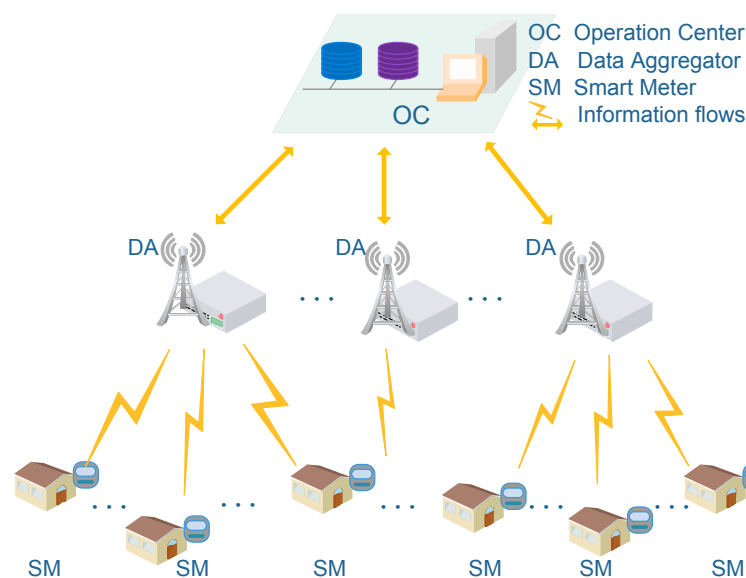
$$\Pr \left[ \mathcal{A}(g_1, g_2, g_2^x, \dots, g_2^{x^q}) = (1/(x + \alpha), \alpha) \right] \geq \epsilon, \quad (1)$$

where the probability is over the random choice of  $x$  in  $\mathbb{Z}_q^*$  and random bits consumed by  $\mathcal{A}$ .

We only introduce bilinear maps and the  $q$ -SDH problem here. For more detailed hard problems and detailed protocols of DAA and IBS, readers can refer to the references of DAA signatures [41] and IBS signatures [43].

## 2.3. System Model

In this paper, we adopt a three-level network model of a smart grid communication network according to [22,23,35]. As depicted in Figure 1, the system can be simply divided into three entities: Smart Meter (SM), Data Aggregator (DA), and Operation Center (OC). In our model, the OC covers  $m$  DAs, and each DA is assumed to be responsible for connecting  $n$  SMs. The detailed functionality of each entity is described as follows.



**Figure 1.** System model of the smart grid communication network.

**Smart Meter (SM):** The smart meter, which is located in its owner’s house, plays the role of metering the household’s electricity consumption and continuously transmitting the near-real-time metering data to the data aggregator in each time period. Meanwhile, in order to guarantee the security of an SM, a tamper-resistant TPM chip is installed in each SM by the manufacturer when the SM is made.

**Data Aggregator (DA):** The data aggregator is responsible for aggregating the electricity consumption of smart meters in its specific domain. It verifies the signatures sent from smart meters, and relays the aggregated data to the operation center.

**Operation Center (OC):** The operation center is the backbone of the smart grid network; it controls the whole system of the smart grid communication network. It communicates with DAs and SMs, and collects the data from DAs for meter data management.

In addition, the communication channel between SM and DA, which can use the technology of WiFi or 3G/4G/5G, is wireless. The connection between DA and OC is wired, and uses the technology of fiber communication networks.

#### 2.4. Construction of Our Proposed Scheme

This section presents our proposed secure and anonymous metering scheme. The scheme mainly consists of five phases: System initialization, membership registration, communications between the SM and DA, detection of malfunctioning meters, and communications between the DA and OC. The DAA signature is used in the communications between the SM and DA, while the IBS signature is used in the communications between the DA and OC. The detailed phases are described as follows.

##### 2.4.1. System Initialization

The system initialization is similar to that of DAA [41] and IBS [43]. We used the same parameters for the initialization of DAA and IBS, since the security of both signature protocols that we used is based on the same assumption (q-strong Diffie–Hellman assumption [46]) and the same bilinear map groups [45]. Given a security parameter  $k$ , the system is initialized by OC as follows.

1. Find a prime  $q > 2^k$ , and select an asymmetric bilinear group pair  $(\mathbb{G}_1, \mathbb{G}_2)$  of order  $q$  to satisfy a pairing function as follows:

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T, \quad (2)$$

along with the generators  $g_2 \in \mathbb{G}_2, g_1 = \psi(g_2) \in \mathbb{G}_1$ , where  $\psi$  is a computable isomorphism from  $\mathbb{G}_2$  to  $\mathbb{G}_1$ .

2. Choose  $\xi_1, \xi_2 \leftarrow \mathbb{G}_1$  and select a system master key  $s \leftarrow \mathbb{Z}_q^*$ ; compute a system public key  $\eta$  where

$$\eta := g_2^s. \quad (3)$$

3. Select secure hash functions  $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*, H_2 : \{0, 1\}^* \rightarrow \mathbb{G}_1, H_3 : \{0, 1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$ .

4. Pre-compute the following pairings:

$$\theta_1 = \hat{e}(g_1, g_2), \quad (4)$$

$$\theta_2 = \hat{e}(\xi_1, g_2), \quad (5)$$

$$\theta_3 = \hat{e}(\xi_2, g_2), \quad (6)$$

$$\theta_4 = \hat{e}(\xi_2, \eta). \quad (7)$$

5. Output the system public key and master key

$$gpk = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, \hat{e}, g_1, g_2, \xi_1, \xi_2, \eta, H_1, H_2, H_3, \theta_1, \theta_2, \theta_3, \theta_4\} \quad (8)$$

$$gsk = s. \quad (9)$$

##### 2.4.2. Membership Registration

The membership registration includes smart meter registration and data aggregator registration. We assume that all of the registrations are executed through a secure channel.

