Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication

Prosanta Gope and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—Information and Communication Technologies (ICT) are one of the underpinning platforms of smart grids, facilitating efficient grid management and operation, optimization of resource utilization, as well as enable new products, features, and services. However, this interconnection of grid technology with ICT leads to various security challenges in the power grid. One such concern is the tampering of usage data from smart meters which may result not only in incorrect billing, but also in incorrect decisions related to demand and supply management. In addition to network based cyber attacks, smart meters are also susceptible to physical attacks since they are installed in customer premises without hardware protection mechanisms. In this paper, we propose a novel privacy-aware authenticated key agreement scheme which can not only ensure secure communication between the smart meters and the service provider, but also the physical security of smart meters. In this regard, we utilize the lightweight cryptographic primitives such as Physically Uncloneable Functions (PUFs) and one-way hash function, etc. Hence, the proposed scheme is suitable even for the resource constrained smart meters.**

***Index Terms*—Privacy-aware, Mutual authentication, Physically uncloneable functions, Fuzzy extractor, Smart grids.**

I. Introduction

Worldwide demand for electric energy is expected to rise 82 percent by 2030 [1]. This demand will primarily be met by building many new coal and natural gas electricity generation plants. Not surprisingly, global greenhouse gas emissions are estimated to rise 59 percent by 2030 as a result. New technology and stricter policies will transform energy industry as "phenomenal" growth in solar and wind power continues. To minimize the need for additional generators, power grids use demand-response management to improve energy efficiency and reduce overall electricity consumption. In this regard, smart grids have emerged as a promising technology to manage the many different forms of renewable energy sources that will be connected to the power grid in the future, from multitudes of household solar panels to vast offshore wind farms. Smart grids are gaining popularity in both academia and industry because of the increased grid reliability and other potential benefits that they offers to the customers. In general, smart grids use advanced Information and Communication Technologies for two-way communication between end users and utility service providers. ICT can be viewed as an essential enabler of smart grids for offering a reliable and cost-effective demand-response management between the customers and the service provider.

Although the integration with ICT offers several benefits in smart girds, it also leads to various security and privacy challenges. For instance, to maintain proper balance between demand and generation of energy, both the customers and the utility service providers need to exchange information. However, an adversary can tamper with or capture this flow of information, which may bring about an imbalance between demand and supply. In addition, the captured information can expose personal information that may be used for targeted advertisements and/or criminal activities. For instance, long-time analysis of the consumers' data can reveal private information related to their daily routines. On the other hand, in order to cheat in billing, an inside attacker in a home or business may try to change the configuration of a smart meter and subject it to physical attacks. Moreover, without hardware protection mechanisms in smart meters, an adversary can obtain secret information (e.g. cryptographic keys) by basic side channel and invasive attacks.

A. Related Work

In recent years, several authentication schemes have been proposed for smart grid environments. Wu et al. proposed a authentication and key distribution scheme for smart grids using elliptic curve cryptography (ECC) [2]. However, Xia et al. pointed out that the scheme presented in [2] is vulnerable to man-in-the-middle attacks and they introduced a new scheme [3]. Subsequently, Park et al. showed that Xia et al.'s scheme cannot ensure security against impersonation attacks [4]. In addition, it also cannot ensure the anonymity of the smart meters. Hereafter, in 2016, Tsai et al. introduced an identity-based signature scheme for smart grids [5]. However, Odelu et al. proved that this scheme cannot provide session key security and also fails to provide strong credentials privacy of the smart meter [6]. Hereafter, few more interesting authentication schemes have been proposed in recent years [7-10]. However, as in [2-6], most of these schemes are based on computationally expensive public-key cryptography which is impractical for the resource constrained smart meters. Furthermore, none of the above existing works has considered the physical security of smart meters, which is greatly important for resisting inside attackers (e.g. a home user) from compromising and controling smart meters for their own profit. Some existing literature has discussed the importance of PUFs in Advance Metering Infrastructure (AMI) [26-28]. However, they do not

P. Gope, is with Department of Computer Science, National University of Singapore, 21 Lower Kent Ridge Rd, Singapore 119077. (E-mail: prosana.nitdgp@gmail.com)

B. Sikdar is with Department of Electrical and Computer Engineering, National University of Singapore, 21 Lower Kent Ridge Rd, Singapore 119077. (Email: bsikdar@nus.edu.sg)

Table I
SYMBOLS AND CRYPTOGRAPHIC FUNCTION

Symbol	Definition
$\mathrm{SID}_{\mathrm{SM}_i}$	Shadow identity of SM_i
CRP(C, R)	Challenge-Response pair
sk	Session key (SM_i -service provider)
PUF_{SM_i}	Physically uncloneable functions of SM_i
$h(\cdot)$	One-way hash function
$\oplus$	Exclusive-OR operation
FE	Fuzzy extractor
||	Concatenation operation

consider the privacy issues in AMI and the noise issues in PUF design, which are greatly important for ensuring secure smart grid communication. Finally, we note that network anonymization systems like Tor may also be used to provide user privacy [29]. However, these anonymity systems are known to be vulnerable to malicious relay nodes. Besides, most of these systems are based on public-key cryptosystems. Hence, they are ill-suited for resource constraints smart meters.

B. Our Contribution

This paper seeks to address all the above issues by proposing an anonymous authenticated key agreement scheme for secure communication in smart grids using computationally inexpensive primitives based on PUFs [15-16]. The key contributions of this paper can be summarized as follows:

- A novel privacy-preserving authentication protocol using PUFs, which can provide several key security properties including resilience against man-in-the-middle attacks, resilience against DoS attacks, and forward secrecy, which are all requirements for secure smart grid communication. One of notable features of the proposed scheme is that it does not require any secret key to be stored on the smart meter but it still can ensure the desired level of security.
- Elimination of noise in the PUF response from the resource constrained PUF-enabled smart meters by using the concept of *fuzzy extractors*.
- A formal security analysis using sequence of games.
- A comparative study of the proposed scheme with closely related existing schemes. It is shown that the proposed scheme is secure and computationally efficient, and requires significantly lower overhead for establishing a session key between a smart meter and the service provider, as compared to the related existing schemes.

The rest of the paper is organized as follows. In Section II we provide a brief introduction to PUFs and fuzzy extractors. In Section III we present the proposed privacy-aware authenticated key agreement scheme for smart grids. Security of the proposed scheme is analyzed in Section IV. A performance analysis is provided in Section V with concluding remarks in Section VI. The symbols and cryptographic functions of the proposed scheme are defined in Table I.

