TAI: A Threshold-based Anonymous Identification Scheme for Demand-Response in Smart Grids

Zhiyuan Sui, Michael Niedermeier and Hermann de Meer

***Abstract*—Smart grids offer benefits compared to the current power grid by using technologies such as AMI and demand-response schemes. However, the introduction of these technologies also leads to challenges in the areas of privacy and identification of disobedient users. Current solutions to these challenges heavily rely on a trusted third party, which may lead to scenarios where the privacy of obedient consumers cannot be preserved. To tackle these concerns, anonymity provides a promising approach to obviating privacy preservation in smart grids. In this paper, a Threshold-based Anonymous Identification Scheme (TAI) for overload audit and privacy preservation in smart grids is proposed, where the use of a trusted third party is no longer required. Privacy preservation depends on the power consumption of consumers in the presence of a demand-response request from the power provider that defines an acceptable consumption threshold at periods of power shortage. Consumers must follow the instruction and curtail their consumption to meet the threshold. By doing so, the consumers who adhere to the power providers' instructions keep their anonymity, whilst the disobedient are be identified. According to our security and performance analysis, TAI significantly improves efficiency compared to previous anonymous identification schemes, while providing anonymity and identification.**

***Index Terms*—Smart Grid, Conditional Anonymity, Demand-Response, Privacy Preservation, Identification**

I. Introduction

Overview: The smart grid is an emerging critical infrastructure that offers significant advantages such as an improved efficiency, economics as well as reliability and sustainability compared to the current power grid. To achieve these goals, integration of the currently isolated power and communication networks as well as the introduction of several new technologies are required. Two of the most important additions are the Advanced Metering Infrastructure (AMI), which enables fine-granular, automated reporting of power consumption as well as generation and demand-response schemes which offer the possibility to send instructions to consumers to adapt their power consumption over a certain period of time, e.g. to prevent a brown- or—in the worst case—black-out in times of power shortage [1]. Incentive based demand-response in smart grids can be approached using two fundamentally different schemes: voluntary and mandatory. In the voluntary-incentive based schemes, the power provider sets the power price according to parameters such as time or current power availability. Consumers who voluntarily adapt their power consumption therefore benefit as their power costs are effectively reduced. In contrast to voluntary demand-response schemes, mandatory schemes for example in Interruptible/Curtailable (IC) or Capacity Market Program (CAP) [2], initial participation is an opt-in system. Once consumers opt to participate, it becomes imperative for them to follow dispatched instructions which are broadcast from their power provider during power shortage else they are penalized. In this paper we focus on the mandatory incentive based approach.

Z. Sui, M. Niedermeier and H. De Meer are with the University of Passau, Innstr. 43, 94032 Passau, Germany (e-mail: {zhiyuan.sui, michael.niedermeier, demeer}@uni-passau.de).

Problem definition: While AMI and demand-response schemes offer benefits to both the power provider and consumers, there are also several possible downsides to these approaches. In AMI, smart meters are used to generate consumption reports, to inform the power provider about the current power and long-term energy consumption of its consumers. This leads to privacy challenges for consumers, as the consumption information can be used to determine their lifestyles and daily routines. In contrast to the threats for consumers, the power provider also faces possible downsides in mandatory demand-response schemes. These originate from the possibility that consumers who participate in a mandatory demand-response program may still behave in a disobedient manner regarding adherence to instructions from the power provider. To handle both scenarios in a satisfactory way, it is required that privacy for obedient consumers, as well as identifiability of disobedient consumers can be guaranteed. Current solutions to this problem are pseudonym-based authentication schemes which rely heavily on trusted third parties as described in [3] and [4]. Additionally, the computational complexity increases as the inclusion of trusted third parties further increases the complexity of the infrastructure notwithstanding the challenging task of selecting suitable third parties. The aforementioned deficiencies in current solutions fuels the necessity for new and better solutions which offer efficient authentication schemes that can identify disobedient consumers whilst protecting the privacy of obedient consumers without the inclusion of a trusted third party into an already computationally complex system.

Our approach: Anonymity and ***unlinkability*** are amongst four basic approaches of privacy alongside ***pseudonymity***, ***unobserveability*** [5], used as solutions to current privacy concerns. Anonymity is an approach that preserves consumer privacy by removing the relationship that exists between their real identity and consumption. In this paper, an efficient anonymous identification scheme for demand-response management is designed: dubbed the Threshold-based Anonymous Identification (TAI) scheme. TAI can

dynamically cloak consumers' identities depending on their power usage. During normal operation, smart meters report the consumption information of all consumers to the power provider anonymously. In [6], it has proven that power shortages pose greater threat to electricity infrastructures than oversupply, so our approach therefore only considers power shortage scenarios. When the power provider detects a power shortage, it broadcasts demand-response instructions to its consumers, demanding them to adapt their power consumption. Obedient consumers adhere to the instructions and curtail their usage hence staying anonymous. Disobedient consumers on the other hand may not adhere and would therefore exceed the given power consumption threshold (e.g. by still using heavy power appliances) hence making them traceable. In TAI, compared to existing works [3] and [4], the provider cannot only identify disobedient consumers without the help of any trusted third party but also provide anonymity to obedient consumers. TAI revokes the consumers' anonymity depending on their power consumption during periods of power shortage. Once a consumption is larger than the predefined threshold set by the power provider, the power provider requests all smart meters to send disavowal proofs. If a smart meter disavows the consumption, the respective consumer that follows the demand-response instruction stays anonymous. Consumers that do not follow the demand-response instructions are identified. Also in TAI, the power provider authenticates a consumption report by using the group public key instead of public key of an individual consumer. With this, TAI reduces the computational complexity to an order of $O(1)$ which is well within the computational performance of low-powered embedded device like smart meters hence making TAI much more suitable for real-time data processing on low power embedded smart meters.

Outline: The remainder of this paper is organized as follows: Section II describes related work or prior arts in the privacy domain. Section III discusses the preliminaries and design background which are later on required for understanding of the proposed scheme. Section IV focuses on the design of a consumption model to illustrate the demand-response program. In Section V, we explain our proposed scheme which features both anonymity and identification, whilst Section VI shows what the scheme can achieve with a given security requirement. Section VII analyzes the developed scheme focusing on performance and compares it to related work. Finally, our conclusions are made in Section VIII.

II. Related Work

Research in the areas of identification and privacy preservation has a long history in smart grids due to the importance of both. However, these two domains are still conflicting, for example, identification requires a consumer to expose enough information to ensure their provided data is correct. Currently, a number of studies have tackled the identification issues in smart grids. Liu et al. [7], [8] propose a witness scheme to ensure identification in smart grids which supports a guaranteed audit of consumers for billing purposes. Xiao et al. [9], [10] propose an adaptive tree-based algorithm to detect malicious meter inspection behavior and energy theft. In order to achieve identification, these schemes require full information of the consumers hence do not consider any privacy issues.

As stated previously, privacy is an important feature in smart grids required to gain consumer acceptance. Current privacy preservation schemes in smart grids can be classified into three categories: data aggregation, credential and anonymity schemes. For power providers, it is not necessary to know all fine-granular consumption data. Instead, aggregated data can be used to forecast the consumption of households. Based on this use-case, data aggregation approaches have been proposed. Ruj et al. [11] propose a framework for secure information aggregation based on the Paillier cryptosystem. In this system, the power provider generates a key pair and publishes its public key. Smart meters encrypt consumption data with the public key provided by the power provider and send them to a gateway. The gateway aggregates the encrypted data which the power provider can recover later the real-time power consumption with its secret key. Here an important assumption is made in that, the gateway is always considered as a trusted party in the framework. Also, to ensure data integrity of the smart meters, identity-base signatures [12] and Boneh-Lynn-Shacham (BLS) signatures [13], have been introduced into the data aggregation schemes. In these approaches, a trusted third party is responsible for the collection of the consumption data from the smart meters. The third party has knowledge of consumption and can locate the source.