###### A. Smart Meter Registration

This is a protocol between the SM and OC. In our model, the smart meter consists of two main components: A host (meter) and a tamper-resistant module (TPM chip). In order to protect the sensitive information of the SM, any operation related to the smart meter's secret key should be calculated in the TPM chip. When a valid smart meter  $SM_i$  ( $i = 1, 2, \dots, n$ ) registers itself into the system, it will finally get a legal DAA credential from the OC, which is shown in Figure 2. In the original DAA scheme [41], the credential is issued by the issuer. The issuer can be the manufacturer, the third party service

provider, or the electricity authority. In this paper, we assume that the credential is issued by the OC. Finally, the credential can be further used for anonymously signing the meter data. The protocol proceeds as follows.

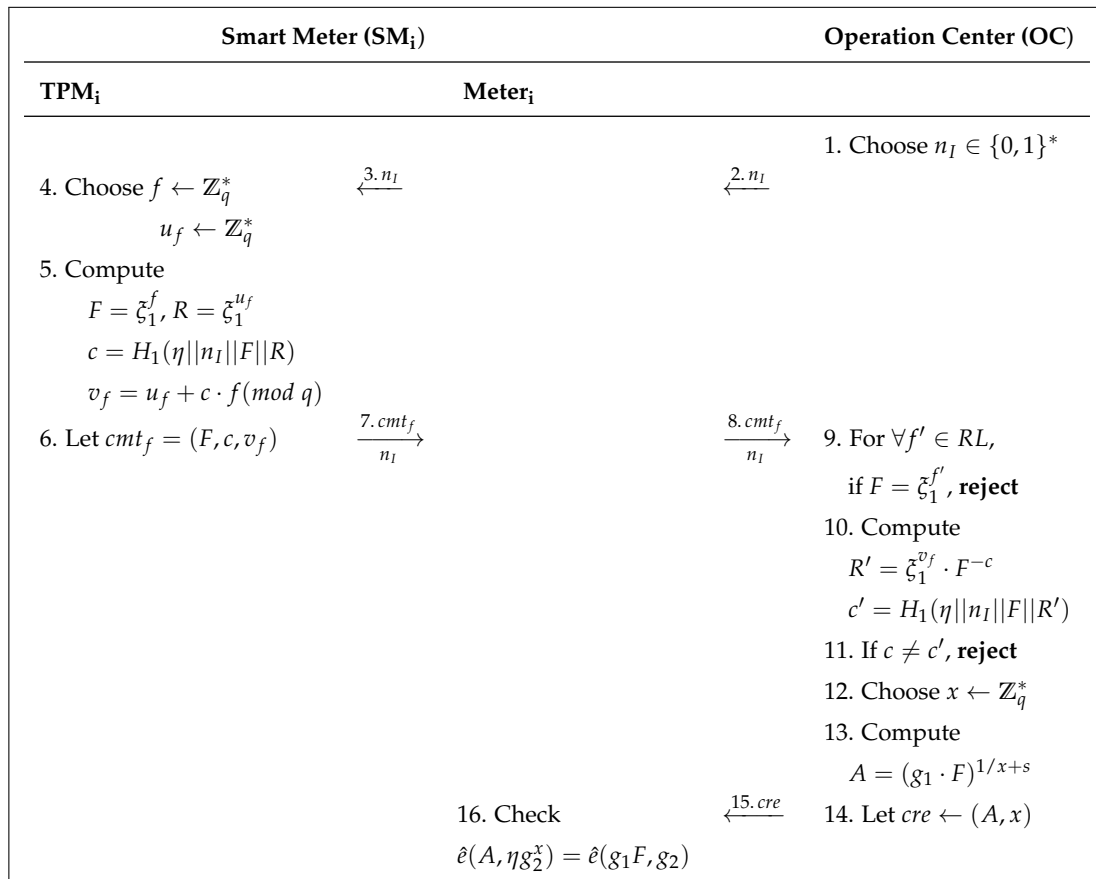


Figure 2. Membership registration of smart meter.

1. The OC randomly chooses a nonce  $n_I \in \{0, 1\}^*$  and sends  $n_I$  to SM<sub>i</sub>.
2. The TPM<sub>i</sub> in the smart meter selects a secret key  $f \leftarrow \mathbb{Z}_q^*$ , and computes the associated public key

$$F = \zeta_1^f. \tag{10}$$

Then, the TPM<sub>i</sub> makes a zero-knowledge proof [47] to prove that the TPM<sub>i</sub> owns the secret key  $f$ , i.e.,

$$PK\{(f) : \zeta_1^f = F\}. \tag{11}$$

Finally, the TPM<sub>i</sub> sends the proof message,  $cmt_f$  and  $n_I$ , to the OC.

3. Upon receiving the  $cmt_f$  and  $n_I$ , the OC checks  $F$  against the  $RL$  to verify the correctness of  $cmt_f$ .  $RL$  is a rogue list, which is set to be empty at the system setup, and will contain the invalid secret key  $f'$  of malfunctioning or rogue smart meters. Then, the OC computes a credential  $cre$  by calculating:

$$A = (g_1 \cdot F)^{1/x+s}. \tag{12}$$

$A$  is a signature on the public key  $F$  (therefore on  $f$ ). Then, the OC sends  $cre = (A, x)$  to SM<sub>i</sub>.

4. SM<sub>i</sub> verifies the correctness of the credential  $cre$  such that

$$\hat{e}(A, \eta g_2^x) = \hat{e}(g_1 F, g_2). \tag{13}$$

Thus, SM<sub>i</sub> gets a membership credential  $cre$  on its secret key  $f$ .

## B. Data Aggregator Registration

When a data aggregator  $DA_j$  ( $j = 1, 2, \dots, m$ ) registers itself into the system, the OC computes the identity-based private key  $S_{ID_j}$  for each of them as follows:

$$S_{ID_j} = g_1^{1/(s+H_1(ID_j))}, \quad (14)$$

where  $ID_j$  is a unique identity string of  $ID_j$  and  $s$  is the system master key. Then, the OC sends  $S_{ID_j}$  to each  $DA$  through a secure channel.