II. PRELIMINARIES

A. Fuzzy Extractor

A (d, λ, ϵ) fuzzy extractor is composed with two algorithms: FE.Gen and FE.Rec [11-13]. FE.Gen is a probabilistic key generation algorithm, which takes a bit string R as input and outputs a key K and helper data hd, i.e., $(K, hd) = \mathrm{FE.Gen}(R)$. On the other hand, FE.Rec is a deterministic reconstruction algorithm that recovers the key K from the noisy input variable R' and the helper data hd, i.e., $K = \mathrm{FE.Rec}(R^{'}, hd)$, if the hamming distance between R' and R is at most d. A fuzzy extractor (FE) ensures security in the extraction of a strong cryptographic key if the min-entropy of the input R is at least λ, and K is statistically ϵ-close to an uniformly distributed random variable in $\{0, 1\}^k$. Since repeated exposure of the helper data may result in additional min-entropy loss [14],[17], the helper data should not be exposed during the execution of the authentication protocol. A (d, λ, ϵ) fuzzy extractor is said to be secure if the following condition holds:

1. $\Pr[K = \mathrm{FE.Rec}(R^{'}, hd) | (K, hd) \leftarrow \mathrm{FE.Gen}(R), \mathrm{HD}(R, R^{'}) \leq d] = 1$, where HD represents the hamming distance.

2. If the min-entropy $\tilde{H}_\infty(R) \geq \lambda$, then $(K, hd) \leftarrow FE.Gen(R)$ is statistically ϵ-close to $(K^{'}, hd)$, where $K^{'} \leftarrow \{0, 1\}^{|K|}$.

B. Physically Uncloneable Function

In this subsection, we provide a brief description of PUFs. A PUF is characterized by a challenge-response pair (*CRP*). It is an integrated circuit (IC) which takes a string of bits as an input challenge and produces a string of bits called the response. The response R of a PUF PUF to a challenge C can be represented as follows: $R = PUF(C)$. A PUF exploits the uniqueness of the physical micro-structure of the IC that is created during the manufacturing process to ensure that no two PUFs are the same. As the PUF output depends on the physical characteristics of the IC, any attempt to tamper with the PUF changes its behavior and renders the PUF useless. Due to this unique property, PUFs have gained popularity as an important paradigm for physical security of resource constrained devices. However, the noise in a PUF's output that results from environmental conditions (e.g. temperature) is still a limiting factor in PUF design, and may result in one or more of the output bits of the PUF being incorrect for any challenge. To address this issue, the concept of fuzzy extractor has been introduced. A $(d, n, l, \lambda, \epsilon)$-secure PUF needs to hold the following requirements:

1) For any two PUFs $PUF_1(\cdot)$ and $PUF_2(\cdot)$, and for any input $C_1 \in \{0, 1\}^k$, $\Pr[\mathrm{HD}(PUF_1(C_1), PUF_2(C_1)) > d] \geq 1 - \varepsilon$.
2) For any PUF $PUF_i(\cdot)$ and for any input $C_1, \cdots, C_n \in \{0, 1\}^k$, $\Pr[\mathrm{HD}(PUF_i(C_1), PUF_i(C_2)) > d] \geq 1 - \varepsilon$.
3) For any two PUFs $PUF_i(\cdot)$ and $PUF_{i*}(\cdot)$, and for any inputs $C_1, \cdots, C_n \in \{0, 1\}^k$, $\Pr[\hat{H_\infty}(PUF_i(C_k), PUF_i*(C_j))_{1 \leq j,k \leq n, i \neq i*, j \neq k} > \lambda] \geq 1 - \varepsilon$. This condition denotes that during the evaluation of different PUFs using multiple inputs, the

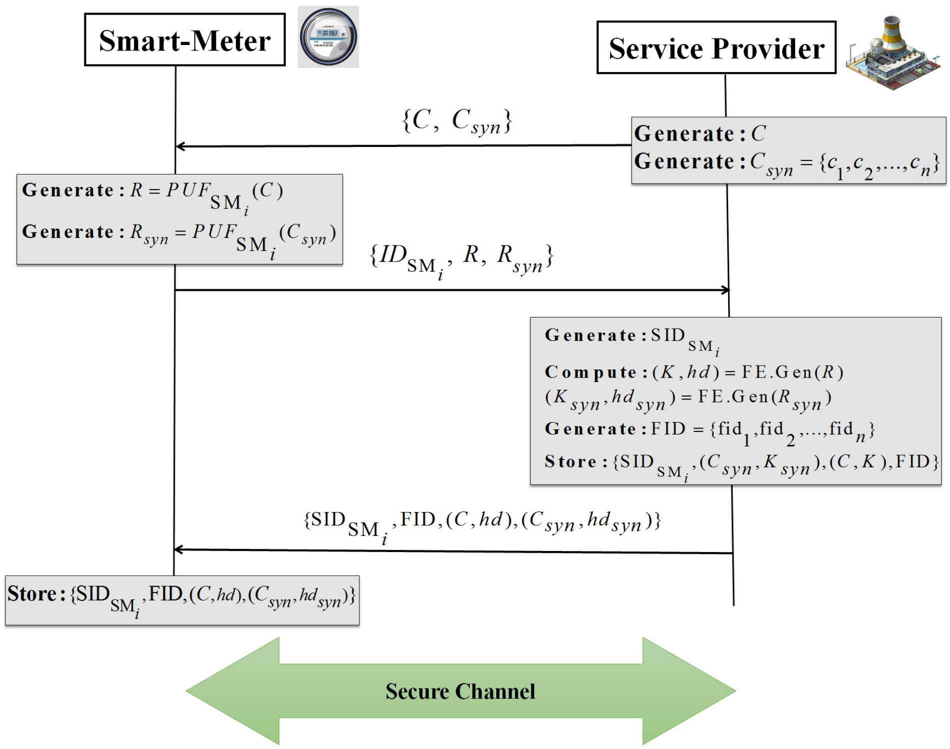

Figure 1. Setup phase of the proposed privacy-aware authenticated key agreement scheme.

min-entropy of the PUF outputs must be larger than λ with high probability [23], when the intra-distance, i.e., the distance between two PUF responses from the same PUF instance and using the same challenge is smaller than d, and the inter-distance, i.e., the distance between two PUF responses from different PUF instances using the same challenge, is greater than d.

C. Pseudorandom Functions

A pseudorandom function PRF:$\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^{k'}$ which takes a secret security parameter $K \epsilon \{0,1\}^k$ and a message $M \epsilon \{0,1\}^*$ as input and provides an arbitrary string PRF(K, M) which is indistinguishable from random string. Now, assuming that h be a polynomial-time computable pseudorandom function. For distinguishing h, a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ may request polynomial bounded queries with its selected inputs and obtain the outputs computed by h for training. After the training phase, $\mathcal{A}$ is given a function, which is either h or a truly random function. We say that h is a pseudo-random function, if it is indistinguishable from a truly random function under $\mathcal{A}$. Namely, $\mathcal{A}$ is given either h or a truly random function according to a random bit {0, 1} and it has only the probability $\frac{1}{2} + \varepsilon$, to distinguish h.

III. Proposed Scheme

In this section, we present the proposed anonymous authenticated key agreement scheme for secure communication in smart grid systems. The proposed scheme consists of two phases: setup phase and authentication phase.

