Lightweight Authenticated Key Agreement for Smart Metering in Smart Grid

Seyed Hamid Baghestani, Farokhlagha Moazami, and Mahdi Tahavori

***Abstract*—Nowadays, with the overconsumption of energy, researchers attempt to optimally manage energy consumption and prevent it from being wasted. One beneficial way to manage energy consumption is to integrate the energy grid with information technology, so that data can be exchanged between producers and consumers in a two-way communication network, which is called a smart grid. This data transfer must take place in a secure environment. However, many protocols have been designed to establish a secure channel to transfer data in the smart grid environment, each of which has some disadvantages that still keep the problem open for this field of research. Recently, Kumar *et al.* proposed a lightweight authentication and key agreement protocol based on elliptic curve cryptography (ECC). In this article, we show that the proposed protocol does not provide the anonymity of smart meters and is vulnerable to smart meter tracing attack. We also propose a new lightweight ECC-based authenticated key agreement protocol that is resistant against all known attacks including the attack presented in this article. Also, the proposed scheme is more efficient than the recent related scheme. We show that the proposed protocol is semantically secure and also we simulate our protocol using the AVISPA.**

***Index Terms*—Anonymity, AVISPA tool, key agreement, mutual authentication, semantic security, smart grid, tracing attack.**

I. Introduction

In RECENT years, global warming has increased due to the consumption of fossil fuels, which has caused environmental problems such as climate change. In addition, electricity demand has risen sharply over the years and due to a shortage of fossil fuels and the inefficiency of the traditional network, such a request can only be made with the help of renewable energy sources, as well as the management of energy production and consumption [1]. These problems led to the emergence of the concept of the smart grid, which meets the needs of the two parties by establishing a two-way flow of energy and information [2]. This two-way communication is done through the advanced metering infrastructure (AMI) that includes smart meters, concentrators, and a measurement data management system (MDMS) [3]. The smart grid allows consumers to be informed instantly about their energy consumption and costs. It also enables energy producers to change tariff consumption dynamically according to grid load and also, according to the needs of the network and environmental conditions, use the appropriate energy production resources. In the smart grid, smart meters are responsible for accurately measuring the amount of consumer's consumption [4], [5].

Despite the benefits mentioned above, the data transmitted in smart grid communications have reached the terabyte speed level and misuse of smart meter readings can lead to customer privacy leaks. It can also impose additional load on the energy network by sending manipulated and inaccurate data [6]. Therefore, security is a key factor in a smart grid design. One of the key requirements for a secure platform in the smart grid environment is data encryption that requires mutual authentication and exchange of a session key [7].

One of the major challenges facing security protocol designers in the smart grid context is the limited computing and memory resources, especially on the smart meters side. Therefore, designers should consider that in addition to meet the security requirements, the protocols they design must be as lightweight as possible. Designing one single authenticated key agreement protocol is more lightweight and has less information leakage than one separate authentication protocol and one separate key agreement protocol. Hence, the design of these protocols has attracted the attention of many researchers in this field [8].

Authenticated key agreement schemes include three phases. Setup phase, registration phase, and authentication and key agreement phase that in the setup phase, functions such as hash functions, mathematical group, mathematical field, and pseudorandom generators are selected and publicly announced. During the registration phase, the parties register in trusted third party and private parameters are generated and provided by the parties that are usually performed through a secure channel. In the authentication and key exchange phase, protocol participants will be able to authenticate themselves to each other and share a session key by using information from the previous two phases.

A. Related Work

According to the all requirements needed, Tsai and Lo [9] presented an authentication scheme based on bilinear pairings. Although the anonymity of the smart meter identifier is one of the advantages for their scheme, due to the high computational cost of the bilinear pairings, the proposed method is not optimal to implement on a smart grid platform with limited resource devices. Since their scheme was not secure in the CK-adversary model [10], Odelu *et al.* [11] proposed another scheme based

Manuscript received 2 April 2021; revised 3 November 2021; accepted 30 June 2022. *(Corresponding author: Farokhlagha Moazami.)*

The authors are with the Cyberspace Research Institute, University of Shahid Beheshti, Tehran 1983969411, Iran (e-mail: se.baghestani@mail.sbu.ac.ir; f_moazemi@sbu.ac.ir; m.tahavori@mail.sbu.ac.ir).

Digital Object Identifier 10.1109/JSYST.2022.3188759

on the properties of bilinear pairings and they proved that Tsai *et al.*'s scheme is vulnerable to ephemeral secret leakage attack in CK-adversary model. They showed that with the leakage of the random value in their scheme, the session key, easily, is revealed by the adversary. Similar to Tsai *et al.*'s scheme, their scheme also is not suitable to implement in the smart grid due to the heavy computational costs of bilinear pairings.

To avoid the heavy computational load of bilinear pairings, Mahmood *et al.* [12] proposed a key agreement scheme using elliptic curve cryptography (ECC) [13], [14]. Although they believe their scheme is appropriate to implement on smart grid devices, the identifier's anonymity was not considered and identifiers are easily accessible by the adversary. Since their scheme also was not safe in the CK-Adversary threat model, Abbasinezhad-Mood and Nikooghadam in [15] applied an ephemeral secret leakage attack to obtain the session key. In [15], there is a lot of computation to generate security parameters at the trusted authority (TA) registration phase. Despite a lot of computation, there is still no way to keep the smart meters identifiers secret. Recently, the same authors proposed an anonymous password-based key establishment scheme [16] that does not require communication to the electricity service provider (SP) over the Internet and can be used effectively for the isolated smart meters.

Wazid *et al.* [17] proposed a three-factor authentication protocol that employs fuzzy extractors and biometric properties to authenticate participants and also their scheme supports anonymity and dynamic addition of smart meters in the smart grid. Recently, Khan *et al.* [18] introduced a password-based key agreement protocol using ECC and symmetric operations that is called PALK. Chaudhary [19] showed that login and authentication phase of PALK is incorrect. Chaudhary [19] showed that in the login and authentication phase the initial part (A) needs to multiply two points of an elliptic curve in order to calculate initial message for which there is no algorithm. Besides, part B needs to use public key of part A (PK_A) to authenticate it after receiving initial message to be able to continue executing the protocol. Since there is no information about PK_A in the sent message to B, Part B cannot proceed the protocol. Chaudhry [19], also, proposed a solution to fix flows of PALK.