### 2.4.3. Communications between the SM and DA

The mutual communications contain the meter data signing protocol in the SM and verification algorithm in the DA.

#### A. The Signing Protocol

This is a protocol performed by  $SM_i$  to produce an anonymous signature on fine-grained metering data. On input of the system public key  $gpk$ , membership credential  $cre = (A, x)$ , membership key  $f$ , meter data  $msg_i$ ,  $Meter_i$  and  $TPM_i$  in  $SM_i$  jointly run the signing protocol. Since meter data should be uploaded to  $DA_j$  without revealing the smart meter's identity ( $f$ ,  $F$ , and  $cre$ ), the smart meter needs to prove the knowledge of  $f$  and  $cre$  ( $F$  is not used in this phase, so we do not need to prove the knowledge of it).

The protocol is depicted in Figure 3, which is similar to the sign protocol of the DAA scheme [41]. Firstly, to allow  $DA_j$  to verify the identity of  $SM_i$  and recognize the malfunctioning/rogue smart meter,  $SM_i$  needs to generate a pseudonym  $K$  instead of public key  $F$  and a proof of knowledge that the pseudonym is generated by its own valid secret key  $f$ , where

$$K = J^f, \quad (15)$$

$$J = H_2(TS || msg_i), \quad (16)$$

where  $TS$  is a timestamp and  $msg_i$  is meter data generated in a timestamp. If  $(J, K)$  is generated more than one time in a time period, the smart meter will be linked; the details will be illustrated in Section 2.4.4 (Malfunctioning Meter Detection). Then,  $SM_i$  needs to compute a blind credential  $T$  as follows:

$$T = A \cdot \zeta_2^a, \quad (17)$$

where  $a \leftarrow \mathbb{Z}_q^*$ . Also,  $SM_i$  needs to provide a proof of knowledge that  $T$  is a blind credential on a valid secret key  $f$ . Finally, using the method of the Fiat–Shamir heuristic [48,49],  $SM_i$  and  $TPM_i$  jointly generate a signature of proof of knowledge

$$\text{SPK}\{(x, f, a) : \hat{e}(T, g_2)^x \cdot \hat{e}(\zeta_1, g_2)^f \cdot \hat{e}(\zeta_2, g_2)^{ax} \cdot \hat{e}(\zeta_2, \eta)^a = \hat{e}(T, \eta) / \hat{e}(g_1, g_2)\}(msg_i). \quad (18)$$

The detailed signature is shown in Figure 3. Finally,  $SM_i$  outputs the signature

$$\sigma_i = (J, K, T, c, TS, n_t, v_f, v_x, v_a, v_b), \quad (19)$$

and sends  $(msg_i, \sigma_i)$  to the data aggregator  $DA_j$ .

TPM <sub>i</sub>		Meter <sub>i</sub>
		1. Let $TS, msg_i \in \{0, 1\}^*$
4. Choose $u_f \leftarrow \mathbb{Z}_q^*$	$\xleftarrow{3. J, TS}$	2. Compute $J = H_2(TS    msg_i)$
5. Compute $K = J^f$ $R_1 = J^{u_f}$ $R_{2T} = \zeta_1^{u_f}$	$\xrightarrow{6. K, R_1, R_{2T}}$	7. Choose $u_x, u_a, u_b, a \leftarrow \mathbb{Z}_q^*$
		8. Compute $b = a \cdot x \pmod q$ $T = A \cdot \zeta_2^a$ $R_2 = \hat{e}(T, g_2)^{-u_x} \cdot \hat{e}(\zeta_1, g_2)^{u_f}$ $\quad \cdot \hat{e}(\zeta_2, g_2)^{u_b} \cdot \hat{e}(\zeta_2, \eta)^{u_a}$ $\quad = \hat{e}(R_{2T} \cdot T^{-u_x} \cdot \zeta_2^{u_b}, g_2) \cdot \theta_4^{u_a}$
10. Choose $n_t \in \{0, 1\}^*$	$\xleftarrow{9. c_h, msg_i}$	$c_h = H_1(\eta    J    K    T    R_1    R_2)$
11. Compute $c = H_1(c_h    TS    n_t    msg_i)$ $v_f = u_f + c \cdot f \pmod q$	$\xrightarrow{12. c, v_f, n_t}$	13. Compute $v_x = u_x + c \cdot x \pmod q$ $v_a = u_a + c \cdot a \pmod q$ $v_b = u_b + c \cdot b \pmod q$
		14. Let $\sigma_i \leftarrow (J, K, T, c, TS, n_t, v_f, v_x, v_a, v_b)$

Figure 3. The signing protocol of the smart meter.

## B. The Verification Algorithm

Upon receiving the anonymous signature  $\sigma_i$  and message  $msg_i$  from  $SM_i$ ,  $DA_j$  runs a verification algorithm to check the validity of  $SM_i$ 's signature  $\sigma_i$ . Firstly,  $DA_j$  checks if the pseudonym  $K$  is generated by an invalid  $f'$  in the rogue list. Then,  $DA_j$  checks if  $\sigma_i$  does prove the knowledge of a secret key  $f$  and knowledge of a valid membership credential  $cre$  on the same  $f$ . The detailed algorithm is described in Figure 4, which is identical to that in the DAA scheme [41]. However, in our algorithm, we check the validity of  $TS$  and  $J$  at the beginning. If  $\sigma_i$  is correct and valid,  $DA_j$  accepts the meter data  $msg_i$ .

However, before uploading all of the meters' electricity consumptions to the operation center,  $DA_j$  needs to perform a phase of detection of malfunctioning meters. If all of the meter data are honestly uploaded by the smart meters, this phase will be ignored.