A. Setup Phase

During meter installation, the utility service provider first randomly generates a challenge C and also a set of synchronization challenges $C_{syn} = \{c_1, c_2, \cdots, c_n\}$ which are later used to address any desynchronization between the service provider and the smart meter. Hereafter, the service provider sends $\{C, C_{syn}\}$ to smart meter SM_i through a secure channel. Then, the smart meter extracts the PUF outputs $\{R, R_{syn}\}$ by using the unique embedded physical function PUF_{SM_i} and sends $\{ID_{\mathrm{SM}_i}, R, R_{syn}\}$ to the service provider, where ID_{SM_i} is the identity of SM_i, through the secure channel. Then, the service provider randomly generates a shadow identity $\mathrm{SID}_{\mathrm{SM}_i}$ and a set of unlinkable fake identities $\mathrm{FID} = \{\mathrm{fid}_1, \cdots, \mathrm{fid}_n\}$, and calculates $(K, hd) = \mathrm{FE.Gen}(R)$ and $(K_{syn}, hd_{syn}) = \mathrm{FE.Gen}(R_{syn})$. After that, the service provider sends $\{\mathrm{SID}_{\mathrm{SM}_i}, \mathrm{FID}, (C, hd), (C_{syn}, hd_{syn})\}$ to the smart meter through the secure channel. Finally, the service provider stores $\{\mathrm{SID}_{\mathrm{SM}_i}, \mathrm{FID}, (C, hd), (C_{syn}, hd_{syn})\}$ for further communication with smart meter SM_i. Details of this phase are depicted in Figure 1.

B. Authentication Phase

The authentication phase of the proposed scheme consists of the following steps:

Step 1: Smart meter SM_i selects its shadow identity $\mathrm{SID}_{\mathrm{SM}_i}$ from its memory and generates a random number n_s and subsequently sends $\{\mathrm{SID}_{\mathrm{SM}_i}, n_s\}$ to the service provider.

Step 2: Upon receiving the authentication request, the service provider first locates $\mathrm{SID}_{\mathrm{SM}_i}$ in its database and reads (C, K). Next, the service provider generates a random number

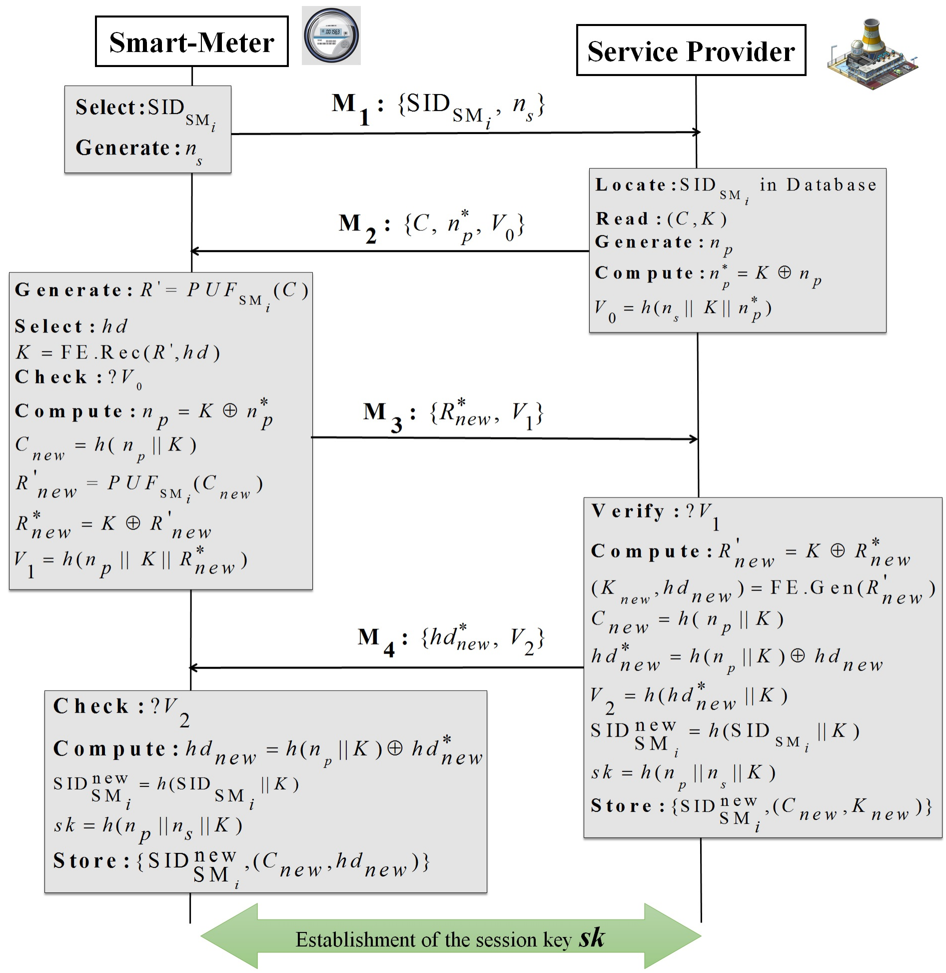

Figure 2. Proposed privacy-aware authenticated key agreement scheme.

n_p and calculates $n_p^* = K \oplus n_p$ and a key-hash response $V_0 = h(n_s||K||n_p^*)$. It then composes a response message $\mathrm{M}_2 : \{C, n_p^*, V_0\}$ and sends it to SM_i.

Step 3: After receiving the response message M_2, SM_i first extracts the PUF response $R^{'} = PUF_{\mathrm{SM}_i}(C)$ and selects the helper data hd from its memory and computes $K = \mathrm{FE.Rec}(R^{'}, hd)$ for reconstructing the key K. After that, SM_i computes and checks the key-hash response parameter V_0. If the verification is successful, SM_i calculates $n_p = K \oplus n_p^*$, $C_{new} = h(n_p||K)$, $R^{'}_{new} = PUF_{\mathrm{SM}_i}(C_{new})$, $R^*_{new} = K \oplus R^{'}_{new}$, and the key-hash response $V_1 = h(n_p||K||R^*_{new})$. It then composes a message $\mathrm{M}_3 : \{R^*_{new}, V_1\}$ and sends it to the service provider.

Step 4: Upon receiving message M_3, the service provider first checks whether the key-hash response parameter V_1 is valid or not. If so, then the service provider calculates $R^{'}_{new} = K \oplus R^*_{new}$, $(K_{new}, hd_{new}) = \mathrm{FE.Gen}(R^{'}_{new})$, $C_{new} = h(n_p||K)$, $hd^*_{new} = h(n_p||K) \oplus hd_{new}$, $V_2 = h(hd^*_{new}||K)$, $\mathrm{SID}^{\mathrm{new}}_{\mathrm{SM}_i} = h(\mathrm{SID}_{\mathrm{SM}_i}||K)$, and $sk = h(n_p||n_s||K)$ and composes a message $\mathrm{M}_4 : \{hd^*_{new}, V_2\}$ and sends it to SM_i.