Data aggregation approaches cloak consumers' privacy by hiding the details of their consumption. However, the power provider requires this detail to identify disobedient or even source of malicious behavior in the grid. To achieve this, credential schemes introduce a trusted third party to ensure trustworthy communication between the power provider and its consumers. The credential can be a pseudonym or a blinded certificate. In [3], the real identities of consumers are encrypted by a control center to establish a pseudonym for each customer. Upon receiving suspicious messages, the control center can revoke the anonymity using its secret key upon request from the power provider. Thus, the trusted third party can identify the source of the suspicious data. Biselli et al. [14] utilize an administrator as an intermediate instance to pseudonymize the messages sent by a gateway using trusted platform modules. Though this provides anonymity, the choice of a trusted third party in itself is a herculean task. Furthermore, Gong et al. [15] employ Boneh-Boyen-Shacham (BBS+) signatures [16] to authenticate consumers' pseudonyms for incentive based demand-response programs. The consumer's real identity is hidden by the BBS+ signature. Since this approach is a voluntary-incentive based scheme, all consumers (obedient and disobedient) are allowed in the system. However the pseudonym is unable to protect consumers' profiles because all consumption data from one source can be linked to the consumer's pseudonym hence resulting in the issue of ***unlinkability***. Unlinkability is an important privacy metric; a con-

sumer's profile contains important information that is linked to its source hence serves as a key metric in identification. To deal with this issue, He et al. [4] employ group signatures where the group manager can revoke the anonymity of smart meters, while the power provider can decrypt their encrypted messages hence both parties are not able to link back to a single consumer. Only law authorities can combine the secret information from both parties to enable them trace disobedient consumer in the case of malicious behavior. However, in this approach law authorities still act as a kind of trusted third party hence the effect of trusted third party is not entirely removed.

The usage of a trusted third party adds additional complexity and insecurity to smart grids, propelling the need for novel, secure and privacy preserving schemes. Anonymity approaches are usually based on various anonymous authentication schemes, for example ring signature and blind signature schemes. Huang et al. [17] constructed a ring signature with forward security for smart grids. With this, a smart meter can prove the validity of its consumption report using several public keys therefore the power provider cannot link the consumption report to its consumer. However, it is also complex to calculate all the smart meters' public keys used. Besides ring signatures, blind signatures are used in [18] to achieve strong anonymity. In this approach, for each consumption report, the power provider signs a signature. A smart meter can convert the signature with which the consumption report can be proved. Signing each report is however also a time-consuming process. Similar to [15], Sui et al. [19] also employ BBS+ signatures for voluntary based demand response programs. The most important difference to [15] is that, [19] prevents two consumption reports from being linked back to a consumer if they are from the same source. However, this is not suitable for a mandatory based scheme since obedient consumers should voluntarily disclose their anonymity. Therefore, constructing an efficient anonymous identification scheme that does not require any third party has practical significance in smart grids.

Group signatures [20] are important anonymous authentication schemes for communication networks. In group signature schemes, the signers authenticate themselves without their individual public keys but with a group public key. The members' identities are hidden in the group. However, the anonymity revocation relies on the trustworthiness of a group manager. Ring signatures [21] further allow a signer to sign a message while remaining unconditionally anonymous. Ring signatures can be viewed as a variant of group signatures without a group manager. In classical ring signature schemes, a signer chooses a set of independent possible signers and hides his public key in the ring. However, unconditional anonymity might lead to abuse because malicious signers cannot be identified. In order to achieve signer identification, Komano et al. [22] propose an anonymous identification scheme, named deniable ring signatures. Deniable ring signatures allow all honest members to cooperate in tracing the origin of disobedient signatures. Based on the security model introduced by [22], Zeng et al. [23] propose a more efficient ring signature scheme in the random oracle model. In ring signature schemes, a member needs to authenticate himself using the public keys of all members. Because of that, its computational complexity is $O(n)$, where n is the number of members in the scheme. In smart grids, there are usually thousands if not hundreds of smart meters and therefore a computation that converges in linear time can be very costly given that most of these smart meters are low-powered embedded devices which cannot handle such computational complexity.

Table I
NOTATION

κ	security parameter, a random unary integer;
p	a prime number of size κ;
$\mathbb{G}$	a cyclic additive group of order p;
$\mathbb{G}_T$	a multiplicative group of order p;
$\mathbb{Z}_p^*$	a ring of order p;
P	a generator of $\mathbb{G}$;
e	a bilinear map: $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$;
EU	electricity utility;
SM	smart meter;
ID	the identity of a SM;
PK	non-interactive zero knowledge proof;
$\mathcal{H}$	a collision resistant hash function.

III. PRELIMINARIES

In the following, some standard notations and acronyms are defined in Table I and are further explained in detail in following subsections.

A. Bilinear Map

Bilinear maps are called pairings because they associate pairs of elements from two groups to yield an element of a third group. It is also used extensively in this paper. Hence we define a bilinear map as follows: Let p be a prime number of size κ, $\mathbb{G}$ and $\mathbb{G}_T$ are additive and multiplicative group respectively with order p. A function $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is said to be a bilinear map if it satisfies the following properties:

1) **Bilinearity:** $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$ for all $a, b \in \mathbb{Z}_p^*$, and all $P_1, P_2 \in \mathbb{G}$.
2) **Non-degeneracy:** $e(P, P) \neq 1$, since $e(P, P)$ is a generator of $\mathbb{G}_T$.
3) **Computability:** $e(P_1, P_2)$ is efficiently computable, for all $P_1, P_2 \in \mathbb{G}$.

For further details on bilinear maps or pairing, see [24].

B. Mathematical Assumptions

The mathematical assumptions in TAI are defined in this subsection.

Definition 1. *(Gap-Discrete Logarithm (Gap-DL) Assumption) There is no probabilistic polynomial time (PPT) algorithm that can compute a number x, where $x \in \mathbb{Z}_p^*$, from a tuple (xP, P), where $P \in \mathbb{G}$.*

With the Gap-DL assumption, a signer can hide his secret key x into his public key xP. Therefore, others cannot computes the secret value x based on the public key.

Definition 2. *(Decisional Diffie-Hellman (DDH) Assumption) There is no PPT algorithm that can distinguish between a tuple* $(\mu, x\mu, \hat{\mu}, T)$ *and a tuple* $(\mu, x\mu, \hat{\mu}, x\hat{\mu})$*, where* $T, \mu, \hat{\mu} \in \mathbb{G}$ *and* $x \in \mathbb{Z}_p^*$*.*

With the DDH assumption, a signer's signature T cannot be linked to his public key $x\mu$.

Definition 3. *(q-Strong Diffie-Hellman (q-SDH) Assumption) There is no PPT algorithm that can compute a pair* $(c, \frac{1}{z+c}P)$*, where* $c \in \mathbb{Z}_p^*$*, from a tuple* $(P, zP, ..., z^qP)$*, where* $P \in \mathbb{G}$ *and* $z \in \mathbb{Z}_p^*$*.*

With the q-SDH assumption, the group member can authorize a member's commitment without knowing his secrete information.

C. Zero-knowledge proof

In TAI scheme, the extensively employed non-interactive zero knowledge proof protocols are based on Gap-DL and DDH assumptions, defined in Subsection III-B. Zero knowledge proof was first proposed by Goldwasser et al. [25]. The purpose of zero knowledge proof protocols, denoted as PK$\{(x) : C = xP\}$ [26], is to help a prover to convince a verifier that he holds some knowledge x, without leaking the knowledge during the verification process.