<p><b>Input:</b> <math>gpk, msg_i, \sigma_i = (J, K, T, c, TS, n_t, v_f, v_x, v_a, v_b)</math></p> <p><b>Output:</b></p> <ol style="list-style-type: none"> <li>1. If <math>TS</math> is not a valid timestamp, or <math>J \neq H_2(TS    msg_i)</math>, return <b>reject</b></li> <li>2. If <math>K = J^{f'}</math> for all <math>f' \in RL</math>, return <b>reject</b></li> <li>3. Compute <math>\hat{R}_1 = J^{v_f} \cdot K^{-c}</math>, <math>\hat{R}_2 = \hat{e}(T, g_2^{-v_x} \cdot \eta^{-c}) \cdot \theta_1^c \cdot \theta_2^{v_f} \cdot \theta_3^{v_b} \cdot \theta_4^{v_a}</math></li> <li>4. If <math>c \neq H_1(H_1(\eta    J    K    T    \hat{R}_1    \hat{R}_2)    TS    n_t    msg_i)</math>, return <b>reject</b></li> <li>5. Otherwise, return <b>accept</b></li> </ol>
--

Figure 4. The verification algorithm of the data aggregator.



#### 2.4.4. Malfunctioning Meter Detection

Malfunctioning meter detection includes two phases: The linking algorithm and the tracing protocol. The linking algorithm is to check if there exists a smart meter signing a message more than once in a time period. If any two signatures are linked, the tracing protocol will help to identify the linked smart meter.

##### A. The Linking Algorithm

This algorithm is run by  $DA_j$ . When  $DA_j$  receives all of the meter data  $\{msg_i\}_{i=1}^n$  from  $SM_i$  ( $i = 1, 2, \dots, n$ ) at a time period  $TS$ , it needs to check if there exists a smart meter signing a message more than once in a time period  $TS$ . If so, this smart meter may be malfunctioning, and we need to identify this meter. Firstly,  $DA_j$  collects all of the messages and signatures generated in a time period  $TS$ . If there exist two identical messages ( $msg_0 = msg_1$ ),  $DA_j$  runs the linking algorithm in Figure 5, and it is similar to the linking algorithm of the DAA scheme [41]. Otherwise, if there are no identical messages, this step as well as the next step are stopped.

**Input:**  $(msg_b, \sigma_b), b = 0, 1$   
**Output:**  
 1. If  $TS_0 \neq TS_1$ , or  $msg_0 \neq msg_1$ , or  $J_0 \neq J_1$ , return  $\perp$   
 2. If **reject**  $\leftarrow Verify(m_b, \sigma_b)$ , return  $\perp$   
 3. If  $J_0 = J_1$  and  $K_0 = K_1$  and  $msg_0 = msg_1$  and  $TS_0 = TS_1$ , return **linked**  
 4. Otherwise return **unlinked**

Figure 5. The linking algorithm for malfunctioning smart meters.

##### B. The Tracing Protocol

After the linking phase, if  $DA_j$  finds out that a suspected pair  $(J_R, K_R)$  was generated more than once in a time period, it will ask  $SM_i$  ( $i = 1, 2, \dots, n$ ) for proof of knowledge that it did not generate  $(J_R, K_R)$  before.  $SM_i$  needs to prove that its secret key  $f_i \neq \log_{J_R} K_R$ , and computes a zero-knowledge proof that

$$PK\{(f_i) : K_i = J_i^{f_i} \wedge K_R \neq J_R^{f_i}\}. \quad (20)$$

We use the zero-knowledge proof protocol designed by Camenisch and Shoup [50] for proving that two discrete logarithms are not equal. The method is as follows. The prover (the smart meter  $SM_i$ ) and verifier (the tracer, which can be the OC) have common inputs  $J_i, K_i, J_R, K_R \in G_1$ , where  $\log_{J_i} K_i \neq \log_{J_R} K_R$ .  $SM_i$  has an additional input  $f_i$ , as follows:

$$f_i = \log_{J_i} K_i. \quad (21)$$

Then,  $SM_i$  shows proof to the tracer with the following steps.

1.  $SM_i$  selects  $\iota \leftarrow \mathbb{Z}_q^*$  and computes  $\tau$  by

$$\tau = \iota \cdot f_i. \quad (22)$$

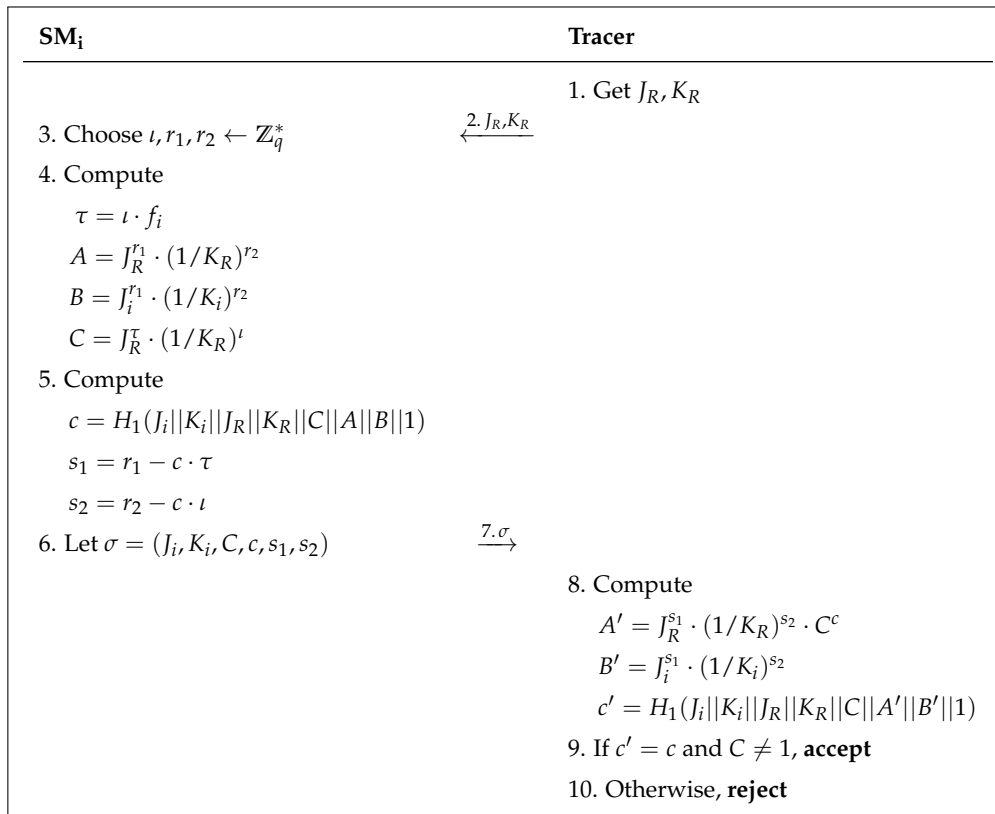
2.  $SM_i$  executes the proof of knowledge that