Step 5: After receiving message M_4, smart meter SM_i first computes and validates V_2. If the validation is successful, then SM_i calculates $hd_{new} = h(n_p||K) \oplus hd^*_{new}$, $\mathrm{SID}^{\mathrm{new}}_{\mathrm{SM}_i} = h(\mathrm{SID}_{\mathrm{SM}_i}||K)$, and the session key $sk = h(n_p||n_s||K)$. In this way, both SM_i and the service provider establish a session key for their secure communication. Next, SM_i updates its memory with $\{\mathrm{SID}^{\mathrm{new}}_{\mathrm{SM}_i}, (C_{new}, hd_{new})\}$ for the next interaction with the service provider.

Note that if any step of the above validation process is unsuccessful, both SM_i and the service provider will abort the execution of the protocol. In case of loss of synchronization between smart meter SM_i and the service provider (which can be detected if SM_i does not get any response from the service provider or if the service provider cannot recognize SM_i), SM_i selects one of the unused fake identities (say fid_j) from $\mathrm{FID} = \{\mathrm{fid}_1, \cdots, \mathrm{fid}_n\}$. It then sends fid_j and a random number n_s to the service provider. On receiving this message, the service provider selects one of the unused pairs of $(c_j, k_j) \in (C_{syn}, K_{syn})$ and sends c_j to SM_i. Then, SM_i locates hd_j in its memory and uses its PUF and FE.Rec to obtain the keying element k_j. At the end of the authentication process, SM_i deletes $\{\mathrm{fid}_j, (c_j, hd_j)\}$ from its memory, and similarly the service provider deletes $\{\mathrm{fid}_j, (c_j, k_j)\}$ from its database. It should be also noted that in the proposed authentication scheme, SM_i is allowed to use almost x FID and (C_{syn}, K_{syn}) pairs, where $x < n - 1$. After that, SM_i needs to request the service provider for a new set of FIDs and (C_{syn}, K_{syn}) pairs. In this regard, SM_i needs to send its $(x+1)$-th fake identity along with a random number n_s and a "Re-Load" message in the authentication request M_1. On seeing the "Re-Load" indication in M_1, and after the authentication and key-establishment process, the service provider will use the session key sk to provide the new set of FIDs and (C_{syn}, hd_{syn}) pairs to SM_i. In this way, we can address the issue of desynchronization or DOS attacks without compromising the privacy of smart meter SM_i and without executing the setup phase on a regular interval. Details of this phase are shown in Figure 2.

IV. Security Model and Analysis

This section first describes the theoretical security and privacy model used for evaluating our proposed scheme. Then we use these models to analyze the security and privacy of the proposed scheme.

A. Security Model

Consider a set of smart meters $\mathcal{M} = \{M_1, M_2, \cdots, M_n\}$ that interact with the service provider S. S initially executes $\mathrm{Setup}(1^k)$ and produces a public parameter pp and a shared secret parameter sp. Here, pp denotes all the available public parameters (crypto suites) of the environment (e.g., PUF output length, coding mode, pseudo-random function (PRF) algorithm name, etc.) and sp represents the secret PUF responses. In this setup phase, S communicates with the smart meters in a secure environment and transfers the security credentials to start the authentication process. During the execution of the authentication phase, these parties interact through an insecure network and mutually authenticate each other. At the end, the parties output 1 (acceptance) or 0 (rejection) as the authentication result. The communication sequence between the parties is called a session and each session is distinguished by its session identifier, denoted by sid. We say that a session has a *matching session* if the messages exchanged between S and members of $\mathcal{M}$ are honestly transferred. For the correctness of the proposed scheme, it is imperative that if a session has a *matching session*, then both the smart meter and service provider always accept the session.

In this section, we consider security against the *man-in-the-middle attack*, which is the canonical security level for any authentication protocol. In this regard, the ability of an attacker is modeled by letting the attacker to control all the communication between a smart meter and the service provider. Here, the attacker is allowed to modify messages between a smart meter and the service provider. The authentication outputs for both parties becomes 1 if and only if the communication messages are honestly transferred. In addition to the canonical security requirement for the *man-in-the-middle attack*, in our model we allow the adversary to obtain the memory contents in the non-volatile memory before and after the session (authentication).

Now we consider a security game, denoted by $\mathrm{Exp}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k)$, between a challenger $\mathcal{C}$ and adversary $\mathcal{A}$ against an authentication protocol Π.

$\mathrm{Exp}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k)$:

1) $(pp, sp) \underleftarrow{Random} \mathrm{Setup}(1^k)$;
2) $(\mathrm{sid}^*, M_j) \underleftarrow{Random} \mathcal{A}_1^{\mathrm{Launch},\mathrm{Send}S,\mathrm{Send}\mathcal{M},\mathrm{Result},\mathrm{Reveal}}(pp, S, \mathcal{M})$;
3) $b := \mathrm{Result}(\mathrm{sid}^*, M_j)$;
4) Output: b.

At the end of the setup phase, $\mathcal{A}$ can interact with the smart meter and the service provider and obtain various information by issuing the following oracle queries:

- $\mathrm{Launch}(1^k)$: Launch a service provider unit S to begin a new session with security parameter k.
- $\mathrm{Send}S$: Send a random message m to S.
- $\mathrm{Send}\mathcal{M}(M_j, m)$: Send arbitrary message m to the meter $M_j \in \mathcal{M}$.
- $\mathrm{Result}(\mathcal{P}, \mathrm{sid})$: Output whether the session sid of $\mathcal{P}$ is accepted or not, where $\mathcal{P} \in \{S, \mathcal{M}\}$.
- $\mathrm{Reveal}(M_j)$: Output the entire information contained in the memory of the meter M_j.

The advantage of the adversary $\mathcal{A}$ against the protocol Π, denoted by $\mathrm{Adv}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k)$, is defined as the probability that the game $\mathrm{Exp}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k)$ outputs 1 when sid^* of $\mathcal{P}$ has no matching session.

Definition 1: *An authentication protocol Π is said to be secure against man-in-the-middle attacks with key compromise if for any probabilistic polynomial time adversary $\mathcal{A}$, $\mathrm{Adv}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k)$ is negligible, i.e., $\mathrm{Adv}^{\mathrm{Sec}}_{\Pi,\mathcal{A}}(k) \leq \epsilon$ in k (for large enough k).*

B. Privacy Model

Now we consider indistinguishability-based privacy. In this case, the adversary randomly picks two smart meters and tries to distinguish the communication derived from any one of the two meters. The privacy experiment between the challenger and the adversary $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ is then described as follows:

$\mathrm{Exp}^{\mathrm{IND*-b}}_{\Pi,\mathcal{A}}(k)$:

1) $(M_0^*, M_1^*, st_1) \underleftarrow{Random} \mathcal{A}_1^{\mathrm{Launch},\mathrm{Send}S,\mathrm{Send}\mathcal{M},\mathrm{Result},\mathrm{Reveal}}(pp, S, \mathcal{M})$;
2) $b \underleftarrow{U} \{0,1\}$, $\mathcal{M}' := \mathcal{M}\{M_0^*, M_1^*\}$;
3) $\Pi_0 \underleftarrow{Random} \mathrm{Execute}(S, M_0^*)$, $\Pi_1 \underleftarrow{Random} \mathrm{Execute}(S, M_1^*)$, $st_2 \underleftarrow{Random} \mathcal{A}_2^{\mathrm{Launch},\mathrm{Send}S,\mathrm{Send}\mathcal{M},\mathrm{Result},\mathrm{Reveal}}(S, \mathcal{M}', \mathcal{I}(M_b^*), \Pi_0, \Pi_1, st_1)$;
4) $\Pi_0' \underleftarrow{Random} \mathrm{Execute}(S, M_0^*)$, $\Pi_1' \underleftarrow{Random} \mathrm{Execute}(S, M_1^*)$;
5) $b' \underleftarrow{Random} \mathcal{A}_3^{\mathrm{Launch},\mathrm{Send}S,\mathrm{Send}\mathcal{M},\mathrm{Result},\mathrm{Reveal}}(S, \mathcal{M}, \Pi_0', \Pi_1', st_1)$
6) Output b'.