D. BBS+ Signature

In the TAI scheme, the power provider utilizes BBS+ signatures to authorize consumers' commitments, with which the consumers can prove their consumption reports without revealing their real identities. The BBS+ signature is improved by Au et al. [16] based on Boneh's signature scheme [27]. BBS+ signatures are unforgeable without random oracles under the $q-$SDH assumption defined in Subsection III-B. It allows the generation of a signature without hash functions.

E. Security Requirements

Because the power provider traces disobedient consumers according to their consumption reports, some consumers might try to send fake consumption reports to misinform the power provider. It is necessary to create a scheme to ensure the security of the electricity infrastructure while guaranteeing the obedient consumers' anonymity. The following features, which are discussed in detail in Section VI, are required.

1) **Unlinkability:** No one can link different consumption reports from the same consumer.
2) **Strong Anonymity:** No one is able to link the consumption data of an obedient consumer to their sources.
3) **Non-frameability:** No one can produce an illegitimate signature to frame a legitimate consumer. The non-frameability of demand-response instructions coming from the power provider cannot be modified.
4) **Identification:** According to the consumption data, disobedient consumption must be identified.
5) **Integrity:** The power provider is able to check if the consumption data really originates from legitimate consumers without unauthorized modification.

IV. Consumption Model

It can be safely assumed that consumers' electricity consumption is much higher than the minimum requirements, therefore during a period of power shortage, the power provider considers as inappropriate for a consumer to use high-power electrical appliances. To indicate a power shortage, the provider broadcasts instructions to the consumers. These instructions may include a consumption threshold for a predicted time interval where a power shortage may occur. The consumers' consumption is therefore expected to decrease to a level lower than that threshold during the power shortage. In this section, we design a consumption model to illustrate the relationship between the power provider's instruction and its electricity generation profile.

A. Network Model

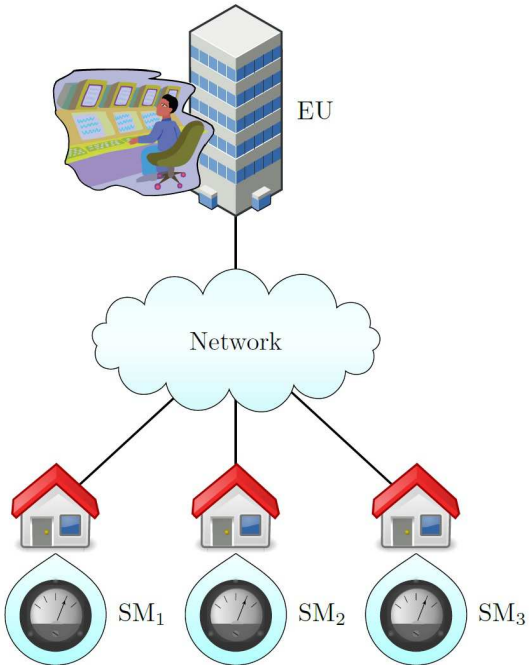


Figure 1. Network Model

In this subsection, the network model is formalized. In contrast to previous trusted third party-based network models, the network model, which is depicted in Figure 1, consists of two entities, SM and EU.

1) **SM:** In a district, there usually exists a reasonable number of households, equipped with smart meters (SMs). A SM is a electricity consumption reporting device present at each consumer's site. The SMs anonymize their consumption data and report them regularly. Consumers do not know the secret knowledge of SMs, which are

assumed to be resistant against tampering. Although SMs are not controlled by their consumers, each SM corresponds to a single consumer. Therefore, there is no discrimination between a consumer and his SM in TAI.

2) **EU:** The electricity utility (EU) is an infrastructure controlled by the power provider and is in charge of the SMs in a concrete area. It collects and analyzes the consumption data from SMs periodically and broadcasts consumption related instructions to customers according to the consumption data. The EU identity is not cloaked as its also important for consumers to know who their utility providers are, hence, the EU is a public entity.

B. Assumptions

The model is based on the following assumptions.

1) The consumers' electricity generation is larger than their basic requirements. It means that a electricity consumption reduction is possible on consumers' side.
2) The number of SMs is denoted as N_{SM}, which is fixed.
3) t_i is an instantaneous time within the interval $t_0 \leq t_i \leq t_n$ of a predicted power shortage where the EU sends instructions.
4) The individual electricity consumption collected from SMs at t_i is denoted as m. Empirically, individuals' electricity consumption is independent of each other. Figure 2 shows the Erlang distribution function $f(m) = 112\frac{0.495^3 m^2 e^{-0.495m}}{2!}$ and the distribution of number of consumers in a sample period of an European district with 112 smart meters in the grid. We can assume that the number of SMs follows an Erlang distribution $f(m)$ regarding their consumption without an instruction. It follows that, the number of SMs is given by $N_{SM} = \sum_{m\geq 0}^{+\infty} f(m)$, where the unit of m is 10Wh.
5) The overall consumption monitored by N_{SM} at t_i without an instruction from the EU is denoted as P_{SM}. Therefore, without an instruction, all consumers' consumption $P_{SM} = \sum_{m\geq 0}^{+\infty} mf(m)$.
6) In the model, all consumers follow the instruction from the EU during a period of power shortage. Consumers who reduce their consumption, shift their consumption to the next time period once they receive an instruction from the EU.
7) The power generation at t_i is denoted as G_i.
8) The consumption threshold for all consumers at t_i is denoted as d_i.

C. Scenario

In this subsection, a scenario is used to prove that there is a valid value d_i, which can ensure that the consumers' electricity consumption P^*_{SM} is not larger than the EU's electricity generation G_i during a power shortage within the interval $t_0 \leq t_i \leq t_n$.

When the EU broadcasts an instruction (d_i, t_i), each consumer's consumption should not exceed d_i at t_i. If a consumer's consumption is not higher than d_i, the consumption would not be detected. The sum of the electricity requirement below the threshold is denoted as $P_{\leq d_i}$, where $P_{\leq d_i} = \sum_{m\geq 0}^{\lfloor d_i \rfloor} mf(m)$. From assumption (6), consumers whose consumption is higher than d_i will reduce their consumption to d_i at t_i. This group of consumers is referred to as obedient consumers. The total consumption above d_i at t_i is denoted as $P_{>d_i}$, where $P_{>d_i} = d_i \sum_{m>\lfloor d_i \rfloor}^{+\infty} f(m)$. From the above, it follows that the overall consumption during the power shortage is given by: $P^*_{SM} = P_{\leq d_i} + P_{>d_i} = \sum_{m\geq 0}^{\lfloor d_i \rfloor} mf(m) + d_i \sum_{m>\lfloor d_i \rfloor}^{+\infty} f(m) \leq G_i$, which is a linear inequality. The only unknown variable, d_i, can be derived.