$$PK\{(\tau, \iota) : C = J_R^\tau \cdot (1/K_R)^\iota \wedge 1 = J_i^\tau \cdot (1/K_i)^\iota\} \quad (23)$$

and sends the result to the tracer.

3. The tracer accepts that the smart meter is not a malfunctioning one if it accepts in step 2. Otherwise, the tracer rejects the meter, and ensures that the present  $SM_i$  is the malfunctioning smart meter.

The detailed proof is shown in Figure 6. The malfunctioning smart meter will be revoked and replaced by the electricity provider.



**Figure 6.** The tracing protocol for malfunctioning smart meters.

#### 2.4.5. Communications between the DA and OC

After the phases of verification and malfunctioning meter detection, the data collector DA<sub>j</sub> collects the meter data at the same timestamp sent from the smart meters in its domain area, and calculates the aggregated electricity consumptions  $M_j$  as follows:

$$M_j = \sum_{i=1}^n msg_i. \quad (24)$$

Then, the DA<sub>j</sub> securely reports the aggregated meter data to the OC using the identity-based signature [43].

##### A. Signing

Using the identity-based private key  $S_{ID_j}$ , DA<sub>j</sub> signs the aggregated meter data  $M_j$  as follows. It picks up a random value  $\mu \leftarrow \mathbb{Z}_q^*$ , and computes the following equations:

$$v = \theta_1^\mu, \quad (25)$$

$$h = H_3(M_j || ID_j || TS, v) \in \mathbb{Z}_q^*, \quad (26)$$

$$\mathcal{S} = S_{ID_j}^{(\mu+h)}, \quad (27)$$

where  $TS$  is the current timestamp.

Then, the signature on  $M_j$  is  $\sigma_j = (h, \mathcal{S}) \in \mathbb{Z}_q^* \times G_1$ . Finally, DA<sub>j</sub> forwards  $(\sigma_j, M_j, ID_j, TS)$  to the OC.

## B. Verification

After receiving  $(\sigma_j, M_j, ID_j, TS)$  from each data aggregator  $DA_j$  ( $j = 1, 2, \dots, m$ ), the OC will check if the sender is valid. It verifies the validity of  $ID_j$  and  $TS$  and checks the correctness of the message signature by computing

$$\tilde{h} = H_3(M_j, \hat{e}(\mathcal{S}, g_2^{H_1(ID_j)} \cdot \eta) \cdot \theta_1^{-h}). \quad (28)$$

If  $\tilde{h} = h$ , the OC accepts the message  $M_j$ .

Lastly, the OC computes the entire meter consumption  $M_{OC}$ , where

$$M_{OC} = \sum_{j=1}^m M_j. \quad (29)$$

Then, the OC receives the meter consumptions of the whole smart grid network at timestamp  $TS$ .

## 3. Results

In this section, we present the results of our study, which contain the security results and performance results.

### 3.1. Security Results

In this section, we show that our proposed secure and anonymous metering scheme achieves the security requirements of correctness and data integrity, as well as authenticity, anonymity, and traceability.

1. **Correctness:** According to the verification procedures in our proposed security protocol, the anonymous signature generated by a valid smart meter and the signature generated by an honest data aggregator can surely pass the verification.
2. **Data Integrity and Authenticity:** The properties of integrity and authenticity require that the entity in the communications should be a valid registered membership, and that no attackers could tamper with or forge the data generated by the entity. In our scheme, all of the smart meters are equipped with a tamper-resistant TPM chip, which prevents meter data from being altered by the attacker. Meanwhile, secure DAA and IBS protocols are used in our scheme to ensure the authenticity. Without valid credentials, a smart meter cannot successfully sign the meter data or forge a valid signature. In addition, without a valid identity-based secret key, a fake data aggregator cannot produce a valid signature that can pass the verification by the operation center. Thus, our scheme satisfies data integrity and authenticity concerns.
3. **Anonymity:** Anonymity is the privacy requirement of our scheme. It requires that each valid signature is unable to expose any of the information of the signer, and no one can distinguish whether two normal signatures are generated by the same signer. In fact, as described in Section 2.4.3, during the data upload,  $SM_i$  hides its credential and uses a pseudonym  $K$  instead of the real identity  $F$ ; as a result, no adversary can recognize the identity of the data owner. Meanwhile, for any two different pairs  $(J_1, K_1)$  and  $(J_2, K_2)$  in signatures  $(\sigma_1, \sigma_2)$ , if the adversary can determine whether they are generated by the same  $SM_i$  (i.e., determine whether  $f_1 = f_2$ , where  $f_1 = \log_{J_1} K_1$ ,  $f_2 = \log_{J_2} K_2$ ), then it will break the decisional Diffie–Hellman (DDH) problem [51]. Thus, our scheme satisfies the requirement of anonymity.
4. **Malfunctioning Meter Traceability:** As presented in Section 2.4.4, our scheme has the property of malfunctioning meter detection. If any two signatures are dishonestly generated by the SM, i.e., the SM signs a message twice in a time period—even though two such signatures can pass the verification—they can be linked and traced by the utilities.

### 3.2. Performance Results

In this section, we evaluate the computational cost of our proposed scheme, and compare the performance with Zhao et al.'s scheme [34].