An authentication and key exchange scheme based on hash functions for Internet of Things proposed by Esfahani *et al.* [20] in which there is a message in each session that is fixed for a particular smart sensor allows the intruder to trace the smart sensor. Zhang *et al.* [21] presented an authentication and key exchange protocol in the smart grid based on hash functions and symmetric cryptography that solved smart meter tracing problem by updating unique and fix data at the end of each session. But to withstand a desynchronization attack, the SP needs to store previous data for each smart meter in its memory. Due to the high number of smart meters, it imposes higher data overhead [22].

Gope and Sikdar [23] proposed an anonymous privacy-aware authenticated key agreement scheme based on physical unclonable function (PUF), which supports the physical security of smart meters. Although their scheme is robust against physical attack and Dolev–Yao adversary model [24], but Tahavori and Moazami [25] showed that their scheme is vulnerable to ephemeral secret leakage attack in the CK-adversary model. Also, it does not provide backward secrecy property in this model. They proposed a new end-to-end key agreement scheme based on PUF and fuzzy extractors, which resistance against physical tampering attacks and also provide security in the CK-Adversary model. Recently, Kaveh and Mosavi [26] designed an authentication scheme based on PUF. In the proposed scheme, smart meter does not require to store any parameter that increases security and reduces the storage burden to zero.

Kumar *et al.* [27] proposed a lightweight authentication and key agreement protocol (LAKA) between smart meter and neighbor area network (NAN) gateway in the smart grid. In their scheme, the NAN gateway performs the offline TA tasks, which means that the parameters of the registration phase of the meters are computed by the NAN. Their design uses ECC-based cryptography with AES as well as MAC; this heterogeneity of encryption functions causes a large amount of memory to be occupied to implement different functions. In this work, we also found that, contrary to the designers' claims, the proposed scheme does not maintain anonymity. Due to the obvious NAN identifier for member smart meters on the network, an internal adversary can trace the rest of the meters and determine whether two sessions belong to one meter or not.

II. Contribution of the Article

In this article, we show that Kumar *et al.*' scheme [27] is vulnerable to smart meter tracing attack and hence vulnerable to proper anonymity and it is also not effective to implement on resource-constrained smart meters. We also propose a new mutual authenticated key agreement scheme based on ECC. We show that the proposed protocol is semantically secure and simulate our protocol using the AVISPA tool. Our scheme improves Kumar *et al.*' scheme in the following six aspects.

1) Resolving the weakness of the Kumar *et al.*'s scheme [27] to provide anonymity and prevent intruders from tracing smart meters.
2) Establishing the security under the CK-adversary model [10].
3) Reducing the use of point multiplication in the elliptic curve on both sides of the protocol. It is an advantage especially on the smart meters, which are devices with limited computational resources.
4) Improving the scalability of the scheme in the face of increased registered meters and optimal utilization of memory resources.
5) Reduction in communication costs.
6) Update the SM secret key at the end of each session.

III. Review of Kumar *Et Al.*'s Scheme

Kumar *et al.*'s scheme [27] consists of three phases: system setup phase, registration phase, and authentication and key establishment phase. In this section, we review the registration and authentication phase of their scheme.

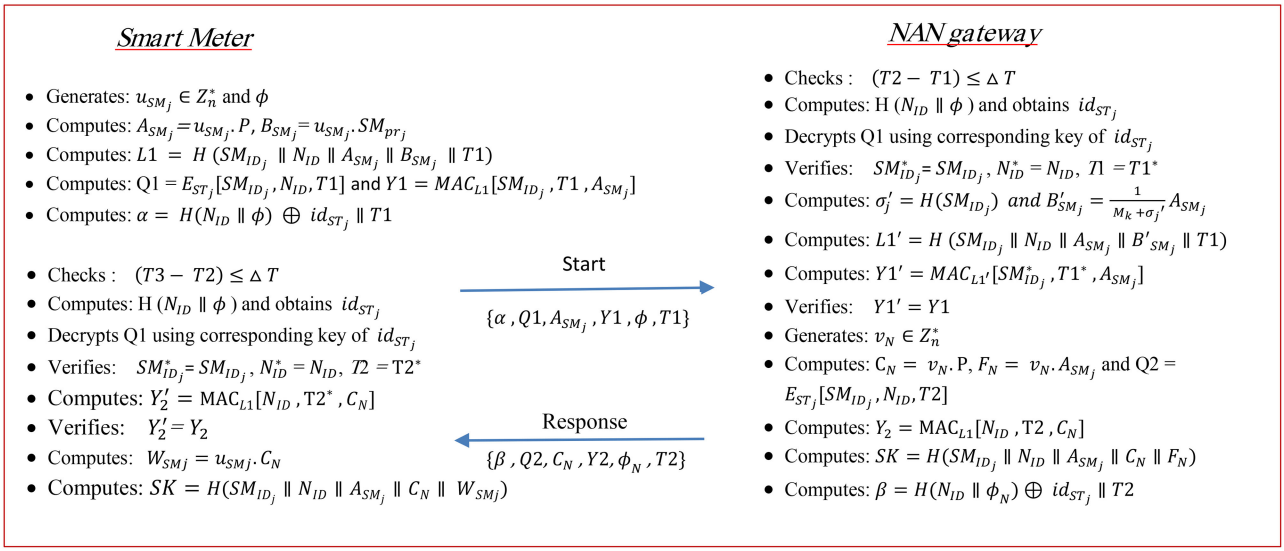

Fig. 1. Flow of the LAKA.

A. Registration Phase

For each SM, (e.g., *j*), first, NAN generates a secret identifier SM_{ID_j} and also generates a secret token ST_j by using its identifier id_{ST_j} and assigns them to the smart meter. NAN uses SM_{ID_j} to calculate $\sigma_j = H(SM_{ID_j})$ and $SM_{pub_j} = (\sigma_j + M_k)P = \sigma_j P + P_s$. Then, NAN uses master key M_k to compute SM's private key $SM_{pr_j} = \frac{1}{M_k + \sigma_j}.p \in G$. Finally, NAN stores all the security parameters including $\{F_p, P, E, n, ST_j, id_{ST_j}, H(), \sigma_j, SM_{pr_j}, N_{ID}, SM_{ID_j}\}$ in secure memory of SM.

B. Authentication and Key Establishment Phase

The steps of this phase are shown in Fig. 1.

IV. Smart Meter Tracing Attack to Kumar *Et Al.*'s Scheme

Tracing attack to Kumar *et al.*'s scheme [27] is applied as follows.