At the end of the setup phase, the adversary $\mathcal{A}_1$ issues the oracle queries and sends the queries containing (M_0^*, M_1^*) to the challenger $\mathcal{C}$. After that, $\mathcal{C}$ flips a random coin $b \underleftarrow{U} \{0,1\}$ and permits the adversary to anonymously interact with M_b^*. For the accomplishment of anonymous access, $\mathcal{A}_2$ invokes the $\mathrm{Send}\mathcal{M}$ query with intermediate algorithm $\mathcal{I}$ as the input to honestly transfer the communication message between $\mathcal{A}_2$ and M_b^*. After the challenge phase, $\mathcal{A}_3$ can continuously interact with all meters including (M_0^*, M_1^*) as $\mathcal{A}_1$. Next, M_0^* and

M_1^* call the Execute query to avoid trivial attacks (such as man-in-the-middle attaks) in the symmetric key based construction, and after that, they send their transcripts (Π_0, Π_1) and $(\Pi_0^{'}, \Pi_1^{'})$ of the protocol Π to the adversary. Therefore, the advantage of the adversary in guessing the correct bit can be defined as follows:

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\mathrm{IND}*}(k) := \left|\Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\mathrm{IND}*-0}(k) \to 1] - \Pr[\mathrm{Exp}_{\Pi,\mathcal{A}}^{\mathrm{IND}*-1}(k) \to 1]\right|$$

C. Security Considerations of the Proposed Authentication Scheme

Now we analyze the security of the proposed authentication protocol by using the above models.

Theorem 1 (Security). *Consider a (d, n, l, λ, ϵ_1)-secure PUF, and let* FE *be a (d, λ, ϵ_2)-secure fuzzy extractor, and h be a ϵ_3-secure pseudorandom function. Then the proposed protocol is secure against man-in-the-middle attacks with memory compromise. In particular, we have* $\mathrm{Adv}_{\Pi,\mathcal{A}}^{\mathrm{Sec}} \leq l.n(\epsilon_1 + \epsilon_2 + \epsilon_3)$.

Proof. The objective of adversary $\mathcal{A}$ is to violate the security experiment. In this context, the goal of $\mathcal{A}$ is to convince the smart meter or the service provider to accept the session without any matching session, especially when the communication is altered by the adversary. Now the following game transformations is considered. Let X_i be the advantage of the adversary at winning the game in Game *i*.

Game 0. It specifies the original game between the challenger $\mathcal{C}$ and the adversary.

Game 1. $\mathcal{C}$ randomly guesses the meter $M^* \overset{U}{\leftarrow} \{M_1, \cdots, M_n\}$. $\mathcal{C}$ aborts the game if the adversary has a different sid^* and/or the adversary does not impersonate M^*.

Game 2. Let l be the maximum number of sessions that the adversary can establish in the game. For $1 \leq j \leq l$, we verify or alter the related parameters of the session between the service provider and M^* up to the l-th session as per the following games:

- **Game $2-j-1$.** At the j-th session, $\mathcal{C}$ evaluates the output of the PUF implemented in M^*. $\mathcal{C}$ aborts the game if the output does not have enough entropy or if it is correlated to the other outputs derived from the inputs to the PUF.
- **Game $2-j-2$.** The output from the fuzzy extractor (K_{syn}, K) is turned into a random bit string.
- **Game $2-j-3$.** In this game the output from the pseudorandom function (PRF), $h(K, \cdot)$ and $h(sk, \cdot)$ is obtained from a truly random function.
- **Game $2-j-4$.** In this game the resultant output from the PRF $h(K_{syn}, \cdot)$ is obtained from a truly random function.
- **Game $2-j-5$.** We change the XORed output $R_{new}^* = K \oplus R_{new}^{'}$ and $hd_i^* = h(sk||N_s) \oplus hd$ to randomly chosen $R_{new}^*, hd^* \overset{U}{\leftarrow} \{0,1\}^{|R_{new}^*, hd^*|}$.

The main idea of the security proof is to modify the messages corresponding to the target smart meter M^* to arbitrary strings. The attacker wins the game and breaks the security of the proposed scheme if he/she can distinguish the random strings from real messages/outputs and/or convince the smart meter or service provider to accept the session while the communication is modified. We proceed with the game transformation starting with the first call of the smart meter M^*. After that, we gradually change the communication message from Game 2-j-1 to Game 2-j-5. We move to the next section, once these transformations are finished. Here, we recursively apply this strategy up to the upper bound l on the number of sessions that the attacker can establish. Through these game transformations, we show that the advantage of the adversary against the authentication protocol can be limited to negligible values as shown in the results of Lemma 1 through 5.

Lemma 1 (Random Guessing): *If there are n smart meters, then $X_0 = nX_1$.*

Sub-Proof: We say that the adversary wins the game when there is a session which the service provider or smart meter accepts, while communication is modified by the adversary. Since we assume that there are at most n smart meters, therefore the probability that the challenger $\mathcal{C}$ can correctly guess the related session is $1/n$.

Lemma 2 (PUF Response): *$X_1 = X_{2-j-1}$ and $X_{2-(j-1)-5} = X_{2-j-1}$ for any $2 \leq j \leq l$, if the PUF used in the smart meters is a $(d, n, l, \lambda, \epsilon_1)$-secure PUF.*

Sub-Proof: Since the PUF used in the proposed protocol is $(d, n, l, \lambda, \epsilon_1)$-secure, it implies that its intra-distance is less than d, the inter-distance is larger than d, and the min-entropy of the PUF is lager than λ. Besides, the PUF also has the desirable property that even if the input to the PUF is exposed, the output derived from the PUF satisfies the sufficient min-entropy property and that makes each output uncorrelated. Here, the challenger does not check the entropy of the output in this game. Now, consider a scenario where an adversary issues the *reveal query* and obtains the stored information from the PUF's memory. In this regard, since X_1, X_{2-j-1} and $X_{2-(j-1)-5}$ use the $(d, n, l, \lambda, \epsilon_1)$-secure PUF, the distance between them is bounded by ϵ_1. Therefore, we can write $|X_1 - X_{2-j-1}| \leq \epsilon_1$ and $\left|X_{2-(j-1)-5} - X_{2-j-1}\right| \leq \epsilon_1$. This means there is no effect on the game transformation.