To analyze our scheme, we mainly focus on six cost-expensive operations: Pairing, exponentiation, scalar multiplication, the map-to-point function, the hash function, and symmetric encryption/decryption. Other lightweight operations such as concatenation and modular addition are ignored due to their high efficiency.

The security level for the RSA public-key encryption algorithm in [34] is 1024 bits. In order to achieve the approximate cryptographic security level, in our scheme, we use the 80-bit security level elliptic curves (MNT curves) introduced in [52,53] by selecting a 170-bit prime  $q$ , with an embedding degree of 6.

The experiments were conducted on a personal computer with the Intel(R) Core(TM) i7-7820X CPU 3.60GHz and 16 GB memory. All of the operations were executed on a GNU Compiler Collection (version 7.1) with the Pairing-Based Cryptography library (PBC-0.5.14) and Openssl crypto library (version 1.1.1).

To simulate the scheme of [34], we adopted the AES-256 as the symmetric encryption–decryption algorithm and the SHA-256 as the hash function. For convenience, some notations are defined in the following list, and the average running time of each operation is presented in Table 2.

**Table 2.** The average execution time of operations (ms).

$T_{pr}$	$T_{mul}$	$T_{exp}$	$T_{hp}$	$T_{sym}$	$T_H$
1.238	0.325	0.286	0.029	0.00779	0.00198

- $T_{pr}$ : The execution time of a bilinear pairing operation  $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ .
- $T_{mul}$ : The execution time of a scalar multiplication in  $\mathbb{G}_1, \mathbb{G}_2$ .
- $T_{exp}$ : The execution time of a modular exponentiation operation.
- $T_{hp}$ : The execution time of the map-to-point function in  $\mathbb{G}_1$ .
- $T_{sym}$ : The execution time of symmetric encryption or decryption.
- $T_H$ : The execution time of the hash function.

Table 3 presents the comparisons with the scheme [34] on the computational cost of communications between the SM and DA. Since in [34], a protocol between the DA and OC was not designed, in Table 4, we only present the computational cost for the communications between the DA and OC in our scheme.

**Table 3.** Comparisons of computational cost for the communications between the SM and DA.

Scheme	Cost on SM	Time (ms)	Cost on DA	Time (ms)
[34]	$(t^1 + 3)T_{exp} + t \times T_{sym} + 3T_H$	$\approx 0.2938t + 0.8639$	$3T_{exp} + 2T_H$	$\approx 0.862$
Ours	$1T_{pr} + 6T_{mul} + 1T_{exp} + 3T_{hp}$	$\approx 3.561$	$1T_{pr} + 4T_{mul} + 4T_{exp} + 3T_{hp}$	$\approx 3.769$

<sup>1</sup>  $t$  is the ring size (total number of SMs) in [34].  $t$  is set to be 10, 50, and 100. When  $t = 10$ , the cost on the SM is 3.802 ms; when  $t = 50$ , the cost on the SM is 15.549 ms; when  $t = 100$ , the cost on the SM is 30.243 ms.

**Table 4.** Computational cost of the communications between the DA and OC.

Cost on DA	Time (ms)	Cost on OC	Time (ms)
$2T_{mul} + 1T_{exp} + 2T_{hp}$	$\approx 0.994$	$1T_{pr} + 1T_{mul} + 1T_{exp} + 2T_{hp}$	$\approx 1.907$

In Table 3, we can see that, for the communications between the SM and DA, the smart meter needs to calculate  $1T_{pr} + 6T_{mul} + 1T_{exp} + 3T_{hp}$  operations in our scheme, while  $(t + 3)T_{exp} + t \times T_{sym} + 3T_H$  operations are computed in that of [34]. The computational complexity of the smart meter

in [34] depends on the ring size  $t$  (i.e., the total number of smart meters in a domain). In this case, the execution time of the smart meter will increase linearly with the growing number of smart meters in a ring. In the real world, the number of smart meters in a domain belonging to a data aggregator will be at least 10. Most of the time, the average number of smart meters can be 50 or even 100. This means that when  $t = 10 \sim 100$ , for each metering, the execution time of a SM in [34] will be at least 3.802 ms and at most 15.549 ms. However, in our scheme, the smart meter only need to spend 3.561 ms for each signing on the metering data. Therefore, for the same purpose of anonymous signatures based on TPM chips, our scheme has an advantage in the computational efficiency on the side of the smart meter. However, as shown in Table 3, our scheme has a drawback, in that the computational complexity in the DA is larger than that in [34]. Even so, this kind of disadvantage is not fatal. In the communications of a smart grid network, the efficient calculation complexity in the smart meter is more important than in the aggregator, since the aggregator has more powerful computational abilities than those of the smart meter.

#### 4. Discussion

In our study, in order to design a tamper-resistant metering scheme, a trusted platform module (TPM chip) is embedded in each smart meter. The TPM is a trusted hardware module which is developed by the Trusting Computing Group (TCG). One of the goals of the TPM is to provide anonymous authentication with a remote verifier [54]. In the earlier version of the TPM, a privacy certification authority (Privacy CA) was adopted by TCG to act as a trusted third party to authenticate the TPM. However, in this solution, it was later found that the real identity of the TPM can be revealed with the help of the Privacy CA. Then, version 1.2 of the TPM Specification [55], the direct anonymous attestation (DAA) [54] was adopted. The construction of DAA prevents the leakage of the real identity of the TPM when anonymously signing a message. Later, the pairing-based DAA [41] was adopted in the TPM 2.0 Specification [56], which further reduced TPM resources; since the TPM has limited computational capacity, most of the operations should be calculated in the host of the TPM. In our paper, we use the property of strong anonymity of DAA to design an anonymous metering scheme. Though the TPM has the disadvantage that the capacity of storage and computation is limited, in our scheme, most of the operations are done in the smart meter (the host of the TPM). Meanwhile, in [34], Zhao et al. also shows that a TPM with cryptography primitives can be used to design a tamper-resistant smart meter. Therefore, our proposed smart metering scheme is practical.