- *Step 1:* The attacker intercepts messages α, ϕ, $T1$ in the first step of the execution.
- *Step 2:* To apply tracing attack, attacker needs to know NAN identity, i.e., NID, which is known by all the SMs in the network. To access N_{ID}, the attacker either can be a known SM of the network or can simply join the network for the purpose of attacking and tracing other meters.
- *Step 3:* Using values α, $\phi, T1$, N_{ID} and equation $\alpha = H(N_{ID} \| \phi) \oplus id_{ST_j} \| T1$), the attacker can easily obtain key identifier of ST_j, i.e., id_{ST_j}.
- *Step 4:* Since id_{ST_j} is provided by NAN to SM at the registration phase and is constant for all sessions of the *j*th meter and NAN, the attacker can trace the SM using id_{ST_j}.

A similar attack can be applied to step 4 of the scheme so that attacker intercepts messages from NAN and obtains id_{ST_j} by using values of β, ϕ_N, $T2$, N_{ID} and equation $\beta = H(N_{ID} \| \phi_N) \oplus id_{ST_j} \| T2$, which makes him able to trace the SM.

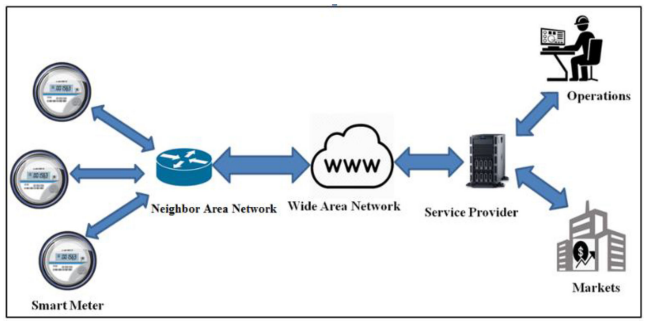

Fig. 2. AMI network model for the proposed scheme.

V. Network Model

As depicted in Fig. 2, the network model used in our proposed scheme adopts smart grid AMI. In terms of network, AMI is a multilayer model that at the lowest level includes a network of smart meters installed in consumer home that is called home area network (HAN). HAN is responsible for transferring consuming data to the AMI and setting data to the smart meters. NAN consists of several HANs and acts as an aggregator to transfer HAN data to the upper layer and vice versa. NANs are connected to the management layer through wide area network. Since the management layer includes MDMS and SP, all the calculations related to electricity bills, electricity distribution, and load balance is done in this layer.

Since our proposed scheme uses timestamp for messages, it is necessary to synchronize the time of participants through a reliable and precise time reference. This time synchronization

TABLE I
SYMBOLS AND DESCRIPTIONS

Symbols	Descriptions
N_{ID}	NAN
SM_{ID_j}	Identity of *j*-th Smart Meter
SM_{s_j}	Smart meter secret key
p, n	Large prime numbers
Fq	A finite field
E	Elliptic curve defined on finite field Fq with prime order n
G	Group of elliptic curve points on E
P	A point on elliptic curve E with order n
H (.)	One-way hash function

could be done by connecting a global positioning system to the network.

VI. THREAT MODEL

A probabilistic polynomial time adversary in Dolev–Yao [24] model has full control of the communication links, which include the ability to read, capture, delete or modify the messages transmitted on the public channel. In order to guarantee that the leakage of some form of secret information stored at a party has the least possible effect on the security of other secrets, in the CK-adversary model, the adversary in addition has the ability to obtain secret information stored in the parties memory via explicit attacks [10]. In the CK-adversary model, the information revealed to the adversary is classified into three categories as follows.

1) Session-state reveal: The internal state of a session (includes ephemeral secret parameters) except the long-term keys is revealed to the adversary.
2) Session-key query: The adversary obtains the session key of a specific session.
3) Party corruption: In this case, the adversary obtains all the internal memory of that party.

According to CK paper [10] in the party corruption, since the attacker obtains all long-term secrets of that party, the attacker can impersonate that party from the time of corruption. In this case, it is important that nothing is learned about the sessions within the corrupted party, which has been kept before party corruption.

VII. PROPOSED AUTHENTICATED KEY AGREEMENT SCHEME

In this section, we propose a new lightweight authenticated key agreement protocol that includes two entities: SM and NAN gateway. In this scheme, NAN is a trusted SP that acts as TA and all smart meters should be registered in NAN. The symbols used in our scheme are defined in Table I.

A. Setup Phase

In this scheme, NAN gateway assigns security parameters to the network members as follows.

First NAN selects an elliptic curve E and a point P of order n on the curve E. Then, it selects a master key M_k and a one-way hash function H_1 and H_2. After that, it stores M_k in its secure database and sends $\{H_1, H_2,\ n,\ E,\ P, F_P\}$ to smart meters.

B. Registration Phase

Smart meters should be registered at the NAN gateway and receive the security parameters. Steps of the registration phase are performed as follows.

Each SM, e.g., *j*th smart meter, selects its secret identity (SM_{ID_j}) and a random number r_1 and sends both of them to NAN. NAN uses SM_{ID_j} and master key M_k to calculate SM's secret key $SM_{s_j} = H_1\ (M_k \parallel N_{ID} \parallel r_1 \parallel SM_{ID_j})$. Then, NAN computes $x_j = SM_{ID_j} \oplus H_1(M_k \parallel N_{ID} \parallel r_1)$ and $y_j = H_1\ (M_k \parallel N_{ID} \parallel x_j) \oplus r_1$ and sends all security parameters including $\{SM_{s_j}, x_j, y_j\}$ to the SM through a secure channel. Finally, NAN stores SM_{ID_j} in its secure memory to recognize the corresponding SM.

C. Authentication and Key Agreement Phase

As shown in Fig. 3, the steps of this phase are performed as follows.