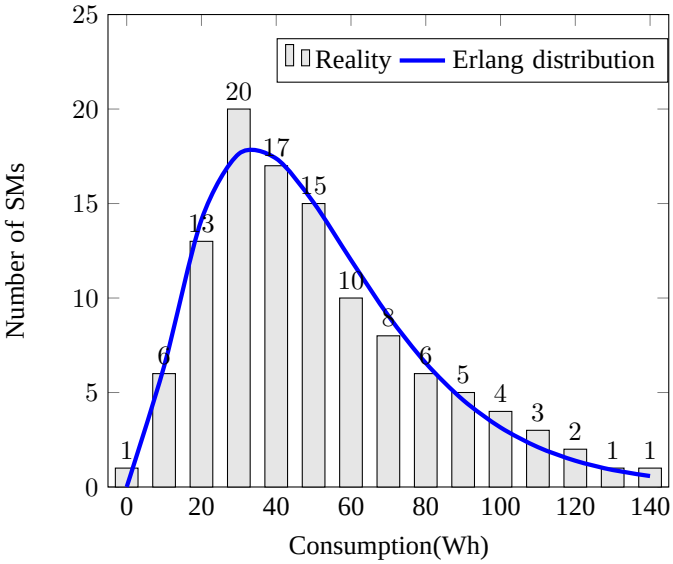


Figure 2. Consumer distribution from 7:45 to 8:00 AM in the first of August

To further illustrate the consumption model, we use a power shortage within a specified time interval as follows. The consumers' original consumption and the power plants' generation curves are shown in Table II, from which it can be seen that the renewable electricity generation decreases after 9:15 AM. The consumers' electricity consumption is 7800Wh but the generation is only 6300Wh. Under the EU's instruction, the overall consumption during this interval should be less than the generation $P^*_{SM} \leq G_i$. Because $f(m|m > 160\text{Wh}) < 1$, $f(m)$ are negligible when $m > 160$Wh, the threshold value and electricity generation should satisfy the inequality: $112(\sum_{m\geq 0}^{7} \frac{m0.58^4 m^3 e^{-0.58m}}{3!} + d_i \sum_{m\geq 8}^{16} \frac{0.58^4 m^3 e^{-0.58m}}{3!})\text{Wh} \leq 6300\text{Wh}$. The unit of m is 10Wh. Based on this inequality, resulting d_i is 72.4 Wh. It means that a consumer whose electricity consumption is larger than 72.4Wh should reduce his consumption below this value. Therefore the consumers reduce their requirements by 1500Wh at 9:15 AM. From our earlier assumptions, consumers who postponed the consumption may want to use their electricity in the next interval, therefore the predicted consumption would be the sum of the current consumption and the difference from the previous interval as illustrated in the third row of Table II. Although the generation is 860Wh larger than the original consumption at 9:45 AM, we have a carry forward of 2930Wh from the previous intervals, therefore we still experience a power shortage at 9:45 AM since the generation is still below the predicted consumption shown in row four of Table II. At 10:15 AM, the generation

is 30Wh more than the predicted consumption therefore no consumption threshold is required. From the example, it can be seen that the power shortage is monitored with the instruction ($\{72.4, 59.8, 88.3, 77.1\}$ Wh, 9:15 - 10:00 AM).

Table II
PROFILE OF EXAMPLE (WH)

Time	**9:15**	**9:30**	**9:45**	**10:00**	**10:15**
Original Generation	6300	6070	6260	6300	6300
Original Consumption	7800	7500	5400	5300	5200
Electricity Difference	-1500	-1430	860	1000	1100
Predicted Consumption	7800	9000	8330	7370	6270
Threshold Value	72.4	59.8	88.3	77.1	–

V. PROPOSED TAI SCHEME

In this section, a detailed description of the TAI scheme is given. We refer to two main parts of the scheme:

1) Anonymous consumption reporting of SMs to EU;
2) Demand-response part, where EU correlates power requirement with supply.

The scheme is described with the aid of Figure 3. During the anonymous report part, the SMs regularly send consumption reports to the EU in an anonymized way. Upon receiving the reports, the EU confirms the validity of the reports. In the demand-response part, if the EU identifies that the power consumption is larger than the possible production, it defines a threshold instruction (D_n, T_n), where D_n is a set of consumption thresholds $\{d_1, .., d_n\}$ and T_n is a set of timestamps $\{t_1, ..., t_n\}$. At $t_i (1 \leq i \leq n)$, all consumers must curtail their power consumption below $d_i (1 \leq i \leq n)$. If a consumer whose consumption is larger than the threshold in the predefined time period exists, the EU broadcasts an identification order (m^*, t^*). The SMs validate the order from the EU and check it against the initial instructions for curtailment of consumption, i.e. whether $m^* > d_i$ at $t^* = t_i$. If the check holds, the SMs produce disavowal proofs; otherwise, the order is rejected. This procedure enables the EU to identify disobedient consumers without compromising the anonymity of obedient consumers. The TAI scheme includes the Setup, Report Generation and Report Reading algorithms as well as the Joining, Instruction Generation and Identification protocols which are discussed in the following subsection.

A. Setup

In TAI, a concrete region is managed by a single EU. The number of SMs is large enough for each consumer to cloak his usage behavior. Each household or company is equipped with a SM. The identity of the SM can be linked to the corresponding consumer by the EU. Both the EU and the SMs have computational abilities. The EU executes the Setup algorithm to generate its long term key pair as follows:

1) Firstly, on input κ, the bilinear pairing generator returns a tuple $(p, \mathbb{G}, \mathbb{G}_T, e, P)$ as defined in Subsection III-A.
2) Secondly, the EU randomly chooses $G, H, Q \in \mathbb{G}$ and an integer $\gamma \in \mathbb{Z}_p^*$, and computes the part of public key $P_{pub} = \gamma P$.
3) Thirdly, the EU chooses collision resistant hash functions $\mathcal{H}_1$: $\{0,1\}^* \to \mathbb{G}$; $\mathcal{H}_2$, $\mathcal{H}_{\mathrm{ID}} : \{0,1\}^* \to \mathbb{Z}_p^*$.
4) Finally, the EU keeps its secret key γ and publishes its public key (P, G, H, Q, P_{pub}) and hash functions ($\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_{\mathrm{ID}}$).

B. Joining

The Joining protocol is carried out between the EU and each SM. The SMs are equipped with tamper-resistant black boxes [28], [29]. Each black box holds a key pair **(SK, PK)**. The EU has access to the public key **PK**. Each black box generates an internal private seed specific to itself. The seed is stored securely within the black box and is never disclosed to anyone or changed, as the black box is assumed to be tamper-resistant. In addition, a secure public key signature scheme, including a signing algorithm **sig** and a verification algorithm **ver**, is selected for a SM with key pair **(SK, PK)**. Each SM shows its real identity and produces its key pair during the protocol execution: At first, the SM randomly generates an integer $x \in \mathbb{Z}_p^*$ as its secret key using its internal seed **seed**. The SM then computes a commitment C on the value x: $C = xP$ and generates a signature $\sigma =$ **sig**$(C \| \mathrm{ID})$. The SM sends $C \| \mathrm{ID}$ as well as its signature σ to the EU. The commitment essentially binds the SM's secret key x. Upon receiving C, the EU executes the verification algorithm to check the validity of the signature. If **ver**$(C \| \mathrm{ID}, \sigma) =$ valid, the EU computes the credentials $\alpha = \mathcal{H}_{\mathrm{ID}}(\mathrm{ID})$ and $S = \frac{1}{\gamma + \alpha}(C + Q)$ and sends S to the SM. The SM confirms the correctness of the credential by checking if the equation $e(S, \alpha P + P_{pub}) = e(C + Q, P)$ holds. The SM's secret key is x, and its public key is (C, S).