#### 5. Conclusions

In this paper, we propose a secure and anonymous smart metering scheme based on direct anonymous attestation (DAA) and identity-based signature schemes. Like many other works, the smart meter is equipped with a TPM chip to store the secret key and execute the anonymous signing of metering data using a DAA signature. However, on account of the limited capacity of the TPM, we divide the signer into two parts (the TPM and the host, i.e., the smart meter). We secure the communications between the data aggregator and the operation center by using identity-based signatures. We show that our scheme satisfies the properties of correctness, data integrity and authenticity, and anonymity. Moreover, our scheme is able to detect malfunctioning smart meters. The experimental results show that our scheme is efficient and practical. In our further work, we will consider how to improve the efficiency of verification in the data aggregator, and design a more secure and efficient metering scheme for smart grid communications.

**Author Contributions:** Conceptualization, F.Z.; Data curation, S.X. and H.L.; Formal analysis, S.X. and Y.T.; Funding acquisition, F.Z.; Investigation, S.X. and F.Z.; Methodology, S.X. and F.Z.; Project administration, F.Z.; Resources, S.X. and H.L.; Software, H.L. and Y.T.; Supervision, F.Z.; Validation, S.X., H.L., and Y.T.; Writing—original draft, S.X.; Writing—review & editing, S.X. and F.Z.

**Funding:** This research was funded by the National Key R&D Program of China (2017YFB0802500) and the National Natural Science Foundation of China (No. 61672550 and No. 61972429).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Khan, M.W.; Wang, J.; Ma, M.; Xiong, L.; Li, P.; Wu, F. Optimal energy management and control aspects of distributed microgrid using multi-agent systems. *Sustain. Cities Soc.* **2019**, *44*, 855–870. [[CrossRef](#)]
2. Khan, M.W.; Wang, J.; Xiong, L.; Ma, M. Modelling and optimal management of distributed microgrid using multi-agent systems. *Sustain. Cities Soc.* **2018**, *41*, 154–169. [[CrossRef](#)]
3. Gungor, V.C.; Lu, B.; Hancke, G.P. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3557–3564. [[CrossRef](#)]
4. Amin, S.M.; Wollenberg, B.F. Toward a smart grid: Power delivery for the 21st century. *IEEE Power Energy Mag.* **2005**, *3*, 34–41. [[CrossRef](#)]
5. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [[CrossRef](#)]
6. Cecati, C.; Citro, C.; Piccolo, A.; Siano, P. Smart operation of wind turbines and diesel generators according to economic criteria. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4514–4525. [[CrossRef](#)]
7. Belvedere, B.; Bianchi, M.; Borghetti, A.; Nucci, C.A.; Paolone, M.; Peretto, A. A microcontroller-based power management system for standalone microgrids with hybrid power supply. *IEEE Trans. Sustain. Energy* **2012**, *3*, 422–431. [[CrossRef](#)]
8. Mashayekh, S.; Stadler, M.; Cardoso, G.; Heleno, M. A mixed integer linear programming approach for optimal DER portfolio, sizing, and placement in multi-energy microgrids. *Appl. Energy* **2017**, *187*, 154–168. [[CrossRef](#)]
9. Klaimi, J.; Rahim-Amoud, R.; Merghem-Boulahia, L.; Jrad, A. A novel loss-based energy management approach for smart grids using multi-agent systems and intelligent storage systems. *Sustain. Cities Soc.* **2018**, *39*, 344–357. [[CrossRef](#)]
10. Liu, G.; Jiang, T.; Ollis, T.B.; Zhang, X.; Tomsovic, K. Distributed energy management for community microgrids considering network operational constraints and building thermal dynamics. *Appl. Energy* **2019**, *239*, 83–95. [[CrossRef](#)]
11. De Rubeis, T.; Nardi, I.; Paoletti, D.; Di Leonardo, A.; Ambrosini, D.; Poli, R.; Sfarra, S. Multi-year consumption analysis and innovative energy perspectives: The case study of Leonardo da Vinci International Airport of Rome. *Energy Convers. Manag.* **2016**, *128*, 261–272. [[CrossRef](#)]
12. Isa, N.M.; Tan, C.W.; Yatim, A. A comprehensive review of cogeneration system in a microgrid: A perspective from architecture and operating system. *Renew. Sustain. Energy Rev.* **2018**, *81*, 2236–2263. [[CrossRef](#)]
13. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45. [[CrossRef](#)]
14. Lisovich, M.A.; Mulligan, D.K.; Wicker, S.B. Inferring personal information from demand-response systems. *IEEE Secur. Priv.* **2010**, *8*, 11–20. [[CrossRef](#)]
15. Barbosa, P.; Brito, A.; Almeida, H. Defending against load monitoring in smart metering data through noise addition. In Proceedings of the 30th Annual ACM Symposium on Applied Computing, Salamanca, Spain, 13–17 April 2015; pp. 2218–2224.
16. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambbotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 21–38. [[CrossRef](#)]
17. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [[CrossRef](#)]
18. Pillitteri, V.Y.; Brewer, T.L. *Guidelines for Smart Grid Cybersecurity*; NIST Interagency/Internal Report (NISTIR)-7628 Rev 1; NIST: Gaithersburg, MD, USA, 2014.
19. De Oliveira, F.B. *On Privacy-Preserving Protocols for Smart Metering Systems*; Springer: Berlin, Germany, 2015.
20. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X.S. A lightweight message authentication scheme for smart grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685. [[CrossRef](#)]
21. Chim, T.W.; Yiu, S.M.; Li, V.O.; Hui, L.C.; Zhong, J. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 85–97.