- *Step 1:* First SM selects random numbers r_2 and $u_{SM_j} \in Z_n^*$, then calculates $A_{SM_j} = u_{SMj}.P$, $B_{SM_j} = r_2 \oplus SM_{s_j}$ and $L_1 = H_1(SM_{ID_j} \parallel r_2 \parallel A_{SM_j} \parallel B_{SM_j} \parallel T_1)$. T_1 is the timestamp in SM. Then, it computes $z_j = H_1(SM_{ID_j} \parallel A_{SM_j}) \oplus r_2$ and finally sends start message including $\{A_{SM_j}, x_j, y_j, z_j, L_1, T_1\}$ to the NAN gateway via insecure channel.
- *Step 2:* After receiving the start message from SM, NAN checks the validity of timestamp T_1 and if the condition does not hold, it aborts the protocol execution. Otherwise, NAN calculates $r_1^* = H_1(M_k \parallel N_{ID} \parallel x_j) \oplus y_j$, and using this value, computes $SM_{ID_j}^* = H_1(M_k \| N_{ID} \| r_1^*) \oplus x_j$. Then, using SM identity that stores in the registration phase, it checks condition $SM_{ID_j}^* = SM_{ID_j}$ and if the condition does not hold, it stops the authentication request. Otherwise, using $r_2 = z_j \oplus H_1(SM_{ID_j} \parallel A_{SM_j})$ NAN can computes r_2. Then, NAN computes $B'_{SM_j} = H_1(M_k \parallel N_{ID} \parallel r_1 \parallel SM_{ID_j}) \oplus r_2$ and $L'_1 = H_1(SM_{ID_j} \parallel r_2 \parallel A_{SM_j} \parallel B'_{SM_j} \parallel T_1)$. Finally, it checks $L'_1 = L_1$. If the condition holds it executes the next step.
- *Step 3:* NAN generates random number $v_N \in Z_n^*$ and calculates $C_N = v_N.P$ and $F_N = v_N.A_{SM_j}$ and by replacing r_1 with r_2, updates values of x_j, y_j and SM_{s_j} according to $x_j^+ = SM_{ID_j} \oplus H_1(M_k \parallel N_{ID} \parallel r_2)$, $y_j^+ = H_1\ (M_k \parallel N_{ID} \parallel x_j^+) \oplus r_2$ and $SM_{s_j}^+ = H_1(M_k \parallel N_{ID} \parallel r_2 \parallel SM_{ID_j})$. After that NAN computes $\omega = H_2\,(SM_{ID_j} \parallel C_N \parallel B_{SM_j}) \oplus (x_j^+ \parallel y_j^+ \parallel SM_{s_j}^+)$ to SM can obtain updated values x_j^+, y_j^+, and $SM_{s_j}^+$. Notice that NAN does not need to know or to store values of x_j^+, y_j^+, and $SM_{s_j}^+$. Then, NAN computes $L_2 = H_1(B_{SM_j} \parallel SM_{ID_j} \parallel r_2 \parallel C_N \parallel \omega)$ and session key $(SK) = H_1(SM_{ID_j} \parallel B_{SM_j} \parallel C_N \parallel F_N \parallel r_2)$ and sends response message including $\{C_N, \omega, L_2\}$ to SM.
- *Step 4:* SM computes $L'_2 = H_1(B_{SM_j} \| SM_{ID_j} \| r_2 \| C_N \| \omega)$ and checks the condition $L'_2 = L_2$ and authenticate NAN. If the condition does not hold, the session ends otherwise, computes $W_{SMj} = u_{SMj}.C_N$ and session key

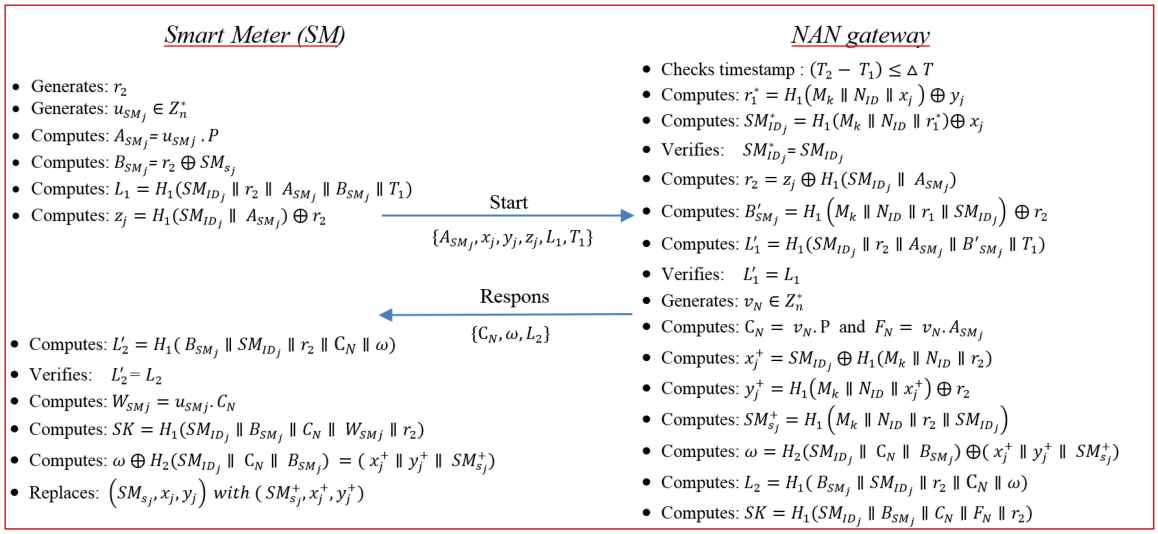

Fig. 3. Authentication and key agreement phase.

$(SK) = H_1(SM_{ID_j} \| B_{SM_j} \| C_N \| W_{SMj} \| r_2)$ to establish a secure communication channel with NAN. Finally, SM computes $\omega \oplus H_2(SM_{ID_j} \| C_N \| B_{SM_j}) = (x_j^+ \| y_j^+ \| SM_{s_j}^+)$ and replaces the values of x_j, y_j, and SM_{s_j} with x_j^+, y_j^+, and $SM_{s_j}^+$.

VIII. Security Analysis

A. Formal Security Analysis

In this section, we present the formal security proof of the proposed protocol under CK-adversary model [10]. In this model, the adversary A can eavesdrop, forge, modify, and intercept all the transmitted messages between the communicating parties and know all the public parameters. The adversary A allowed to communicate with the oracle U through the following queries. Here, U is for SM_i or NAN.

1) $h(m)$: In this query, if $h(m)$ is requested before, the oracle answers it with the previous value. Otherwise randomly chooses a number as the response of this query.
2) Execute(SM_i, NAN): This query simulates the passive attacks, when this query issue by the adversary he/she obtains all the transmitted messages between SM_i and NAN during the execution of the protocol.
3) Send (M, U): This query simulates the active attacks, when the adversary sends the modified message M to U, the oracle U answers it with corresponding messages according to the protocol description.
4) SSReveal(U): If this query is issued by the adversary, then the adversary obtains all the session-specific state information held by the oracle U.
5) SKReveal(U): If this query is issued by the adversary then the adversary obtains the session key held by the oracle U.
6) Corrupt(U): By this query, the adversary A is allowed to learn all long-term private parameters of the entity U.
7) Test(U): This query returns a session key or a random value. When this query is issued, the oracle U tosses a coin b, if $b = 1$ returns the session key otherwise returns a random value.