Lemma 3 (FE Output): *If the* FE *is a (d, λ, ϵ_2)-secure fuzzy extractor, then $X_{2-j-1} = X_{2-j-2}$ for any $1 \leq j \leq l$.*

Sub-Proof: As discussed, the fuzzy extractor is secure if the min-entropy of the PUF input R in the $\mathrm{FE.Gen}(R) = (K, hd)$, is at least λ and K is statistically ϵ_2-close to a uniformly random variable in $\{0,1\}^k$, even if the helper data hd is disclosed. Now, since the PUF provides enought min-entropy λ, the property of the (d, λ, ϵ_2)-fuzzy extractor ensures that the output of the fuzzy extractor is close to a random string. Therefore, no adversary can distinguish the difference between the games X_{2-j-1} and X_{2-j-2}. Therefore, the advantage of the adversary in distinguishing the two games can be represented as $|X_{2-j-2} - X_{2-j-1}| \leq \epsilon_2$.

Lemma 4 (Authentication with Secure PRF): *$\forall\ 1 \leq j \leq l$, $|X_{2-j-2} - X_{2-j-3}| \leq \mathrm{Adv}_{h(.),\beta}^{\mathrm{PRF}}(k)$, where $\mathrm{Adv}_{h(.),\beta}^{\mathrm{PRF}}(k)$ denotes the advantage of β to break the security of the* PRF $h(\cdot)$.

Sub-Proof: If there is a difference between these games, then we can construct an algorithm β which breaks the security of the PRF $h(\cdot)$. β sets up all the security credentials and simulates our protocol except the *i*-th session. β can access the real PRF $h(K,\cdot)$ or a truly random function. When the adversary invokes the *i*-th session, β sends $\{n_p^* \overset{U}{\leftarrow} \{0,1\}^k\}$ as the output of the service provider. When $\mathcal{A}$ sends $n_p^{\#}$ to the service provider, β continues the computations as per the protocol specifications and issues $n_p^{\#}$ to the oracle instead of the normal computation of $h(\cdot)$. Upon receiving V_1, β outputs $\{R^*_{new}, V_1\}$ as the response of the smart meter. When the adversary sends $\{R^{\#}_{new}, V_1^{\#}\}$, β issues $n_p^{\#}$ to the oracle and obtains V_1, which is used to authenticate the smart meter.

If β accesses the real PRF, then this simulation is similar to Game $2-j-2$. Otherwise, it can be argued that the oracle query invoked by β is completely random, where the distribution is equivalent to Game $2-j-3$. Therefore, we can write $|X_{2-j-2} - X_{2-j-3}| \le \text{Adv}^{\text{PRF}}_{h(\cdot),\beta}(k)$.

Lemma 5 (Secure PRF): $\forall 1 \le j \le l$, $|X_{2-j-3} - X_{2-j-4}| \le \text{Adv}^{\text{PRF}}_{h(\cdot),\beta}(k)$.

Sub-Proof: This lemma can be proved in a way similar to the proof for Lemma 4.

Lemma 6 (Random String): $\forall\ 1 \le j \le l$, $X_{2-j-2} = X_{2-j-4} = X_{2-j-5}$.

Sub-Proof: The fuzzy extractor FE and the PRF $h(\cdot)$ are already changed to the truly random function in the above games. Therefore, K and $h(K||n_p)$ are used as an effective one-time pad to encode $R^{'}_{new}$ and hd_{new}, respectively. Therefore, no adversary can differentiate $R^*_{new} = K \oplus R^{'}_{i+1}$ and $hd^*_{new} = h(K||n_p) \oplus hd_{new}$ from a randomly chosen string.

Theorem 2 (Privacy): *Consider a* $(d, n, l, \lambda, \epsilon_1)$*-secure physically uncloneable function,* and let FE *be a* (d, λ, ϵ_2) fuzzy extractor, and let h be a ϵ_3-secure pseudorandom function. Then our protocol satisfies the indistinguishability-based privacy property.

Proof: The proof of this theorem is similar to that for Theorem 1. In Theorem 1, we have shown that that the proposed authentication protocol is secure against any forgery attacks. According to the game transformation described in the proof of Theorem 1, if we repeatedly modify the messages communicated for the smart meters M_0^* and M_1^*, then the entire transcript will be identical to random strings. Thus, no information that identifies the challenger's coin will be leaked. Also, all the parameters stored in the smart meter such as $\{\text{SID}_{\text{SM}_i}, \text{FID}, (C, K), (C_{syn}, K_{syn})\}$ are randomly generated and each pair can only be used once. Hence, these parameters do not provide any information about the smart meter. The probability that the challenger can identify M_0^* and M_1^* so that the game transformation is finished within a polynomial time is $1/n^2$. Therefore, we can argue that our proposed scheme satisfies indistinguishability-based privacy.

D. Informal Security Analysis

1) *Protection Against Impersonation Attacks*: In the proposed scheme, if an adversary tries to impersonate as a legitimate smart meter SM_i, then he/she needs to send a valid authentication request $\text{M}_1 : \{\text{SID}_{\text{SM}_i}, n_s\}$ and a valid response message $\text{M}_3 : \{R^*_{new}, V_1\}$. However, since the PUF and the micro-controller of the smart meter are considered to be inseparable [18], the adversary does not have access to the PUF. Therefore, he/she cannot compute $R^{'} = PUF_{\text{SM}_i}(C)$, $K = \text{FE.Rec}(R^{'}, hd)$, $n_p = K \oplus n_p^*$, $C_{new} = h(n_p||K)$, $R^{'}_{new} = PUF_{\text{SM}_i}(C_{new})$, $R^*_{new} = K \oplus R^{'}_{new}$, and $V_1 = h(n_p||K||R^*_{new})$. As a result, the adversary cannot create a valid response message $\text{M}_3 : \{R^*_{new}, V_1\}$, which is essential to convince the service provider. On the other hand, if the adversary tries to impersonate as a legitimate service provider, then he/she needs to know the secret K. Without knowing the secret K, the adversary cannot generate a valid key-hash response $V_0 = h(n_s||K||n_p^*)$ and $V_2 = h(hd^*_{new}||K)$. In this way, we ensure security against impersonation attacks.

2) *Anonymity of the Smart Meter*: In the proposed scheme, the smart meter needs to use a valid shadow identity SID_{SM_i} for each session, and a shadow identity SID_{SM_i} cannot be used twice. Therefore, no one except the service provider can recognize the activity of a smart meter. Besides, in case of loss of synchronization, the smart meter needs to use one of the unused fake identities fid_j from $\text{FID} = \{\text{fid}_1, \cdots, \text{fid}_n\}$. After that, the smart meter needs to delete the chosen fid_j from its memory. Therefore, changing the pseudonym in each session ensures identity intractability. This approach of the proposed scheme helps to achieve privacy against eavesdropper (PAE).