C. Report Generation

In order to achieve a real-time consumption report, a SM can run the report generation algorithm to produce a legitimate signature as follows: Firstly, by using the knowledge of secret key x, the SM binds the consumption data m and the timestamp t with the element T. The SM computes the hash value $\mu = \mathcal{H}_1(m \| t)$ and $T = x\mu$. The SM then proves $e(S, \alpha P + P_{pub}) = e(xP + Q, P)$ and $T = x\mu$ with the non-interactive zero knowledge proof Π:

$$PK \left\{ \begin{pmatrix} S \\ x \\ \alpha \end{pmatrix} : \begin{array}{l} e(S, \alpha P + P_{pub}) = e(xP + Q, P) \\ T = x\mu \end{array} \right\}$$

The procedure of the proof is formally described below:

1) The SM randomly picks integers $r, k_0, k_1, k_2, k_3 \in \mathbb{Z}_p^*$.
2) In order to cloak its identity, the SM transforms its original credential S into a temporary one $U = S + rH$, where $r \in \mathbb{Z}_p^*$, and hides r in $R = rG$. Then, the SM generates M_1, M_2, N and V to blind r, α, x and S respectively, $M_1 = k_1 G$, $M_2 = k_2 G - k_3 R$, $N = k_0 \mu$, $V = e(P, P)^{k_0} e(H, P_{pub})^{k_1} e(H, P)^{k_2} e(U, P)^{-k_3}$.
3) The SM calculates a hash value $g = \mathcal{H}_2(T \| R \| M_1 \| M_2 \| N \| U \| V \| m \| t)$, and hides x in

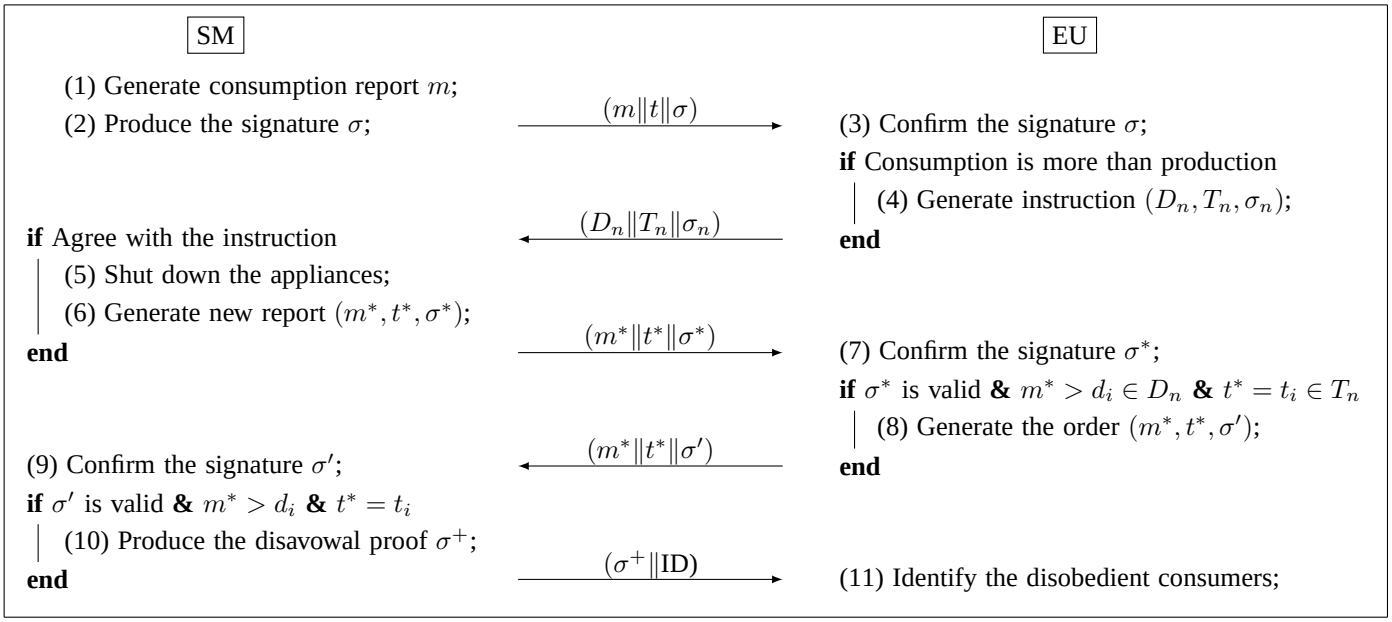


Figure 3. Flow chart of TAI

s_0, r to s_1 and α in s_2 and s_3. $s_0 = k_0 + gx$, $s_1 = k_1 + gr$, $s_2 = k_2 + gr\alpha$, $s_3 = k_3 + g\alpha$.

The SM can show that both the temporary credential and the element T correspond to the same secret key x and credential α without leaking any information about them. Given two signatures, it is impossible to determine whether they are produced by the same SM. Consequently, anonymity is achieved. In the end, the SM outputs $(T, R, U, g, s_0, s_1, s_2, s_3, m, t)$ as the signature.

D. Report Reading

After the receipt of the consumption report, the EU checks the validity of the timestamp. If it is invalid, the EU ignores the report. Otherwise, the EU executes the report reading algorithm to check whether the signature does prove the knowledge of secret key x as well as the knowledge of the valid credential S.

The EU firstly computes the hash value $\mu = \mathcal{H}_1(m\|t)$ and the elements $M_1' = s_1G - gR$, $M_2' = s_2G - s_3R$, $N' = s_0\mu - gT$ and $V' = e(P,P)^{s_0} e(H, P_{pub})^{s_1} e(Q,P)^g e(U, P_{pub})^{-g} e(U,P)^{-s_3} e(H,P)^{s_2}$.
Next, the EU confirms that $g = \mathcal{H}_2(T\|R\|M_1'\|M_2'\|N'\|U\|V'\|m\|t)$ holds with the hash value. If it holds, the EU accepts the consumption report; otherwise, the EU rejects it.

E. Instruction Generation

Once the EU finds that the anticipated power consumption is larger than the production, it executes the Instruction Generation protocol to order the consumers to decrease their power requirements.

The EU first defines the instruction (D_n, T_n). If a consumer power consumption is above the EU defined threshold $d_i \in D_n$, the consumption must be be reduced below d_i at $t_i \in T_n$. The EU then generates a valid signature to prove its identity. It randomly picks $k_4 \in \mathbb{Z}_p^*$, computes $W = k_4P$, $f = \mathcal{H}_2(D_n\|T_n\|W\|t)$ and $s_4 = k_4 - f\gamma$. The EU broadcasts the instruction and the signature (D_n, T_n, s_4, f, t) to all SMs.

Upon receiving the usage instructions, a SM checks whether the timestamp and the instruction are valid and its usage satisfies the instruction. It computes $W' = fP_{pub} + s_4P$, checks whether $f = \mathcal{H}_2(D_n\|T_n\|W'\|t)$ and its usage $m > d_i$. If they hold, the SM must reduce their power consumption under d_i; otherwise, it just ignores the instruction and signature.

F. Identification

After the instruction generation, if the EU still finds that there exists a valid consumption (m^*, t^*), where $m^* > d_i$ and $t^* = t_i$, it executes the identification protocol to identify the disobedient consumer.

The EU produces a valid identification order which includes the disobedient consumer's consumption data, a timestamp, and the EU's proof. The EU randomly picks $k_5 \in \mathbb{Z}_p^*$, and computes $X = k_5P$, $l = \mathcal{H}_2(m^*\|X\|t^*\|t)$, $s_5 = k_5 - l\gamma$. Then, the EU broadcasts the identification order (m^*, t^*, l, s_5, t) to all SMs.

After receiving the identification order, a SM computes $X' = lP_{pub} + s_5P$ and checks whether $l = \mathcal{H}_2(m^*\|X'\|t^*\|t)$, $m^* > d_i$ and $t^* = t_i$. If they do not hold, the SM ignores the order; otherwise, the SM generates a disavowal proof. It computes a hash value $\mu = \mathcal{H}_1(m^*\|t^*)$ and $T' = x\mu$, randomly picks $k_6 \in \mathbb{Z}_p^*$ and computes $A = k_6P$ and $B = k_6\mu$ to blind x. The SM computes another hash value $h = \mathcal{H}_2(m^*\|T'\|A\|B\|C\|t^*)$ and hides x in $s_6 = k_6 - hx$. The SM sends the proof $(\text{ID}_j, T', s_6, h, t^*)$ to the EU.

Upon receiving of the proof, the EU checks the validity of the proof. It computes $A' = s_6P + hC$ and $B' = s_6\mu + hT'$. The EU accesses the public key C of ID_j and checks whether $h = \mathcal{H}_2(m^*\|T'\|A'\|B'\|C\|t^*)$ holds. If it holds and $T \neq T'$, the EU can determine that the SM does not belong to a

disobedient consumer; otherwise, the EU can determine that ID_j is a disobedient consumer.

VI. Security Analysis

A security analysis of the TAI scheme is carried out in this section. In particular, following the security requirements discussed in Subsection III-E, the analysis is divided into five parts: unlinkability, strong anonymity, non-frameability, identification and integrity.

A. Unlinkability

In the TAI scheme, the unlinkability of the SMs' identities is intractable under the DDH assumption. A SM generates its consumption report using its secret key x. The essence of the Report Generation algorithm is to replace the static public key (S, C) with a temporary one (U, R, M_1, M_2, V). Because $\mathcal{H}_1$ is a collision resistant function, the temporary key pairs do not contain any useful information that can link two signatures.

After that, the SMs send their messages and signatures in an anonymized way. It is infeasible to decide whether two elements (T, N) and (T', N') are generated using the same secret information x under the DDH assumption. Obedient SMs reply the identification order only when the consumption data m is larger than the threshold and the timestamp is in the predefined interval. As long as the consumer follows the instruction, no one can determine whether two signatures are from the same SM.

During the Identification protocol, the obedient SM signs the identification order with its secret key x. Due to the collision resistance of hash function $\mathcal{H}_1$, no one can link its disavowal proof (T^*, A, B, t) to its previous signature (T, R, U, t).

B. Strong Anonymity

The strong anonymity of the TAI scheme is based on its unlinkability. According to the analysis of unlinkability, no one can link two different consumption reports from the same SM. If an attacker can construct a probabilistic polynomial time scheme that can find the source of a consumption report, we can link all consumption reports to their sources. This means we can construct another probabilistic polynomial time scheme to link two different consumption reports if they are from the same SM.

As such, neither the EU nor other consumers can trace a legitimate signature from an obedient SM unless it knows the secret key. Therefore, its usage is still anonymous. Hence, TAI satisfies the strong anonymity requirement.

C. Non-frameability

In the scheme, the non-frameability of the consumption data and proofs of SMs and instructions of the EU are based on the Gap-DL assumption.

First, the non-frameability of SMs is discussed. During the Joining protocol, a SM computes $C = xP$ and cloaks its secret key x using the Gap-DL assumption. Therefore, the EU has no knowledge of the secret x. The Report Generation algorithm and the Identification protocol for SMs are also non-interactive zero knowledge proofs. If the EU or other SMs can produce an illegitimate but valid signature or proof that can be linked to the target SM, it can solve the Gap-DL assumption, according to the security of non-interactive zero knowledge proof [30].

Secondly, the non-frameability of the EU is investigated. Similar to the SM, the non-frameability of the EU is also based on security of non-zero knowledge proofs. Without the knowledge of secret γ, no one can produce a valid but illegitimate instruction or identifying order framing the EU.

D. Identification

The identification of the scheme is based on both the Gap-DL assumption and the $q-$SDH assumption. There are two cases for disobedient consumers to break identification requirement. The first one is to generate a valid fake consumption report, which is larger than the threshold but is linked to no one. The EU authorizes the SM's commitment with a BBS+ signature. Intuitively, a BBS+ signature implies that an adversary, who can corrupt and control a polynomial number of key pairs held by the corresponding SMs, cannot forge a new key pair by itself without the help of the EU. This in turn means that the Joining protocol is secure. Both the consumption data signature (T, R, U) and the disavowal proof (T', A, B) are signed by the same secret key. According to the analysis of non-frameability, a disobedient SM cannot frame an obedient SM. It means an attacker cannot produce a fake proof to pass the identification protocol. The second case is to generate a valid fake disavowal proof. The disavowal protocol is a Schnorr signature, which is based on Gap-DL assumption. The disobedient SMs can only submit their data, where $T = T'$. Therefore, the disavowal proof cannot be forged. Based on the Gap-DL assumption and the $q-$SDH assumption, obedient SMs can always disavow a disobedient signature. The EU can determine that anyone who cannot disavow the signature has to be a disobedient SM. Therefore, the TAI scheme can provide identification.

E. Integrity

In TAI, the integrity of the power consumption data is based on its non-frameability and identification. According to the analysis of non-frameability, it can be seen that an adversary cannot produce an illegitimate but valid key pair (x, C) linked to a legitimate SM. According to the analysis of identification, the adversary cannot produce an illegitimate key pair (α^*, C^*, S^*), which satisfies $e(S^*, \alpha^* P + P_{pub}) = e(C^* + Q, P)$, without the help of the EU. This means that the Joining protocol is secure. Proof Π is a standard non-interactive zero knowledge proof. According to the security of zero knowledge [30], the EU knows the secret corresponding to a legitimate SM, but it has no knowledge on the secret information of the signer. This implies that the Generation Report algorithm is secure. Without holding a valid key pair, no one can produce a valid signature and pass the verification algorithm. Therefore, such a signed message cannot be forged or modified without being detected.

F. Comparison

From the security analysis, it can be seen that TAI satisfies all security requirements of Subsection III-E. Moreover, the TAI scheme is compared to related works that are described in Section II. Comparison results are depicted in Table III, where unlinkability is denoted as Unlink.; strong anonymity is denoted as Anoy.; non-frameability is denoted as Non-fra.; identification is denoted as Iden.; and data integrity is denoted as Integ.. Unlinkability and anonymity of aggregation schemes depend on a trusted third party, which can collude with the EU to link SMs to their consumption data. Identification of credential schemes is also based on a trusted third party. Therefore, it can also link obedient consumers' consumption data to their sources. Since anonymity schemes provide unconditional anonymity, disobedient consumers cannot be identified in those schemes.

Table III
COMPARISON OF FUNCTIONALITY

	Unlink.	**Anony.**	**Non-fra.**	**Iden.**	**Integ.**
Aggregation	×	×	√	√	√
Credential	×	×	√	√	√
Anonymity	√	√	√	×	√
TAI	√	√	√	√	√

VII. PERFORMANCE ANALYSIS

In this section, firstly, the signature sizes are discussed. Secondly, the computational complexity is described. Thirdly, a comparison of TAI to other schemes is done.

A. Communication overhead

Firstly, the communication overhead of consumption reports which are generated by the SMs and delivered to the EU are analyzed. The consumption report is in the form of $m\|T\|R\|U\|g\|s_0\|s_1\|s_2\|s_3\|t$ for a SM and its size is $|m| + 3|\mathbb{G}| + 5|\mathbb{Z}_p^*| + |t|$, where $|m|, |\mathbb{G}|, |\mathbb{Z}_p^*|$ and $|t|$ are the length of the consumption data, the length of element from $\mathbb{G}$, the length of element from $\mathbb{Z}_p^*$ and the length of timestamp, respectively. Secondly, the communication overhead of the demand-response part which includes the instruction generation and identification is assessed. If the EU finds that the power requirement is too large to provide, it will generate the power usage instruction in the form of $D_n\|T_n\|s_4\|f\|t$. The size of that is $|D_n| + 2|\mathbb{Z}_i^*| + 2|t|$. If the EU finds a SM which does not follow the instruction, it will broadcast the identification order to all SMs. The form of the order is $m^*\|t^*\|l\|s_5\|t$, with a size of $|m^*| + 2|\mathbb{Z}_p^*| + 2|t|$. The form of each SM's proof is $\mathrm{ID}\|T'\|s_6\|h\|t^*$. Its size is $|\mathrm{ID}|+|\mathbb{G}| + 2|\mathbb{Z}_p^*| + |t|$.

B. Computational Complexity

Compared with exponentiation G_e, multiplication G_m and pairing evaluations G_p, the overheads of hash evaluations and arithmetic operations are neglectable [31]. Therefore, only G_e, G_m and G_p are analyzed. Several bilinear pairings operations are fixed and can be calculated in advance. For example, the EU can calculate $e(P, P)$ in the initialization algorithm and set it as the public key. The computational costs are presented in Table IV.

Based on the computational costs, the scheme is emulated on a Ubuntu 12.04 virtual operating system with a Intel Core i5-4300 dual-core @ 2.60 GHz CPU, using one core and 1 GB of RAM. All results are obtained running 20 test repetitions for each algorithm and number of consumers. The simulation utilizes PBC cryptography libraries [31], which are free C libraries that perform the required mathematical operations underlying pairing-based cryptosystems. To achieve 80 bits security level, similar to existing works [13], the length of $\mathbb{G}$ is set to 161 bits and p to 160 bits. In the simulation, the communication overhead and delay between the EU and SMs is neglected. The simulation results are presented in Table IV, where Devia. stands for the standard deviation and Inter. stands for the 95% confidence interval.

Table IV
COMPUTATIONAL PERFORMANCE

	Party	**Computational cost**	**Mean**	**Devia.**	**Inter.**
Setup	EU	$4G_p + G_m$	37.48	0.69	0.33
Joining	EU	G_m	3.76	0.32	0.17
	SM	$2G_p + 2G_m$	18.74	0.35	0.17
Report Gene.	SM	$G_p + 3G_e + 8G_m$	31.00	0.68	0.32
Report Read.	EU	$2G_p + 4G_e + 8G_m$	48.18	0.41	0.19
Ins. Gene.	EU	G_m	3.35	0.13	0.06
	SM	$2G_m$	4.57	0.10	0.05
Identification	EU	$5G_m$	11.02	0.13	0.06
	SM	$5G_m$	12.04	0.10	0.05

C. Comparison

Based on the computational performance of TAI described in Subsection VII-B, the computational time and communication overhead for each consumption report is analyzed with changing number of consumers. The results are compared to the conditionally anonymous ring signature (CRS) [23] and deniable ring signature (DRS) [22]. CRS and DRS both provide similar security properties. In order to achieve more accurate simulation environment, different Ubuntu virtual machines are used to simulate the SM and the EU. The SM is simulated using a 798 MHz CPU and 256 MB RAM which is not far away from a real SM. The EU is simulated on a device with 2.60 GHz CPU and 1GB RAM, however, it is still assumed that the computational ability from the EU side is unlimited. The results are depicted in Figure 4 and 5 respectively. The 95% confidence intervals are not visible in both figures. The mean interval sizes for Figure 4 are: TAI 1.01, CRS 0.63, and DRS 0.97. For Figure 5, the mean 95% confidence interval

sizes are: TAI 0.36, CRS 0.33, and DRS 0.33. It can be shown that the computational cost for a SM and the EU is constant in TAI during the data demand part. Whereas, the computational cost for a SM and the EU are $G_p+4G_e+nG_m$ and $(4q-1)G_e$ in the CRS and $2G_p + 3G_e + qG_m$ and $4nG_e$ in the DRS, where n is the number of SMs in the system. According to the comparison, it is concluded that TAI has significant advantages over CRS and DRS in terms of computational cost for smart grid systems.

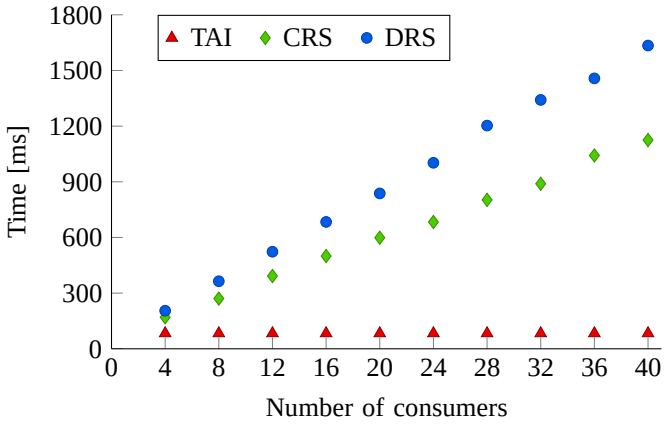


Figure 4. Computational cost of SM for Report Generation

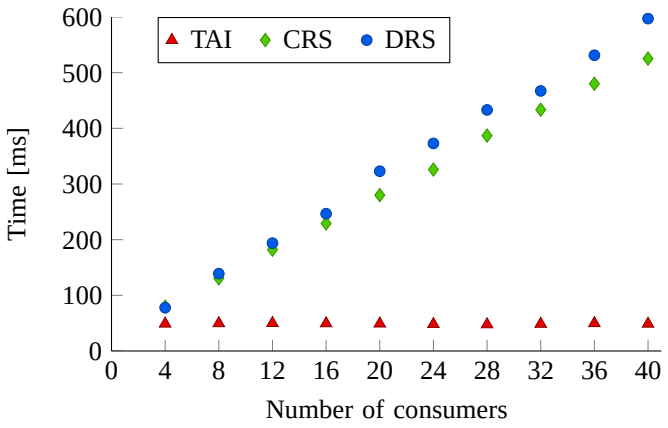


Figure 5. Computational cost of EU for Report Reading

Next, the signature size among the TAI scheme, CRS, and DRS, whose signature sizes are $161n + 804$ bits and $481n + 161$ bits respectively, are compared, where n is the number of SMs. Form Figure 6, it can be seen that TAI reduces the communication overhead in comparison to CRS and DRS.

According to the analysis above, one of the highlights of TAI is that the communication overhead and computation complexity are constant. In CRS [23], the identification is based on the Gap-DL assumption. A SM must use other peer SMs' public keys to cloak its identity. This requires that the SM calculates the signature for all other SMs' public keys. The identification of the TAI scheme is based on the $q-$SDH assumption. The SM produces its commitment, whilst the EU produces the credential to authorize the commitment. The

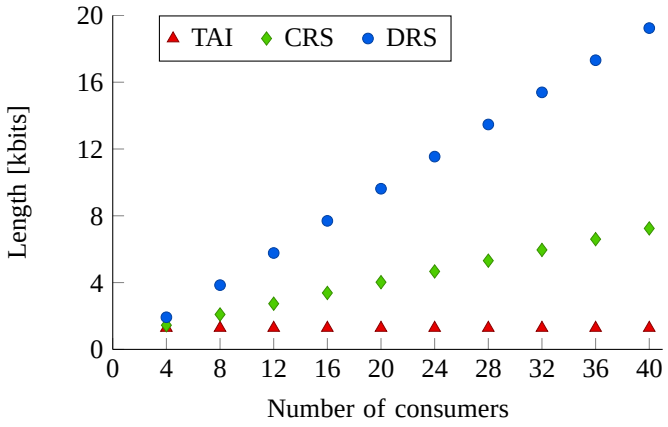


Figure 6. SM to EU communication overhead

report generation part employs non-interaction zero knowledge proof, which cloaks the SM's key pair.

VIII. Conclusion

In this paper, a novel secure anonymous identification scheme for demand-response management in smart grids has been presented. It has been shown that, the scheme provides strong anonymity and identification against privacy leaking and power overloading. A consumption model was built to testify that a threshold value can be found to fill the gap between power consumption and generation during power shortage, where consumers' power consumption should be lower than the threshold value. Hence enabling EU to identify consumers whose power consumption are contradictory to defined threshold during power shortage whilst at the same time keeping anonymous, the identity of complaint consumers. The security analysis proves that TAI can achieve unlinkability, strong anonymity, non-frameability, identification and integrity. To the best of our knowledge, there is no previous work on anonymous identification schemes that can simultaneously fulfill these requirements in smart grids. From the performance analysis, one key highlight of the TAI scheme is its constant convergence time. Compared with other two conditionally anonymous ring signatures (CRS and DRS), TAI significantly reduces the computational cost and improves communication efficiency.

Acknowledgment

The research leading to these results was supported both by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1), the East-Bavarian Centre of Internet Competence, funded by the Bavarian Ministry of Economic Affairs and Media, Energy and Technology, as well as COST (European Cooperation in Science and Tehcnology) Action No. CA15127, RECODIS (Resilient communication services protecting end-user applications from disaster-based failures).

REFERENCES

[1] Yuan-Liang Lo, Shih-Che Huang, and Chan-Nan Lu, "Non-technical loss detection using smart distribution network measurement data," in *Innovative Smart Grid Technologies - Asia (ISGT Asia), Tianjin, 2012, IEEE*, 21.-24. May, 2012, pp. 1–5.

[2] Farrokh Rahimi and Ali Ipakchi, "Demand response as a market resource under the smart grid paradigm," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 82–88, 2010.

[3] T.W. Chim, S.M. Yiu, L. C K Hui, and V.O.-K. Li, "Pass: Privacy-preserving authentication scheme for smart grid network," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, Brussels*, 17-20, May, 2011, pp. 196–201.

[4] Daojing He, Chun Chen, Jiajun Bu, S. Chan, Yan Zhang, and M. Guizani, "Secure service provision in smart grid communications," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 53–61, 2012.

[5] Stefanos Gritzalis, "Enhancing web privacy and anonymity in the digital era," *Information Management & Computer Security*, vol. 12, no. 3, pp. 255–287, 2004.

[6] Patrick O Leu and Daniel Peter, "Case study: Information flow resilience of a retail company with regard to the electricity scenarios of the sicherheitsverbundsübung schweiz (swiss security network exercise) svu 2014," in *International Conference on Critical Information Infrastructures Security*. Springer, 2015, pp. 159–170.

[7] Jing Liu and Yang Xiao, "An accountable neighborhood area network in smart grids," in *Embedded and Multimedia Computing Technology and Service, Gwangju*, pp. 171–178. Springer, 6.-8., Sep., 2012.

[8] Jing Liu, Yang Xiao, and Jingcheng Gao, "Achieving accountability in smart grid," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 493–508, 2014.

[9] Zhifeng Xiao, Yang Xiao, and DH Du, "Exploring malicious meter inspection in neighborhood area smart grids," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 214–226, 2013.

[10] Zhifeng Xiao, Yang Xiao, and DH-C Du, "Non-repudiation in neighborhood area networks for smart grid," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 18–26, 2013.

[11] Sushmita Ruj and Amiya Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 196–205, 2013.

[12] Hongwei Li, Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin Shen, "Edr: An efficient demand response scheme for achieving forward secrecy in smart grid," in *Global Communications Conference (GLOBECOM), 2012 IEEE, Anaheim*, 3.-7., Dec, 2012, pp. 929–934.

[13] Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, 2012.

[14] Anna Biselli, Elke Franz, and Maurílio Pereira Coutinho, "Protection of consumer data in the smart grid compliant with the german smart metering guideline," in *Proceedings of the first ACM workshop on Smart energy grid security, Berlin*. ACM, 4.-8., Nov., 2013, pp. 41–52.

[15] Yanmin Gong, Ying Cai, Yuanxiong Guo, and Yuguang Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," 2015.

[16] Man Ho Au, Willy Susilo, and Yi Mu, "Constant-size dynamic k-taa," in *Security and Cryptography for Networks*, pp. 111–125. Springer, 2006.

[17] Xinyi Huang, Joseph K Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, vol. 64, no. 4, pp. 971–983, 2015.

[18] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Huaqun Wang, "An anonymous data aggregation scheme for smart grid systems," *Security and Communication Networks*, vol. 7, no. 3, pp. 602–610, 2014.

[19] Zhiyuan Sui, Ammar Alyousef, and Hermann de Meer, "Iaa: Incentive-based anonymous authentication scheme in smart grids," in *Internet Science*, pp. 133–144. Springer, 2015.

[20] David Chaum and Eugène Van Heyst, "Group signatures," in *Advances in Cryptology EUROCRYPT 91, Brighton*. Springer, 8.-11., Apr., 1991, pp. 257–265.

[21] Ronald L Rivest, Adi Shamir, and Yael Tauman, "How to leak a secret," in *Advances in Cryptology ASIACRYPT 2001, Gold Coast*, pp. 552–565. Springer, 9.-13., Dec., 2001.

[22] Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, and Shinichi Kawamura, "Toward the fair anonymous signatures: Deniable ring signatures," in *Topics in Cryptology–CT-RSA 2006, San Jose*, pp. 174–191. Springer, 13.-17., Feb., 2006.

[23] Shengke Zeng, Shaoquan Jiang, and Zhiguang Qin, "An efficient conditionally anonymous ring signature in the random oracle model," *Theoretical Computer Science*, vol. 461, pp. 106–114, 2012.

[24] Dan Boneh and Matt Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001, Satan Barbara*. Springer, 19.-23., Aug., 2001, pp. 213–229.

[25] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on computing*, vol. 18, no. 1, pp. 186–208, 1989.

[26] Jan Camenisch and Markus Stadler, "Efficient group signature schemes for large groups," in *Advances in Cryptology CRYPTO'97, Santa Barbara*, pp. 410–424. Springer, 17.-21., Aug., 1997.

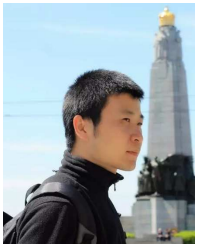
[27] Dan Boneh and Xavier Boyen, "Short signatures without random oracles," in *Advances in Cryptology-EUROCRYPT 2004, Interlaken*. Springer, 2. -6. May, 2004, pp. 56–73.

[28] Yu Inamura, Takehiro Nakayama, and Atsushi Takeshita, "Trusted mobile platform technology for secure terminals," *NTT DoCoMo Technical Journal*, vol. 7, no. 2, pp. 25–29, 2005.

[29] Sid Stamm, Nicholas Paul Sheppard, and Reihaneh Safavi-Naini, "Implementing trusted terminals with a and sitdrm," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 1, pp. 73–85, 2008.

[30] David Pointcheval and Jacques Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[31] Ben Lynn, "Pbc library," *Online: http://crypto. stanford. edu/pbc*, 2006.



Zhiyuan Sui received his Master degree in computer science from Xidian University, Xi'an, China in 2011 and the Bachelor degree in mathematics form Shandong Jianzhu University, Ji'nan, China in 2008. He is currently working as a scientific assistant at the Computer Networks and Computer Communications group of Prof. De Meer. His research interests include applied cryptography, privacy preservation, and security in critical infrastructure (Smart Grid). He is currently involved in the EU FP7 project HyRiM(Hybrid Risk Management).

Michael Niedermeier received his diploma in computer science from the University of Passau, Germany, in 2009. He is working as a research associate at the Group of Computer Networks and Computer Communications and at the Institute of IT Security and Security Law (ISL) at the University of Passau since 2009. His main research areas focus on system modeling, novel performability enhancements, as well as functional safety and security in distributed systems such as the smart grid.

Hermann de Meer received his PhD degree in Computer Science from the University of Erlangen-Nuremberg (Germany). He held postdoctoral research positions at Hamburg University (Germany), University of Texas at Austin (USA), Duke University (USA) and Columbia University (USA). After his Readership at University College London (UCL) (UK) he was appointed as Professor at the University of Passau (Germany) in 2003. His area of research comprises Computer Networking and Energy Systems. Special focus has been on Network Virtualization, IT-Security of the Smart Grid, Demand Side Management, E-Mobility, Industry Automation, Resilience and Risk Management of Distributed Systems.