22. Li, H.; Lin, X.; Yang, H.; Liang, X.; Lu, R.; Shen, X. EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 2053–2064. [[CrossRef](#)]
23. Jo, H.J.; Kim, I.S.; Lee, D.H. Efficient and privacy-preserving metering protocols for smart grid systems. *IEEE Trans. Smart Grid* **2015**, *7*, 1732–1742. [[CrossRef](#)]
24. Liu, Y.; Guo, W.; Fan, C.L.; Chang, L.; Cheng, C. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. *IEEE Trans. Ind. Informatics* **2018**, *15*, 1767–1774. [[CrossRef](#)]
25. Xue, K.; Yang, Q.; Li, S.; Wei, D.S.; Peng, M.; Memon, I.; Hong, P. PPSO: A privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid. *IEEE Internet Things J.* **2018**, *6*, 2486–2496. [[CrossRef](#)]
26. Zhang, S.; Zheng, T.; Wang, B. A privacy protection scheme for smart meter that can verify terminal's trustworthiness. *Int. J. Electr. Power Energy Syst.* **2019**, *108*, 117–124. [[CrossRef](#)]
27. Mustafa, M.A.; Cleemput, S.; Aly, A.; Abidin, A. A secure and privacy-preserving protocol for smart metering operational data collection. *IEEE Trans. Smart Grid* **2019**, *10*, 6481–6490. [[CrossRef](#)]
28. Barbosa, P.; Brito, A.; Almeida, H.; Clauß, S. Lightweight privacy for smart metering data by adding noise. In Proceedings of the 29th Annual ACM Symposium on Applied Computing, Gyeongju, Korea, 24–28 March 2014; pp. 531–538.
29. McLaughlin, S.; McDaniel, P.; Aiello, W. Protecting consumer privacy from electric load monitoring. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 87–98.
30. Zhao, J.; Jung, T.; Wang, Y.; Li, X. Achieving differential privacy of data disclosure in the smart grid. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 504–512.
31. Zhu, L.; Zhang, Z.; Qin, Z.; Weng, J.; Ren, K. Privacy protection using a rechargeable battery for energy consumption in smart grids. *IEEE Netw.* **2016**, *31*, 59–63. [[CrossRef](#)]
32. Zargar, S.H.M.; Yaghmaee, M.H. Privacy preserving via group signature in smart grid. In Proceedings of the Electric Industry Automation Congress (EIAC), Mashhad, Iran, 13–14 February 2013.
33. Kishimoto, H.; Yanai, N.; Okamura, S. An Anonymous Authentication Protocol for the Smart Grid. In *Smart Micro-Grid Systems Security and Privacy*; Springer: Berlin, Germany, 2018; pp. 29–52.
34. Zhao, J.; Liu, J.; Qin, Z.; Ren, K. Privacy protection scheme based on remote anonymous attestation for trusted smart meters. *IEEE Trans. Smart Grid* **2016**, *9*, 3313–3320. [[CrossRef](#)]
35. Diao, F.; Zhang, F.; Cheng, X. A privacy-preserving smart metering scheme using linkable anonymous credential. *IEEE Trans. Smart Grid* **2014**, *6*, 461–467. [[CrossRef](#)]
36. Gong, Y.; Cai, Y.; Guo, Y.; Fang, Y. A privacy-preserving scheme for incentive-based demand response in the smart grid. *IEEE Trans. Smart Grid* **2015**, *7*, 1304–1313. [[CrossRef](#)]
37. Efthymiou, C.; Kalogridis, G. Smart grid privacy via anonymization of smart metering data. In Proceedings of the First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 238–243.
38. Stegelmann, M.; Kesdogan, D. Gridpriv: A smart metering architecture offering k-anonymity. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 419–426.
39. Finster, S.; Baumgart, I. Pseudonymous smart metering without a trusted third party. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Melbourne, VIC, Australia, 16–18 July 2013; pp. 1723–1728.
40. LeMay, M.; Gross, G.; Gunter, C.A.; Garg, S. Unified architecture for large-scale attested metering. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 3–6 January 2007; p. 115.
41. Brickell, E.; Li, J. A pairing-based DAA scheme further reducing TPM resources. In Proceedings of the International Conference on Trust and Trustworthy Computing, Berlin, Germany, 21–23 June 2010; pp. 181–195.
42. Chen, L.; Li, J. Flexible and scalable digital signatures in TPM 2.0. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 37–48.

43. Barreto, P.S.; Libert, B.; McCullagh, N.; Quisquater, J.J. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, 4–8 December 2005; pp. 515–532.
44. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
45. Boneh, D.; Boyen, X.; Shacham, H. Short group signatures. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; pp. 41–55.
46. Boneh, D.; Boyen, X. Short signatures without random oracles. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; pp. 56–73.
47. Schnorr, C.P. Efficient identification and signatures for smart cards. In Proceedings of the Conference on the Theory and Application of Cryptology, Santa Barbara, CA, USA, 20–24 August 1989; pp. 239–252.
48. Fiat, A.; Shamir, A. How to prove yourself: Practical solutions to identification and signature problems. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Linköping, Sweden, 20–22 May 1986; pp. 186–194.
49. Pointcheval, D.; Stern, J. Security proofs for signature schemes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 12–116 May 1996; pp. 387–398.
50. Camenisch, J.; Shoup, V. Practical verifiable encryption and decryption of discrete logarithms. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; pp. 126–144.
51. Boneh, D. The decision diffie-hellman problem. In Proceedings of the International Algorithmic Number Theory Symposium, Portland, OR, USA, 21–25 June 1998; pp. 48–63.
52. Miyaji, A.; Nakabayashi, M.; Takano, S. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2001**, *84*, 1234–1243.
53. Scott, M. On the efficient implementation of pairing-based protocols. In Proceedings of the IMA International Conference on Cryptography and Coding, Cirencester, UK, 17–19 December 2011; pp. 296–308.
54. Brickell, E.; Camenisch, J.; Chen, L. Direct anonymous attestation. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 132–145.
55. Trusted Computing Group. TPM 1.2 Main Specification. Available online: <https://trustedcomputinggroup.org/resource/tpm-main-specification> (accessed on 3 December 2019).
56. Trusted Computing Group. TPM 2.0 Library Specification. Available online: <https://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2018-2028-000642.asp> (accessed on 3 December 2019).



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).