3) *Protection Against Physical Attacks*: Suppose an inside adversary (e.g. a consumer) intends to perform physical tampering on the smart meter in order to influence the consumption reading and thus the electricity bill. However, any such attempt to tamper with the PUF changes the behavior of the device and renders the PUF useless. As a result, the PUF will not be able to produce the desired output $R^{'} = PUF_{\text{SM}_i}(C)$ during the execution of the proposed authentication protocol. Therefore, the service provider can detect such attempts at tampering. In addition, since PUFs are safe against cloning and a PUF cannot be recreated [19], the proposed scheme is secure against cloning attacks.

4) *Protection Against Replay Attacks*: In the proposed scheme, an adversary cannot reuse the message $\text{M}_1 : \{\text{SID}_{\text{SM}_i}, n_s\}$ since SID_{SM_i} changes in each session.

Table II
PERFORMANCE COMPARISON BASED ON SECURITY FEATURES

Scheme	SP1	SP2	SP3	SP4	SP5	SP6
Wu and Zhou [2]	No	No	No	No	No	No
Xia and Wang [3]	No	No	Yes	No	No	No
Tsai and Lo [5]	Yes	Yes	Yes	Yes	No	No
Odelu et al. [6]	Yes	Yes	Yes	Yes	Yes	No
Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes

SP1: Anonymity of the smart meter; **SP2:** Privacy against eavesdropper; **SP3:** Protection against man-in-the-middle attacks; **SP4:** Forward secrecy; **SP5:** Session key security; **SP6:** Physical security of the smart meter

Table III
PERFORMANCE COMPARISON BASED ON COMPUTATION COST

Scheme	Smart Meter	Service Provider
Wu and Zhou [2]	$3T_{mp}$+T_m+$T_{cert_{gen}}$+T_h	$4T_{mp}$+T_m+$T_{cert_{ver}}$+$4T_h$+T_s
Xia and Wang [3]	T_s+ $4T_h$	T_s+ $4t_h$
Tsai and Lo [5]	$4T_{mp}$+T_e+$5T_h$	$3T_{mp}$+T_e+ $2T_b$+$5T_h$
Odelu et al. [6]	$3T_{mp}$+T_e+ $6T_h$	$2T_{mp}$+T_e+ $2T_b$+$6T_h$
Proposed Scheme	FE.Rec + $5T_h$+T_{PUF}	FE.Gen + $6T_h$
T_{mp}: Execution time of a multiplication point operation; T_m: Execution time of a multiplication operation;		
T_e: Execution time of a modular exponential operation; T_s: Execution time of a symmetric encryption/decryption;		
T_b: Execution time of a bilinear pairing; T_h: Execution time of a hash operation;		
T_{PUF}: Execution time of a PUF operation; $T_{cert_{gen/ver}}$: Execution time of a certificate generation/verification operation		

The adversary cannot reuse message M_2 since a new challenge C is used in each session. Similarly, an adversary also cannot resend the messages M_3 and M_4 since a new response R'_{new} and new helping data hd_{new} are used in each session. In this way, we ensure security against replay attacks.

5) *Session Key Security*: Only a legitimate smart meter SM_i who knows the helper data *hd* can derive $R' = PUF_{SM_i}(C)$, $K = \text{FE.Rec}(R', hd)$, $n_p = K \oplus n_p^*$, and $sk = h(n_p||n_s||K)$. Similarly, only the legitimate service provider who knows the key element K can compute the session key $sk = h(n_p||n_s||K)$. Besides, since the session key is generated based on two random numbers n_p and n_s, and there is no relationship between the session keys. Therefore, if one of the session keys is compromised, it does not help to recover any past or future session keys. In this way, we provide protection against *known session key attacks*.

V. PERFORMANCE ANALYSIS AND COMPARISON

In this section we compare the proposed scheme with other related schemes, such as the schemes of Wu and Zhou [2], Xia and Wang [3], Tsai and Lo [5], and Odelu et al. [6]. In order to analyze the performance of the proposed scheme, particularly on the security front, our scheme has been compared with [2], [3], [5] and [6], by considering the major security properties (shown in Table II). From Table II, we see that the schemes presented in [2] and [3] cannot ensure most of the important security properties such as anonymity of the smart meter, privacy against eavesdropper, etc. Even though Odelu et al.'s scheme can provide several security properties, like other existing schemes, it cannot ensure the physical security of the smart meter, which may allow inside attackers (e.g. home users) to compromise and control the smart meter for their own profit. On the other hand, the proposed PUF-based authentication scheme can ensure all the important security properties (as shown in Table II). Since any attempt at physical tampering of the smart meter will affect the PUF's behavior, the service provider can comprehend such attacks during the execution of the authentication process.

Next, we compare the proposed scheme in terms of the computation cost. From Table III, we can see that both the proposed scheme and the scheme presented in [3] are based on symmetric key cryptographic systems. Hence, they impose lower computational overhead on the smart meter, as compared to the other schemes. Now, for analyzing the performance of the proposed scheme with respect to others, we conducted simulations of the cryptographic operations used in the proposed scheme and [2], [3], [5] and [6] on an Ubuntu 12.04 virtual machine with an Intel Core i5-4300 dual-core 2.60 GHz CPU (operating as the service provider, as per the scheme). To simulate a smart meter, we use a single core 798 MHz CPU and 256 MB of RAM, which is not very different from a real smart meter [20]. The simulation uses the JPBC library Pbc-05.14 [21], and the JCE library [22] to evaluate the execution time of different cryptographic operations used in the proposed scheme and [2], [3], [5], and [6]. Here, for the T_{PUF} operation we consider the simulation result of [24] on a 128-bit arbiter PUF circuit on an MSP430 micro-controller machine with 798 MHz CPU. In addition, for FE.Gen($\cdot$) and FE.Rec($\cdot$) operations, we adopt the code-offset mechanism using BCH code [25]. For symmetric-key based encryption/decryption time T_s, we consider the 256-bit AES-CBC encryption mode.

Table IV
EXECUTION TIME OF VARIOUS CRYPTOGRAPHIC OPERATIONS

Operation	Smart Meter	Service Provider
T_{mp}	5.9 ms	2.6 ms
T_m	22.93 ms	14.5 ms
T_b	9.23 ms	3.78 ms
$T_{cert_{gen}}$	57.63 ms	-
$T_{cert_{ver}}$	-	17.24 ms
T_h	0.026 ms	0.011 ms
T_e	7.86 ms	2.34 ms
T_s	0.079 ms	0.041 ms
T_{PUF}	0. 12 ms	-
FE.Gen (.)	-	1.17 ms
FE.Rec (.)	3.28 ms	-

Now, from Figure 3, we can see that the total computation time for [3] is lower than others. However, this scheme cannot ensure most of the important security features which are desirable for smart grid security (as shown in Table 2). On the other hand, the proposed scheme has significantly lower