The oracle instances SM_i and NAN are said to be partner provided that they can authenticate each other and successfully share a session key. A session key SK is called fresh if it is established whenever SSReveal, SKReveal, and Corrupt queries of SM_i and NAN have not been requested. The goal of the adversary A is to distinguish a fresh session key from a random number. The security of the proposed scheme is modeled by the game $Game(U, A)$ in which A can make many queries to U. If the adversary issues a $\text{Test}(U)$ query where the session key is fresh, then the oracle U tosses a coin b. If $b = 1$ returns the session key, otherwise returns a random value. The goal of the adversary is the guessing of bit b rightly. Let $\Pr[Succ]$ be the probability that the adversary A wins the game $Game(U, A)$ then the advantage of A to break the semantic security of our proposed scheme defined as $Adv(A) = |2\Pr[Succ] - 1|$.

Lemma (Difference Lemma): Let A_1, A_2, and A_3 be the event defined in some probability distribution. If $A_1 \wedge \neg A_3 \Leftrightarrow A_2 \wedge \neg A_3$ then $|\Pr[A_1] - \Pr[A_2]| \leq \Pr[A_3]$.

Definition [Elliptic Curve Diffie–Hellman Problem (ECDHP)]: Let G be a cyclic group generated by an elliptic curve point P. For the given points xP, $yP \in G$, finding point xyP is computationally infeasible. Let $Adv_{ECDHP}(A)$ denote the probability of solving ECDHP by a polynomial time algorithm A then $Adv_{ECDHP}(A)$ is negligible.

Theorem: The advantage of the adversary A to break semantic security of the proposed scheme is given by

$$Adv(A) \leq \frac{O(q_s + q_e)^2}{2n} + \frac{O(q_h)^2}{2^l} + \frac{O(q_s)}{2^l} + O(q_h Adv_{ECDHP}(A)) \quad (1)$$

where the adversary can query at most q_e Execute queries, q_s Send queries, and q_h $Hash$ queries.

Proof: To prove the semantic security of the proposed scheme, we define a sequence of games that is started with the real attack G_0 and ended in a game G_4. For each game G_i, we define an event $Succ_i$ in which the adversary, after the $Test$ query, correctly guesses the bit b.

Game $\boldsymbol{G}_0$: This game is the real game against the proposed scheme in the random oracle model. Thus, from the definition, we have

$$Adv\ (A) = \left|2\Pr\left[Succ_0\right] - 1\right|. \tag{2}$$

Game $\boldsymbol{G}_1$: In this game, we simulate all the oracles for each queries as description of the proposed protocol and consider three lists to store the answers of the oracles. Let L_H store answers of the hash queries H_1 and H_2. L_A is to maintain answers of the random oracle queries asked by A and L_T is for the transcript in the channel. Since the oracles are simulated as done in the real attack, we have

$$\Pr\left[Succ_0\right] = \Pr\left[Succ_1\right]. \tag{3}$$

Game $\boldsymbol{G}_2$: In this game, we simulate all the oracles in game G_1 but avoid some collisions occurring in the transcripts and hash queries by the adversary. Games G_1 and G_2 are indistinguishable unless there exists a collision occurrence in the transcripts or hash queries. Using the birthday paradox and since the adversary queries at most q_h hash queries, the probability of occurrence of hash collision is at most $\frac{O(q_h)^2}{2^l}$. Since u_{SM_j} and v_N are chosen randomly from Z_n^*, hence, according to the birthday paradox, in the transcript the probability of occurrence of collision is $\frac{O(q_s+q_e)^2}{2n}$. Therefore, we have

$$\left|\Pr\left[Succ_1\right] - \Pr\left[Succ_2\right]\right| \leq \frac{O(q_s+q_e)^2}{2n} + \frac{O(q_h)^2}{2^l}. \tag{4}$$

Game $\boldsymbol{G}_3$: In this game, we abort the game if A has been lucky and successfully guessed the values L_1 and L_2without oracle queries. This situation only appears in $Send$ queries. Thus, two games G_2 and G_3 are perfectly indistinguishable unless the smart meter rejects L_2 or the NAN gateway rejects L_1. Hence, we have

$$\left|\Pr\left[Succ_2\right] - \Pr\left[Succ_3\right]\right| \leq \frac{O\left(q_s\right)}{2^l}. \tag{5}$$

Game $\boldsymbol{G}_4$: In this game, we consider the session-key security. The security goal is that the adversary A cannot obtain the past session keys except if the secret information of the participants are compromised by the adversary. So, we can consider the following two cases.

- *Case 1:* SSReveal(SM_i) and SSReveal(NAN). In this case, we assume that the adversary A can obtain ephemeral secret keys $\{r_2, u_{SM_j}, v_N\}$ of SM_i and NAN, since the session key computed as $SK = H_1(SM_{ID_j} \parallel B_{SM_j} \parallel C_N \parallel F_N \parallel r_2)$, the adversary A cannot obtain the session key with the available information without obtaining H_1. With this information the adversary cannot obtain SM_{ID_j} and B_{SM_j}, hence cannot compute the session key.
- *Case 2:* (*Perfect Forward Secrecy*): Corrupt(SM_i) and Corrupt(NAN). In this case, we assume that the adversary A can obtain secret parameters of SM_i and *NAN*, i.e., $\{SM_{s_j}, SM_{ID_j}, M_k, N_{ID}\}$. The adversary to compute the session key $SK = H_1(SM_{ID_j} \parallel B_{SM_j} \parallel C_N \parallel W_{SMj} \parallel r_2)$ needs to obtain $W_{SMj} = v_N.u_{SMj}$. P that is equal to solve ECDHP.

So, by the above two cases, we have

$$\left|\Pr\left[Succ_3\right] - \Pr\left[Succ_4\right]\right| \leq O\left(q_h Adv_{ECDHP}\left(A\right)\right). \tag{6}$$

Therefore, we have

$$\begin{aligned}\frac{1}{2}Adv\ (A) &= \left|\Pr\left[Succ_0\right] - \frac{1}{2}\right| \\ &\leq \left|\Pr\left[Succ_0\right] - \Pr\left[Succ_1\right]\right| \\ &\quad + \left|\Pr\left[Succ_1\right] - \Pr\left[Succ_2\right]\right| \\ &\quad + \left|\Pr\left[Succ_2\right] - \Pr\left[Succ_3\right]\right| \\ &\quad + \left|\Pr\left[Succ_3\right] - \Pr\left[Succ_4\right]\right| \\ &\quad + \left|\Pr\left[Succ_4\right] - \frac{1}{2}\right|. \end{aligned} \tag{7}$$

Using (3) and since $\Pr[Succ_4] = \frac{1}{2}$, we conclude that

$$\begin{aligned}\frac{1}{2}Adv\ (A) &= \left|\Pr\left[Succ_0\right] - \frac{1}{2}\right| \\ &\leq \left|\Pr\left[Succ_1\right] - \Pr\left[Succ_2\right]\right| \\ &\quad + \left|\Pr\left[Succ_2\right] - \Pr\left[Succ_3\right]\right| \\ &\quad + \left|\Pr\left[Succ_3\right] - \Pr\left[Succ_4\right]\right|. \end{aligned} \tag{8}$$

Finally, by (4)–(6), we have

$$\begin{aligned}Adv\left(A\right) \leq\ & \frac{O(q_s+q_e)^2}{2n} + \frac{O(q_h)^2}{2^l} + \frac{O\left(q_s\right)}{2^l} \\ & + O\left(q_h Adv_{ECDHP}\left(A\right)\right).\end{aligned}$$

B. Informal Security Analysis

1) Mutual Authentication: In the proposed scheme NAN gateway verifies SM_j by examining the condition $L_1' = L_1$. According to the steps of the proposed scheme, only the authorized SM with the correct SM_{s_j} and SM_{ID_j} is able to calculate correct L_1. Similarly, SM_j verifies the NAN by checking the condition $L_2' = L_2$ and only the authorized NAN with the correct M_k and N_{ID} is able to calculate correct L_2. The session ends as soon as any of the conditions are not met.

2) Replay Attack: In the proposed scheme, all the transmitted messages at each session use timestamp and random numbers so they are different from the other sessions. This freshness of messages is based on random numbers that each party obtains and uses the random value used by the other party, thus deploying old messages would not accept by other party. So our scheme is resistant to replay attack.

3) Man-in-the-Middle Attack (MITM): In MITM attack, the attacker is in the middle of communicating parties and intends

to sabotage and disrupt the normal execution of the protocol by changing and sending messages. Suppose that intruder wants to alter message L_1. Since L_1 includes B_{SM_j} that is calculated using secret key of the smart meter and it is unknown to intruder, the attack fails. Also, the attacker is not able to change any of the messages x_j and y_j. Because, NAN gateway, obtains the secret identity of SM using messages $\{x_j,\ y_j\}$ and its master key M_k, and compares the obtained identity with the identity stored in its database and if condition $SM^*_{ID_j} = SM_{ID_j}$ does not hold, ends the protocol. Furthermore, if the attacker wants to modify or change message z_j, NAN gateway calculates a wrong random number r_2 and as a result the equality $L'_1 = L_1$ does not hold. Similarly, any modification in messages from NAN cannot lead to the equality $L'_2 = L_2$.

4) Impersonation Attack: In the proposed scheme, the attacker will not be able to send a message to the NAN gateway without having SM_{ID_j}, that can pass the equality $L'_1 = L_1$. In addition, if we assume that the attacker has access to the secret smart meter identifier in any way, without the secret key SM_{s_j} and random number r_2, it cannot calculate B_{SM_j} to sent to NAN such that $L'_1 = L_1$. Similarly, an attacker will not be able to send a response message as a legitimate NAN gateway without having the master key M_k and N_{ID} that equality $L'_2 = L_2$ hold.

5) Anonymity and Untraceability: The purpose of the feature is to prevent an attacker from obtaining the actual ID of the smart meters and gateways by intercepting messages transmitted in an unsecure communication channel and also at a higher level, the attacker may not even be able to find any relation between two particular sessions for one smart meter. In this scheme, the actual IDs of the meters are not sent over the unsecure channel without the use of a one-way hash function. They are also merged with random values that cause these values to vary in each session. But to prevent smart meters from being tracked, all messages exchanged at each session need to be different from other sessions. If we consider the messages $\{A_{SM_j}, x_j,\ y_j,\ z_j, L_1, T_1\}$ that is sent by the smart meter in the first step, we find that the messages L_1 and z_j contains random values r_2 and A_{SM_j}, so in each session will be different. And also the values x_j and y_j are updated at the end of each session. Similarly, we can see that messages $\{C_N, \omega, L_2\}$ that are sent from NAN to the smart meter in the second step also use random values and will be different in each session.

6) Forward/Backward Secrecy: Forward/backward secrecy ensures that if adversary obtains the current session key, the security of the next/previous session should not be compromised. In our proposed protocol, all sensitive parameters in session key are protected with the hash function and session key of the other sessions is computed using ephemeral session parameters like B_{SM_j}, C_N, r_2, and F_N of the current session, which are independent of the other sessions.

7) Perfect Forward Secrecy: Perfect forward secrecy means reveal long-term secret parameters of both parties do not lead to reveal previous sessions key. In the proposed protocol, assume that the adversary A access to the memory of SM_i and NAN, which includes $\{SM_{ID_j},\ N_{ID},\ M_k,\ x_j^+,\ y_j^+,\ SM_{s_j}^+\}$. To compute session key $SK = H_1(SM_{ID_j} \parallel B_{SM_j} \parallel C_N \parallel W_{SMj} \parallel r_2)$, the adversary needs to obtain $W_{SMj} = u_{SMj}.C_N = v_N.u_{SMj}.P = v_N.A_{SM_j} = F_N$ that is equal to solve ECDHP.

8) Desynchronization Attack: Where parties need to update their values simultaneously, may be vulnerable to desynchronization attack. In this case, after one party updates its desired values, the attacker forges the communicated data in such a way that the other party cannot update the values simultaneously. In our scheme, the values of x_j, y_j, and SM_{s_j} are updated at the end of the protocol but only smart meters store these values and the second side of the protocol, NAN, does not need to store updated values.

9) Denial-of-Service (DoS) Attack: In the proposed scheme, NAN gateway, at the beginning of the second step checks the validity of data received from SM and terminates the session if it is not approved. Similarly, at the beginning of the third step,

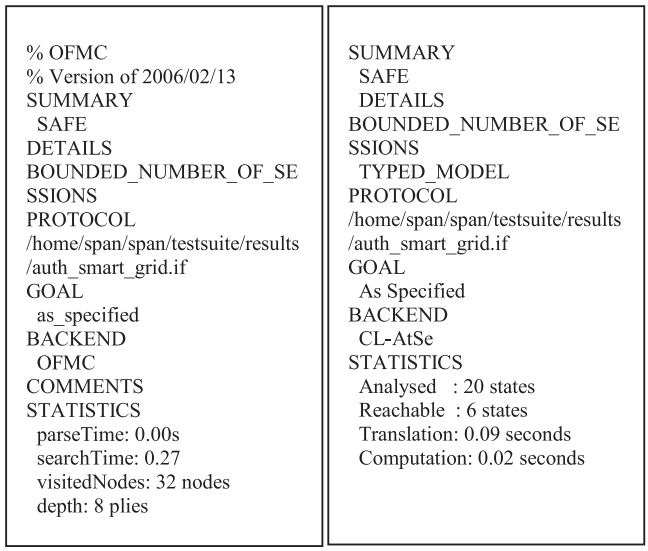

Fig. 4. Output reports of analysis using OFMC and CL-AtSe backends.

TABLE II
EXECUTION TIME OF DIFFERENT CRYPTOGRAPHIC ELEMENTS

Notation	Description	HiPerSmart Card	Pentium IV
TH	general hash operation	~1 ms	~0.01 ms
Tse	symmetric enc/dec	~2 ms	~0.02 ms
Tae	asymmetric enc/dec	~100 ms	~1 ms
Te	exponentiation	~100 ms	~1 ms
Tmp	EC point multiplication	~130 ms	~1.17 ms
Tadd	EC point addition	~10 ms	~0.1 ms
Tb	bilinear pairing	~380 ms	~3.16 ms
TMAC	MAC operation	~1 ms	~0.01 ms

TABLE III
NUMBER OF BITS OF DIFFERENT PARAMETERS

parameters	Value (bits)
Hash (except H_2) and MAC	128
pseudo random number and identifier	128
timestamp	32
ECC point	320

TABLE IV
COMPARISON OF OTHER RECENT PROTOCOLS

Scheme	F1	F2	F3	F4	F5	F6	F7	F8	Smart Meter (SM)	ET (ms)	NAN (SP)	ET (ms)	NoM	CC
[9]	✓	✓	×[39]	✓	✓	×[11]	✓	×	*4Tmp +Te + 5TH*	625	*3Tmp +Te + 2Tb + 5TH*	10.88	3	3456
[11]	✓	✓	×[39]	×[40]	✓	✓	✓	×	*3Tmp +Te + 6TH*	496	*2Tmp + Te + 2Tb + 6TH*	9.72	3	3712
[12]	✓	✓	✓	×[12]	×[15]	×[15]	×	✓	*5Tmp + 2Tadd +4TH*	674	*5Tmp + 2Tadd + 4TH*	6.09	2	1856
[15]	✓	×[41]	✓	×[15]	✓	✓	×	✓	*4Tmp + 2Tadd + 4TH*	544	*4Tmp + 2Tadd + 4TH*	4.92	3	1856
[16]	✓	✓	✓	×[42]	✓	✓	✓	✓	*2Tmp + 4TH*	264	*2Tmp +8TH + 2Tse*	2.46	3	1536
[18]	×[19]	✓	✓	✓	✓	✓	✓	✓	*4Tmp +11TH + 2Tse*	535	*4Tmp +8TH + 2Tse*	4.8	2	2752
[33]	✓	✓	×[39]	✓	✓	✓	✓	×	*2Tmp +Te + 5TH*	365	*3Tmp + Te + Tb + 5TH*	7.72	3	2720
[34]	✓	✓	✓	×[40]	✓	×[43]	✓	×	*4Tmp +1Tadd + 5TH*	535	*6Tmp +2Tadd + 6TH*	7.28	3	1856
[35]	✓	✓	×[39]	×[40]	×[39]	✓	✓	✓	*4Tmp + 1Tadd + 5TH*	535	*4Tmp + 1Tadd + 5TH*	4.83	3	1344
[36]	×[44]	✓	×[44]	✓	✓	✓	✓	✓	*3Te + 3TH*	303	*4Te + 3TH*	4.03	2	2624
[37]	×[45]	✓	✓	✓	✓	✓	✓	✓	*3Tmp + Tadd + 7TH*	407	*3Tmp + Tadd + 7TH*	3.68	3	1760
[38]	✓	✓	✓	✓	✓	✓	✓	×	*3.5Tmp + Tadd + 4TH*	469	*4.5Tmp + 2Tadd + 6TH*	5.525	2	1600
LAKA [27]	✓	✓	✓	×	✓	✓	×	✓	*3Tmp + 4TH + 2TMAC +2Tse*	400	*3Tmp + 5TH +2TMAC +2Tse*	3.62	2	2112
Ours	✓	✓	✓	✓	✓	✓	✓	✓	*2Tmp + 5TH*	**265**	*2Tmp + 11TH*	**2.45**	**2**	**1696**

F1: Impersonation and MITMs resistance; F2: Replay attack resistance; F3: DoS attacks resistance; F4: Anonymity and untraceability; F5: Perfect forward secrecy; F6: Resistance against ephemeral secret leakage attack; F7: Formal security proof; F8: Check with automatic verification tools; ET: Execution Time; NoM: Number of Messages; CC: Communication Cost (bits).

SM checks the validity of data received from NAN. Hence our scheme is resistant against denial of service attack on both sides. Another way of doing a DoS attack is to send old messages. Since our scheme is resistant to replay attack, it can also resist this type of DoS attack.

10) Resistance Against Ephemeral Secret Leakage Attack: If all random session numbers such as r_1, r_2, u_{SMj} and v_N are leaked, all of the sensitive session parameters, such as SM_{ID_j}, SM_{s_j}, M_k, N_{ID}, $SM_{s_j}^+$, x_j^+, y_j^+, L_1, L_2, and B_{SM_j} as well as the session key remain secure.

C. Security Verification Using AVISPA Tool

We analyzed the secrecy and authentication goals by OFMC and CL-AtSe backends in the AVISPA tool [28]–[30]. As depicted in Fig. 4, the output reports are "SAFE." Roles specification for smart meter, session, and environment are written in the HLPSL [29] language.

IX. PERFORMANCE ANALYSIS

Since smart meters are resource-limited devices, security protocols for such devices need to be lightweight in function computation and also optimized in communication cost and data overhead.

A. Computational Costs

To compare the computational cost of the proposed scheme with similar schemes, according to the reports [11], [31], and [32], we use Table II, which shows the execution time of different cryptographic operations. These reports use a Pentium IV computer 3 GHz for SP (NAN) and Philips HiPerSmart card 36 MHz for smart meter. It is clear from Table II that ECC schemes can generally have lower computational cost than bilinear pairings schemes or asymmetric cryptography. But, however, the times of point multiplication operations on the ECC are much longer than operations such as hash. We reduced the used point multiplication operations on the ECC and used lightweight operations such as hash operation. Table IV presents the comparison of our scheme with other schemes in terms of computational costs.

B. Communication Costs

Another criterion for measuring the lightness of schemes is communication costs. That means, how many bits of data have been exchanged. To compare communication costs, we use data in Table III to calculate the number of bits of messages that are transmitted during the authentication phase execution. In the proposed scheme, the messages $start = \{A_{SM_j}, x_j, y_j, z_j, L_1, T_1\}$ and $response = \{\mathrm{C}_N, \omega, L_2\}$ are 864 and 832 b, respectively, and hence, the total communication cost is 1696 b. Table IV presents the comparison of our scheme with other schemes in terms of communication costs.

C. Scalability and Data Overload

Since our scheme does not use symmetric encryption, the secret token ST_j with its identifier id_{ST_j} is not used and NAN just needs to store identifier SM_{ID_j} for each SM in its memory. This is very optimal in terms of scalability and data overload due to the increase in the number of smart meters.

X. CONCLUSION

In this article, the protocol proposed by Kumar *et al.* was analyzed and the security analysis of the protocol showed that their scheme is vulnerable to tracing attack on smart meters. It does not meet proper anonymity and it is also not optimal to implement on smart meters. Then, we proposed a new scheme based on the elliptical curve and evaluated it to meet the security requirements and formally analyzed the security of our proposed scheme by AVISPA tool and showed that the proposed protocol is semantically secure. We showed that our scheme is lightweight and practical in terms of computing, memory usage, and data exchange costs, which makes it suitable to implement in the context of smart energy grids.

REFERENCES

[1] F. Y. Okay and S. Ozdemir, "A fog computing based smart grid model," in *Proc. Int. Symp. Netw., Comput. Commun.*, May 2016, pp. 1–6.

[2] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surv. Tut.*, vol. 16, no. 4, pp. 1933–1954, Oct.–Dec. 2014.

[3] C. Sun, A. Hahn, and C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[4] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renewable Sustain. Energy Rev.*, vol. 59, pp. 710–725, Jun. 2016.

[5] M. E. Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Commun. Surv. Tut.*, vol. 17, no. 1, pp. 179–197, Jan.–Mar. 2015.

[6] L. Zhu *et al.*, "Privacy-Preserving authentication and data aggregation for fog-based smart grid," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 80–85, Jun. 2019.

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

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surv. Tut.*, vol. 16, no. 1, pp. 5–20, Jan.–Mar. 2013.

[9] J. L. Tsai and N. W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[10] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology– Eurocrypt*. Innsbruck, Austria: Springer, 2001, pp. 453–474.

[11] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[12] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Gener. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[13] H. Debiao, C. Jianhua, and H. Jin, "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security," *Inf. Fusion*, vol. 13, no. 3, pp. 223–230, Jul. 2012.

[14] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag, 2003.

[15] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Gener. Comput. Syst.*, vol. 84, pp. 47–57, Jul. 2018.

[16] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Novel anonymous key establishment protocol for isolated smart meters," *IEEE Trans. Ind. Electron.*, vol. 67, no. 4, pp. 2844–2851, Apr. 2020.

[17] M. Wazid, A. K. Das, N. Kumar, and J. Rodrigues, "Secure three factor user authentication scheme for renewable energy based smart grid environment," *IEEE Trans. Ind. Inform.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.

[18] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Elect. Power Energy Syst.*, vol. 121, Oct. 2020, Art. no. 106121.

[19] S. A. Chaudhry, "Correcting PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Elect. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106529.

[20] A. Esfahani *et al.*, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[21] L. Zhang, L. Zhao, S. Yin, C. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," *Future Gener. Comput. Syst.*, vol. 100, pp. 770–778, Nov. 2019.

[22] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, no. 2, pp. 429–443, Dec. 2017.

[23] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jun. 2018.

[24] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[25] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 1616–1628, May 2020, doi: 10.1007/s12083-020-00911-8.

[26] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.

[27] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, Jul. 2019.

[28] "AVISPA: Automated validation of internet security protocols and applicationss." [Online]. Available: http://www.avispa-project.org

[29] "HLPSL Tutorial: A beginner's guide to modeling and analyzing internet security protocols," The AVISPA Team, Jun. 30, 2006. [Online]. Available: http://www.avispa-project.org

[30] L. Lamport, "The temporal logic of actions," *ACM Trans. Program. Lang. Syst.*, vol. 16, no. 3, pp. 872–923, May 1994.

[31] Y. Tseng, S. Huang, T. Tsai, and J. Ke, "List-free ID based mutual authentication and key agreement protocol for multiserver architectures," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 1, pp. 102–112, Jan.–Mar. 2016.

[32] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Inform.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.

[33] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, "An anonymous authentication and key establish scheme for smart grid: FAuth," *Energies*, vol. 10, no. 9, 2017, Art. no. 1354.

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

[35] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[36] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019.

[37] M. Jo, S. Jangirala, A. K. Das, X. Li, and M. K. Khan, "Designing anonymous signature-based authenticated key exchange scheme for IoT-enabled smart grid systems," *IEEE Trans. Ind. Inform.*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021.

[38] M. Qi and J. Chen, "Two-pass privacy preserving authenticated key agreement scheme for smart grid," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3201–3207, Sep. 2021.

[39] A. Braeken, P. Kumar, and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, pp. 2662–2675, Oct. 2018.

[40] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2830–2838, Sep. 2019.

[41] Y. Chen, J. Martínez, P. Castillejo, and L. López, "A bilinear map pairing based authentication scheme for smart grid communications: PAuth," *IEEE Access*, vol. 7, pp. 22633–22643, 2019.

[42] X. Li, T. Chen, Q. Cheng, S. Ma, and J. Ma, "Smart applications in edge computing: Overview on authentication and data security," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4063–4080, Mar. 2021.

[43] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Trans. Ind. Inform.*, vol. 16, no. 3, pp. 1495–1502, Mar. 2020.

[44] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and efficient message authentication scheme for smart grid," *Secur. Commun. Netw.*, vol. 2019, no. 4, May 2019, Art. no. 4836016.

[45] B. Baruah and S. Dhal, "An authenticated key agreement scheme for secure communication in smart grid," in *Proc. 13th Int. Conf. Commun. Syst. Netw.*, 2021, pp. 447–455.