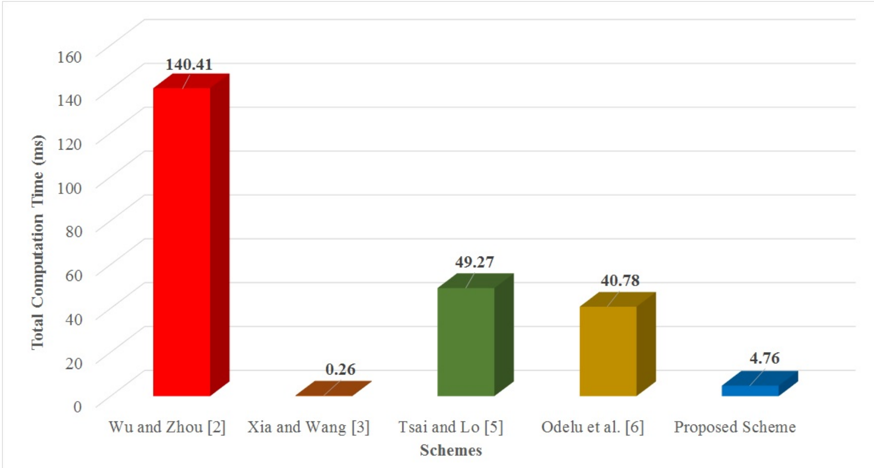

Figure 3. Performance comparison based on execution time.

computational cost than [2], [5], and [6]. In addition, the proposed scheme can ensure all the important security features (including physical security of the smart meter) and is hence well suited for secure communication in smart grids.

VI. Conclusion

In this paper, we presented a novel privacy-aware authenticated key agreement scheme for secure smart grid communication. The proposed scheme allows a legitimate smart meter to anonymously interact with the service provider using a session key. In this context, we utilized lightweight cryptographic primitives such as one-way hash functions, physically uncloneable functions, etc. Unlike existing schemes, the proposed scheme supports the physical security of the smart meters. We conducted security and performance analyses to show that the proposed scheme is secure and has reasonable computational overhead, and is hence better suited for secure smart grid communication.

Acknowledgment

This research was supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

References

[1] International Energy Outlook 2017, Energy Information Administration, U.S. Department of Energy, (https://www.eia.gov/outlooks/ieo/execsumm.php).

[2] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2 no. 2 pp. 371-378 Jun. 2011.

[3] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3 no. 3 pp. 1437-1443 Aug. 2012.

[4] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution proposed by Xia and Wang" *IEEE Trans. Smart Grid*, vol. 4 no. 3 pp. 1613-1614 Sep. 2013.

[5] J.-L. Tsai and N.-W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[6] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, 2016, DOI: 10.1109/TSG.2016.2602282.

[7] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2016.

[8] P. Gope, and B. Sikdar, "An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-based Billing and Demand-Response Management in Smart Grids," *IEEE Internet of Things Journal*,DOI:10.1109/JIOT.2018.2833863, 2018.

[9] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795–1802, 2016.

[10] I. Doh, J. Lim, and K. Chae, "Secure Authentication for Structured Smart Grid System," in International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15), Fukuoka, Japan, 2015, pp. 200–204

[11] Y. Dodis, J. Katz, L. Reyzin, A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," In: Advances in Cryptology (CRYPTO), LNCS, vol. 4117, pp. 232–250. Springer 2006.

[12] Y. Dodis, L. Reyzin, A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *In: Advances in Cryptology (EUROCRYPT)*. LNCS, vol. 3027, pp. 523–540, 2004.

[13] X. Boyen, "Reusable cryptographic fuzzy extractors," *In: ACM Conference on Computer and Communications Security (ACM CCS).* pp. 82–91. ACM 2004.

[14] J. Delvaux, D. Gu, I. Verbauwhede, M. Hiller, and M-D Yu, "Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications, " *In: Cryptographic Hardware and Embedded Systems (CHES).* LNCS vol. 8913 pp. 412-430, Springer 2016.

[15] G. Suh, S. Devadas, "EPhysical unclonable functions for device authentication and secret key generation," in: Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE, 2007, pp. 9–14.

[16] P.S. Ravikanth, Physical One-Way Functions, Ph.D. thesis, Massachusetts Institute of Technology, 2001.

[17] P. Gope, J. Lee, and T~Q. S. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," *IEEE Transactions on Information Forensics and Security,* vol. 13(11), pp. 2831-2843, 2018

[18] S. Guilley, and R. Pacalet, "SoCs security: a war against side-channels," *Annals of Telecommunications*, vol. 11.pp. 998-1009, 2004.

[19] P. Tuyls, and L. Batina, :RFID-tags for Anti-Counterfeiting, Topics in Cryptology CT-RSA", LNCS vol. 3860, pp. 115-131, San Jose. CA, 2006.

[20] Atmel's family of smart power meters. http://www.atmel.com/products/smart-energy/power-metering/ (accessed on 28 May 2017).

[21] Pbc library. Tech. rep. http://crypto.standford.edu/pbc/(accessed on 16 April 2017).

[22] Oracle Technology Network. Java Cryptography Architecture (JCA). [Online]. Available: http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/CrypoSpec.html, accessed Apr. 20, 2017.

[23] F. Armknecht, D. Moriyama, A.-R Sadeghi, M. Yung, "Towards a unified security model for physically unclonable functions," *In: Sako, K. (ed.)*

CT-RSA 2016. LNCS, vol. 9610, pp. 271-287. Springer, Heidelberg (2016). doi:10.1007/ 978-3-319-29485-8 16

[24] C. Herder, M. D. Yu, F. Koushanfar and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,”*In Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[25] Y. Dodis et al., “Fuzzy extractors: How to generate strong keys from from biometrics and other noise data. *SIAM J. Compt*. vol. 38, no. 1, pp. 97-139, 2008.

[26] https://eprint.iacr.org/2016/009.pdf (accessed on 16 March 2018).

[27] S. Ryu, “PUF based Smart Meter Security with Sx Chain,” *International Journal of Control and Automation*. vol. 9(9), pp. 407-414, 2016.

[28] https://project-sparks.eu/wp-content/uploads/2016/09/03-puf-belfast-workshop-20160826.pdf. (accessed on 16 March 2018)

[29] R. Dingledine, N. Mathewson and P. Syverson, “Tor: The second-generation onion router,” Naval Research Lab Washington DC, 2004.

Prosanta Gope received the M.Tech. degree in computer science and engineering from the National Institute of Technology (NIT), Durgapur, India, in 2009, and the PhD degree in computer science and information engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, in 2015. He is currently working as a Research Fellow in the department of computer science at National University of Singapore (NUS). Prior to this, Dr. Gope served over one year as a Postdoctoral Research Fellow at Singapore University of Technology and Design (SUTD) established in collaboration with Massachusetts Institute of Technology (MIT). His research interests include lightweight authentication, authenticated encryption, access control system, and security in mobile communication and hardware security of the IoT devices. He has authored over 50 peer-reviewed articles in several reputable international journals and conferences, and has three filed patents. He received the Distinguished Ph.D. Scholar Award in 2014 given by National Cheng Kung University, Tainan, Taiwan.

Biplab Sikdar (S’98-M’02-SM’09) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include computer networks, and security for IoT and cyber physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing.