IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 July 2024, accepted 20 July 2024, date of publication 29 July 2024,
date of current version 30 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3434532

RESEARCH ARTICLE

SGAK: A Robust ECC-Based Authenticated Key Exchange Protocol for Smart Grid Networks

AKBER ALI KHAN[1], VINOD KUMAR[2], RAMAKANT PRASAD[3,4], AND M. JAVED IDRISI[5]
[1]Department of Applied Sciences and Humanities, IIMT College of Engineering, Greater Noida, Uttar Pradesh 201310, India
[2]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi 110032, India
[3]Department of Mathematics, Gargi College, University of Delhi, New Delhi 110049, India
[4]Department of Applied Sciences, National Institute of Technology Delhi, New Delhi, Delhi 110040, India
[5]Department of Mathematics, College of Natural and Computational Science, Mizan-Tepi University, Tepi Campus, Ethiopia

Corresponding author: M. Javed Idrisi (javed@mtu.edu.et)

ABSTRACT A smart grid (SG), also referred to as an electric grid, represents an exceptionally reliable, efficient, and secure system for transmitting both electricity and data. Researchers and the power industry are becoming increasingly interested in SG because of its varied responsibilities. To achieve secure communication in SG environment, there is a need to establish a key exchange between participants. In an SG environment, a number of key exchange techniques have been developed for secure communication. Nevertheless, the most of them do not offer anonymity and function inadequately for SG communication. In this paper, we propose a robus key exchanged and authentication protocol for SG environment using elliptic curve cryptography. The proposed protocol provides anonymity and mutual authentication between participants in SG environment. In addition to an informal security analysis, we offer a formal security analysis of the proposed protocol based on the random oracle model. Further, we provide comparison of the security and functionality features of the proposed protocol with existing ECC-based protocols. A performance analysis in terms of computational and communication costs is carried out in comparison with existing dozen advanced authentication and key exchanged protocols, showing the superiority of the proposed protocol. Our protocol achieves high security with minimum computational and communication costs. The proposed protocol reduced computational cost ≈79.64%, cost of communication is reduced ≈71.54%, while energy consumption reduced to ≈79.65% respectively of the mean value of all alternatives, thus proving the robustness of the presented protocol for securing SG communications.

INDEX TERMS Authentication, elliptic curve cryptography (ECC), random oracle model, smart grid, security and privacy.

I. INTRODUCTION

Smart grid is an electric grid that uses information and communication technology (ICT) to provide information about the actions of participants and power suppliers in a robotic way. ICT is one of the subsidiary steps of SG in which facilitate efficient grid management and process, optimize the resource as well as the features and services of new products. The traditional power grid is usually used to transfer power to a large number of users from the central generator to the substation. The traditional power grid has one-way communication, manual monitoring, few sensors, centralize generation, and restricted control. However, SG has bidirectional communication, distributed generation, and self-monitoring, and so on. [1]. Using ICT, SG is efficient to transfer electricity in an organize way and also manages critical conditions in the grid system. In general, SG can respond to all possible events in the whole grid, such as utilization, distribution, power generation and necessary procedures. For example, when there is an error of a medium voltage transformer in the distribution framework, the SG can usually change the power and reopen the power distribution services. Thus, SG is an electric grid framework that utilizes bidirectional data integration in the cross-generation,

The associate editor coordinating the review of this manuscript and approving it for publication was Fabio Mottola.

transmission, substation, distribution, and computational intelligence domains to ensure secure, efficient, sustainable, and reliable operations. This explanation covers the overall spectrum of energy infrastructure from generation to the endpoint of power utilization [2]. In SG research, many scholars can express various visions for SG due to different focus and perspective. SG has various innovations that perform an essential role at the distribution level. After using these innovations, the structure of SG can be further extended [3], [4]. These include advanced computerized meters, distribution robotization, low-cost communications, distributed vitality tools, broadband communications for dispersion applications, distributed capacity, voltage strength, reactive power control dependent on smart coordination controls, fault investigation and reconfiguration protocol depend on keen exchanging tasks. There are many properties of SG infrastructure such as better consumer loyalty, improved system performance, improved capacity to supply data for rate cases, the permeability of utility activity, cost regulation, start to finish control and impact access to historical information for a vital arrangement. However, for an SG network to function well, its ICT components must be protected from several cyberattacks such as man-in-the-middle attacks, replay attack, impersonation attacks, DoS attack, and so on. In a smart grid communication, the trusted authority is responsible for the registration of users. Once registered, users can communicate through public channels. However, this communication system can be unsafe to security attacks or the compromise of sensitive data, leading to unpredictable consequences.

The user privacy and security can be achieved with the help of having an appropriate authentication mechanism in the network. The security plans for user authentication play an important role to protect a network or system against attacks such as impersonation. If a secure user authentication mechanism is not used then a network is completely open to various security attacks such as unauthorized access to SG communication, impersonation, denial of service and man-in-the-middle attacks etc,. The absence of an appropriate authentication mechanism may also result in loss or illegal modification of SG Communication which might be a serious concern. This illegal modification of SG Communication could potentially cause substantial harm to the SG network. That's why authentication and key agreement protocol are needed to ensure the security and privacy of smart grid communication. Authentication protocols are particularly effective in addressing security issues during the interaction between communication participants. Security issues in smart grid communication are as follows.

- **Issues against devices:** Any Internet of Things (IoT) device that is capable of connecting to communication networks and exchanging data with other smart grid devices is vulnerable to cyberattacks. The most often targeted device by an attacker is the smart meter that are connected to the smart grid.
- **Issues against communications:** Attacker could modify or intercept communications within the smart grid network. For example, an attacker can modify SG communications to reduce a power bill.
- **Issues against the system:** Attacks on the SG Network, including network operators, power plants, and utility firms. Adversary often find that attacks on the SG Network are the most lucrative and destructive.
- **Privacy risks:** Smart devices in SG Communication collect detailed consumption data, which, if detected or accessed without authorization, can reveal sensitive information about individuals and their behavior.
- **Security management risks:** The utility provider monitor and control a large number of devices in a SG communication. It's critical that customers have faith in the utility company with their information data. Hence, utility provider must monitor individual devices for possible cyber attacks.

A. SECURITY REQUIREMENTS

Security and privacy are very critical issues in smart grid communication system due to the interconnected nature of the smart grid communication. The following are some essential security objectives for the smart grid communication system must be accomplish:

1) **Privacy:** Smart devices in SG Communication collect detailed consumption data, which, if detected or accessed without authorization, can reveal sensitive information about individuals and their behavior. Therefore for ensuring the privacy of all communicated information in the smart grid communication system is essential. So, it is necessary to establish a protocol to identify and stop illegal data tampering or alterations.
2) **Authentication:** Unauthorized manipulation or control of smart grid operations may result from unauthorized access to devices or systems. So, it is required mutual authentication protocol to stop unauthorized access.
3) **Access Control:** Role-based access control mechanisms should restrict user privileges, ensuring that users can only access data and functions relevant to their roles and responsibilities.
4) **Encryption:** All communication between participant must be encrypted to protect against eavesdropping and data tampering.
5) **Data Integrity:** Data integrity checks, such as message authentication codes, should be used to verify the integrity of data during transmission.
6) **Confidentiality:** Only the designated recipients are allowed to view the encoded communications. Information about attacks and malevolent stalkers should not be accessible.
7) **Redundancy and Fault Tolerance:** To ensure system availability, redundancy and fault tolerance mechanisms should be in place to handle hardware or communication failures gracefully.

By meeting these security requirements, the proposed SG system can provide a robust and reliable platform for applications in SG communication. It is important to recognize that the SG system effectiveness and applicability may vary depending on specific use cases and operational environments. Continuous research and development efforts are required to address limitations and expand the system scope in response to evolving needs and challenges.

B. RELATED WORK

Many authentication and key agreement schemes for SG communication have recently been published. Fouda et al. [5] suggested a computational Diffie-Hellman based protocol for different SM and equipment that are related to SG communication. Due to exponential operations, the computation and communication costs of this protocol are much higher. After that, Mahmood et al. [6] shows that [5] does not maintain insider attack and perfect forward secrecy (PFS) and has high communication and computation costs. Mood and Nikooghadam [7] also mention [5] does not maintain CK model [8] and has public key infrastructure issue. Chim et al. [9] designed a scheme to maintain the privacy of users. Mahmood et al. [6] mention in his paper Chim et al. [9] can not provide key agreement, mutual authentication, and perfect forward secrecy. Also Mahmood et al. shows that [9] does not stand with to impersonation attack and insider attack. Nicanfar and Leung [10] suggested a key agreement protocol for SG network. The advantage of their protocol is maintain both forward and backward confidentiality. Wu and Zhou [11] presented a key distribution scheme for SG environment. Unluckily, Xia and Wang [12] point out that the protocol [11] is not standing with the man in the middle attack and they recommended a new key based protocol for the SG environment. After that, Park et al. [13] show that Xia and Wang [12] scheme not secure against impersonation attack and does not maintain unknown key share attack. Tsai and Lo [14] presented a key distribution protocol for SG environment and shows that Wu and Zhou protocol [11] vulnerable to anonymity, replay attack, PFS and impersonation attack also shows that Xia and Wang [12] scheme vulnerable to impersonation attack on SM side, PFS, replay attack and man in the middle attack. Odelu et al. [15] presented an authentication designed for SG system and shows that Tsai and Lo [14] protocol does not provide SM credentials or privacy, also insure against secret leakage and security attacks. Sule et al. [16] designed an authentication and key exchange scheme that computation and communication cost are quite similar to Fouda et al. [5].

Mahmood et al. [17] presented an authentication scheme based on RSA that is more computationally efficient than Fouda et al. [5] and Sule et al. [16]. Li et al. [18] have submitted an authentication and key exchanged framework for SG communication system, which depending on public key infrastructure and there are more computational and communication costs required. Further, Mahmood et al. [6] designed another framework for SG environment by using ECC and hash functions. Unfortunately, Kumar et al. [19] review this protocol and found their protocol have some security issues such as insider attack, impersonation attack, etc. Mood and Nikooghadam [20] designed an authentication and a key distribution scheme by using ECC. However, Breaken et al. [21] proved that Mood and Nikooghadam [20] does not offer session key security under the CK model [8] and insecure against DoS attack. Wazid et al [22] suggested three-factor user authentication protocol for SG communication powered by renewable energy. Gope and Sikdar [23] proposed an authenticated key agreement mechanism for SG communication by utilizing a physically unclonable function (PUF). The authors claimed that their approach secure against denial-of-service attacks and provide strong security against man-in-the-middle attacks. Nevertheless, the fuzzy extractor that the PUF uses has drawbacks, as noted in [24]. Khan et al. [25] proposed mutual authentication scheme for smart grid communications by using fuzzy techniques and ECC. Further, [26], [27], [28], [29], [30], and [31] proposed authentication and key exchange protocol for SG communication enabled with Iot devices, smart metering communication system and other environment. Consequently, most of the above mentioned protocols are either vulnerable for security attacks or require higher communication and computation costs. Although, most of above given protocols are insecure in SG communication and computationally high cryptographic protocols which is unsuitable for SG environment.

C. SYSTEM MODEL

Smart gird consists of important domains that is the power plant, the power transmission, the power distribution, the power operation center, service providers and power customer domain that contains home area network (HAN), building area network (BAN), industrial area network (IAN), etc. with a smart meter (SM) as shown in Figure 1. The power operation and service provider manages power flow, the participants and all third-party operations respectively [32] and [33].

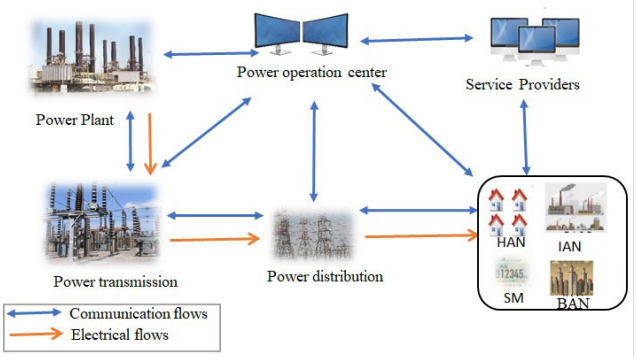

FIGURE 1. Smart grid network.

D. SECURITY THREAD MODEL

In this section, we define the adversary model that our proposed system or protocol is designed to defend against. Understanding the capabilities and objectives of potential adversaries is crucial for designing effective security mechanisms. In this proposed research adversary model is based on the widely recognized threat landscape outlined by CK model [8]. we consider adversaries with a range of capabilities and resources, including:

- **Passive Eavesdroppers:** These adversaries can intercept and monitor communication between legitimate entities but do not have the ability to modify or inject data into the communication channel.
- **Active Attackers:** These adversaries have the capability to actively manipulate the communication channel. They can alter, inject, or replay messages to disrupt communication or compromise the integrity and confidentiality of data.
- **Insider Threats:** We also consider the possibility of insider threats, where individuals with legitimate access to the system may abuse their privileges to undermine security, leak sensitive information, or engage in other malicious activities.
- **Resourceful Adversaries:** In some scenarios, adversaries may have substantial computational resources, enabling them to mount sophisticated attacks such as cryptographic attacks, brute-force attacks, or advanced malware.

E. MOTIVATION AND CONTRIBUTION

There are several authentication and key agreement scheme that are used to secure network communications; each has advantages and disadvantages. These schemes include identity-based, public key-based, and lightweight protocols. Key pairs are necessary for public key-based mutual authentication protocol, however key revocation is challenging Identity-based authentication is susceptible to vulnerability if identity details are stolen because it relies on recognized information for identification. Although lightweight protocols are designed to minimize computation and communication costs for systems with limited resources, their simplicity may make them more vulnerable to some types of attacks. To ensure secure communication, we consider elliptic curve cryptography as a viable solution to the problems with SG networks previously described. Most of the presented authentication protocols for SG communication fail to accomplish their objectives of security and privacy as discussed above. These vulnerabilities motivated us to study the current authentication framework and to design a novel mutual authentication and key agreement protocol for SG environment, which can fulfill all possible security feature with much less computation and communication overhead.

The main contribution of the proposed protocol are as follows:

- This paper presents a lightweight anonymous authenticated ECC-based key exchanged scheme for SG communication.
- The proposed protocol is secure from various type of active and passive attacks and maintain various cryptographic properties.
- We have provided a formal security analysis of SGAK using the random oracle model as well as informal security analysis for the proposed protocol to ensure its reliability and security.
- In this study, we prioritized security in order to facilitate effective communication and reduce computing overhead by exchanging fewer messages throughout the authentication and key agreement phases of the scheme design.
- Apart from its benefits in terms of security and performance, the proposed protocol reduce the amount of energy consumption in comparison to other existing protocols used by the users intelligent devices, which satisfies deployment criteria in real-world scenarios.

F. ROAD MAP OF THE PAPER

This is the format for the remaining portion of this research: Throughout the investigation, we have followed certain mathematical guidelines and notations, which are given in Section II. Section III, proposed scheme. Section IV, security analysis of SGAK. Section V, performance analysis. Finally, conclusion of SGAK.

II. PRELIMINARIES

In this section, we briefly describe some mathematical definitions and notations.

A. NOTATIONS

Table 1, provides the following helpful notations along with their explanation.

TABLE 1. Notations used.

Notation	Explanation
ECC	Elliptic curve cryptography
$\mathcal{A}$	Adversary
ID_i	The unique identity of entity i
Z_q^*	Finite field of integer of order $q-1$
$h(.)$	Secure one way hash function
U_i	The i^{th} entity
q	Sufficiently large prime's
SK_i	The session key of entities i
$D_K(.)$	Symmetric decryption using the key K
$\|\|$	Concatenation operation
$E_K(.)$	Symmetric encryption using the key K
ΔT	Maximum transmission delay
G	Elliptic curve group under addition
g	Generator of G
M	Master key
$\stackrel{?}{=}$	Whether equal or not
$\oplus$	The bitwise XoR operation
TA	Thrust authority
ϵ	Sufficiently small
$\cong$ or $\approx$	Approximate number

B. ELLIPTIC CURVE OVER A FINITE PRIME FIELD

The public key encryption scheme known as Elliptic Curve Cryptography makes use of the elliptic curve principle. ECC provides improved performance at a similar security level and requires a smaller key size as compared to traditional cryptographic methods like RSA. The core idea behind ECC is that it used to generate public and private keys, perform data encryption and decryption, digital signatures, and other cryptographic operations by using the addition and multiplication operations on elliptic curve points. The discrete logarithm problem connected to elliptic curves, which requires finding a point P on the elliptic curve, is the foundation of its security. The following formula provides the elliptic curve over prime finite field $E : v^2 = u^3 + ru + s$ mod q,where $r, s \in Z_q^*$ with $4r^3 + 27s^2$ mod $q \neq 0$ is called non-singular elliptic curve and Group of elliptic curves described as $G = \{(u, v) : u, v \in Z_q^*, (u, v) \in E\} \cup \{\Theta\}$, where group G identity under addition is known as the point Θ. The definition of the scalar multiplication over group G is define as $aP = P + P + P \ldots\ldots\ldots\ldots\ldots\ldots + P\ (a - times)$ where $a \in Z_q^*$. Additional details about ECC and its use in [34].

C. ONE-WAY HASH FUNCTION

Collision-resistant one-way secure hash function which is defined from a arbitrary length of string to a fixed length of string as $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$ where the output of hash function is $h(x) \in \{0, 1\}^n$ finite length of sting and input $x \in \{0, 1\}^*$ is of arbitrary length of string [35], [36].

The properties of the secure hash function are as follows [37].

- $h(x)$ is applicable to all data sections.
- Every output message has a definite $h(x)$.
- The hash function is called weak-collision if for any input x, getting other input $x_2 \neq x_1$ such that $h(x_1) = h(x_2)$ is computationally hard.
- Strong-collision resistance is the name given to the hash function if $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$ is difficult to compute.
- The advantage of an attacker $\mathcal{A}$ is stated as:

$Adv_{\mathcal{A}}^{HASH}(t) = Pr[(x_1, x_2) \Leftarrow_R \mathcal{A} : x_1 \neq x_2 \ and \ h(x_1) = h(x_2)]$, and $(x_1, x_2) \Leftarrow_R \mathcal{A}$ denotes the set of (x_1, x_2) is generated by $\mathcal{A}$. It is said that $h(.)$ is collision-resistant if $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon$, for any $\epsilon > 0$.

D. ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM(ECDLP)

For given tuple $< V, cV >$, where $c \in Z_q^*$, $V \in G$, Using any polynomial constrained approach to calculate c is computationally difficult. The probability of $\mathcal{A}$ that can solve ECDLP is $Adv_{ECDLP}(\mathcal{A}) = Pr[\mathcal{A}(V, cV) = c : c \in Z_q^*, V \in G]$.

The time-bounded probabilistic polynomial for any $\mathcal{A}$, $Adv_{ECDLP}(\mathcal{A})$is insignificant, in other words $Adv_{ECDLP}(\mathcal{A}) < \epsilon$ [20].

E. ELLIPTIC CURVE DIFFIE-HELLMAN PROBLEM(ECDHP)

Given $cV, dV \in G$ for all $c, d \in Z_q^*$. cdV is difficult to compute. $\mathcal{A}$ has the following probability of solving ECDHP as $Adv_{ECDHP}(\mathcal{A}) = Pr[\mathcal{A}(cV, dV) = cdV : c, d \in Z_q^*, V \in G]$.

The time-bounded polynomial with probabilistic properties for any adversary $\mathcal{A}$, $Adv_{ECDHP}(\mathcal{A})$ is insignificant that is $Adv_{ECDHP}(\mathcal{A}) < \epsilon$ for a sufficiently small ϵ [20].

F. ELLIPTIC CURVE GAP DIFFIE-HELLMAN PROBLEM (ECGDHP)

Let $\lambda X, \mu X \in G$. The probability for $\mathcal{A}$ to computes $\lambda\mu X$ with an ECGDHP oracle in polynomial time ζ is $Advt_{\mathcal{A}}^{ECGDHP}(\zeta) \leq \epsilon$ [39].

G. ELLIPTIC CURVE DECISIONAL DIFFIE-HELLMAN PROBLEM (ECDDHP)

Let $\lambda X, \mu X, \nu X \in G$. $\mathcal{A}$ probability of choosing whether $\nu X = \lambda\mu X$ polynomial time ζ is $Advt_{\mathcal{A}}^{ECDDHP}(\zeta)$ and ϵ is a negligibly tiny positive real number, where $Advt_{\mathcal{A}}^{ECDDHP}(\zeta) \leq \epsilon$ [39].

III. THE PROPOSED PROTOCOL

We proposed a robust authentication protocol for SG communication. The proposed protocol consists of four phases, including initialization phase, registration phase, login and authentication phase, as well as key update phase. For the general point of view, the authentication environment of SGAK is given in Figure 2.

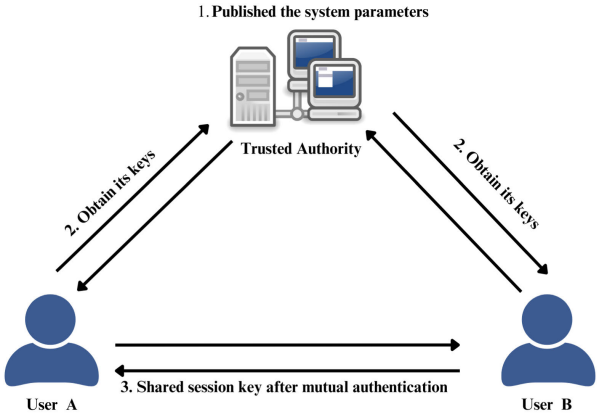

FIGURE 2. Typical authentication environment of SGAK.

A. INITIALIZATION

In this stage, the non-singular elliptic curve is selected by TA as $E_q(r, s)$ and g as the base point. Further, TA selects $h(.)$ and generates its private key x_i. Finally, TA publishes the system parameter $\{E_q(r, s), g, q, h(.)\}$.

B. REGISTRATION

In this phase, U_i registered itself with TA and performed the following steps.

Step 1. During the registration procedure, U_i selects ID_i and T_{R1}, and then sends to TA over a secure channel.

Step 2. On receiving $\{ID_i, T_{R1}\}$, TA verify $T_{R2} - T_{R1} \leq \bigtriangleup T$ if verification is successful then TA generates $x_i \in Z_q^*$ and computes $X_i = x_i.g$, $d_i = h(ID_i \| X_i)$ and $Y_i = x_i + M.d_i$. After that TA sends $\{Y_i, X_i\}$ towards user U_i through a secure medium.

Step 3. On receiving $\{Y_i, X_i\}$, U_i verify $Y_i.g \stackrel{?}{=} X_i + (h(ID_i \| X_i)).PK$ if verified then, U_i sets his/her public key as $PK_i = Y_i.g$.

C. LOGIN AND AUTHENTICATION

Once authentication is completed between U_A and U_B they establish a common session key for the subsequent encrypted communication process. The login and authentication process of the proposed protocol contains the following steps, which displayed in Table 2.

Step 1. In the authentication phase U_A selects his/her ID'_A, calculate $d'_A = h(ID'_A \| X_A)$ and then verify $d'_A \stackrel{?}{=} d_A$ if this hold then U_A produces a random once as $a \in Z_q^*$, computes $M_A = a.g$, $ID_{A1} = ID_A \oplus h(M_A \| PK \| T_1)$ and encrypt $E_1 = E_{K_1}(ID_{A1}, M_A)$ with the help of key $K_1 = h(PK_B \| X_A \| T_1)$. After that U_A sends $\{E_1, T_1\}$ towards U_B through a public channel.

Step 2. Once obtaining $\{E_1, T_1\}$, U_B checks the time stamp condition as $T_2 - T_1 \leq \Delta T$ if this condition hold then U_B decrypt $(ID_{A1}, M_A) = D_{K_1^*}(E_1)$ with the help of key $K_1^* = h(PK_B \| X_A \| T_1)$ and computes $ID_A^* = ID_{A1} \oplus h(M_A \| PK \| T_1)$. After that U_B generates a random value $b \in Z_q^*$ and computes $M_B = b.g$, $N = h(M_A \| M_B \| ID_A^* \| ID_B \| T_1)$, computes session key as $SK_B = h(ID_A^* \| ID_B \| N \| M_A \| M_B \| b.a.g \| T_3)$, $ID_{B1} = ID_B \oplus h(M_A \| M_B \| T_3)$ and encrypt $E_2 = E_{K_2}(ID_{B1}, N, M_B)$ with the help of $K_2 = h(M_A \| T_3 \| ID_A^*)$. Further, U_A sends $\{E_2, T_3\}$ towards U_A through a public channel.

Step 3. On receiving $\{E_2, T_3\}$, U_A checks the time-stamp condition $T_4 - T_3 \leq \Delta T$ if this condition hold then U_A computes $K_2^* = h(M_A \| T_3 \| ID_A)$ and decrypt $(ID_{B1}, N, M_B) = D_{k_2^*}(E_2)$. Further U_A computes the followings: $ID_B^* = ID_{B1} \oplus h(M_A \| M_B \| T_3)$, $N^* = h(M_A \| M_B \| ID_A \| ID_B^* \| T_1)$ and verifies $N^* \stackrel{?}{=} N$ if verification is successful subsequently select its session key as $SK_A = h(ID_B \| ID_B^* \| N^* \| M_A \| M_B \| a.b.g \| T_3)$. Hence, $SK = SK_A = SK_B$

D. KEY UPDATION

This crucial security feature deals with a number of eventualities, such as lost or compromised keys, policy adherence, rotation techniques, dynamic access control changes, and key expiration.

Step 1. The users initiates the process by selecting a new private key, $a^{new} \in Z_q^*$, and computes pupblic key $M_A^{new} = a^{new}.g$, $ID_{A1}^{new} = ID_A \oplus (M_A^{new} \| PK^{new} \| T_1^{new})$ and encrypt $E_1 = E_{K_1^{new}}(ID_{A1}^{new}, M_A^{new})$ with the help of key $K_1^{new} = h(PK_B \| X_A \| T_1^{new})$. After that U_A sends $\{E_1^{new}, T_1^{new}\}$ towards U_B through a public channel.

Step 2. Once obtaining $\{E_1^{new}, T_1^{new}\}$, U_B checks the time stamp condition as $T_2^{new} - T_1^{new} \leq \Delta T$ if this condition hold then U_B decrypts $(ID_{A1}^{new}, M_A^{new}) = D_{K_1^*}(E_1^{new})$ with the help of key $K_1^{*new} = h(PK_B^{new} \| X_A^{new} \| T_1^{new})$ and computes $ID_A^{*new} = ID_{A1}^{new} \oplus h(M_A^{new} \| PK^{new} \| T_1^{new})$. After that U_B generates a random value $b^{new} \in Z_q^*$ and computes $M_B^{new} = b^{new}.g$, $N^{new} = h(M_A^{new} \| M_B^{new} \| ID_A^{*new} \| ID_B^{new} \| T_1^{new})$, computes session key as $SK_B^{new} = h(ID_A^{*new} \| ID_B^{new} \| N^{new} \| M_A^{new} \| M_B \| b^{new}.a^{new}.g \| T_3^{new})$, $ID_{B1}^{new} = ID_B \oplus h(M_A^{new} \| M_B^{new} \| T_3^{new})$ and encrypt $E_2^{new} = E_{K_2^{new}}(ID_{B1}^{new}, N^{new}, M_B^{new})$ with the help of $K_2^{new} = h(T_3^{new} \| ID_A^{*new})$. Further, U_A sends $\{E_2^{new}, T_3^{new}\}$ towards U_A through a public channel.

Step 3. On receiving $\{E_2^{new}, T_3^{new}\}$, U_A checks the time-stamp condition $T_4^{new} - T_3^{new} \leq \Delta T$ if this condition hold then U_A decrypt $(ID_{B1}^{new}, N^{new}, M_B^{new}) = D_{K_2^*}(E_2^{new})$, where $K_2^{*new} = h(T_3^{new} \| ID_A^{*new})$. Further U_A computes the followings: $ID_B^{*new} = ID_{B1}^{new} \oplus h(M_A^{new} \| M_B^{new} \| T_3^{new})$, $N^{*new} = h(M_A^{new} \| M_B^{new} \| ID_A^{new} \| ID_B^{*new} \| T_1^{new})$ and verifies $N^{*new} \stackrel{?}{=} N^{new}$ if verification is successful subsequently select its session key as $SK_A^{new} = h(ID_B^{new} \| ID_B^{*new} \| N^{*new} \| M_A^{new} \| M_B^{new} \| a^{new}.b^{new}.g \| T_3^{new})$.

IV. SECURITY ANALYSIS

In this section, we examine the accuracy of the proposed protocol using two main techniques: a theoretical security proof inside the Random Oracle Model and an informal security justification. These comprehensive method provides in depth evaluation of the accuracy and security of the proposed protocol.

A. FORMAL SECURITY ANALYSIS

According to the security model as discussed above, this subsection presents the security proof of SGAK under random oracle model. The proposed protocol contains three participants, namely, U_A, U_B and TA. During the registration phase only, TA have a limited time role. Therefore, communication between U_A and U_B usually. Each oracle in this model returns a value, either accept or reject or $\perp$, according to how the attacker interacted with the following queries:

- $h(messages)$**:** Suppose $\mathcal{A}$ yields a random value in response to this oracle request $hv \in \{0, 1\}^L$ as the hash value of the message.
- $Execute(U_A, U_B)$**:** This query mimics passive attacks, where the attacker can view the messages that the participant modifies in real time throughout the protocol.

TABLE 2. Login and authentication phase.

U_A	U_B
Inputs ID'_A Computes $d'_A = h(ID'_A \| X_A)$ Verifies $d'_A \stackrel{?}{=} d_A$ hold then Generates $a \in Z_q^*$ Computes $M_A = a.g$ Computes $ID_{A1} = ID_A \oplus h(M_A \| PK \| T_1)$ Computes $K_1 = h(PK_B \| X_A \| T_1)$ Encrypted $E_1 = E_{K_1}(ID_{A1}, M_A)$ Sends $M_1 = \{E_1, T_1\}$ $\cdots\cdots\cdots\cdots\cdots\cdots \longrightarrow$ (via public channel)	Verifies $T_2 - T_1 \leq \Delta T$ Computes $K_1^* = h(PK_B \| X_A \| T_1)$ Decrypted $(ID_{A1}, M_A) = D_{K_1^*}(E_1)$ Computes $ID_A^* = ID_{A1} \oplus h(M_A \| PK \| T_1)$ Generates $b \in Z_q^*$ Computes $M_B = b.g$ Computes $N = h(M_A \| M_B \| ID_A^* \| ID_B \| T_1)$ Computes $SK_B = h(ID_A^* \| ID_B \| N \| M_A \| M_B \| b.a.g \| T_3)$ Computes $ID_{B1} = ID_B \oplus h(M_A \| M_B \| T_3)$ Computes $K_2 = h(M_A \| T_3 \| ID_A^*)$ Encrypted $E_2 = E_{K_2}(ID_{B1}, N, M_B)$ Sends $M_2 = \{E_2, T_3\}$ $\longleftarrow \cdots\cdots\cdots\cdots\cdots\cdots$ (via public channel)
Checks $T_4 - T_3 \leq \Delta T$ Computes $K_2^* = h(M_A \| T_3 \| ID_A)$ Decrypted $(ID_{B1}, N, M_B) = D_{k_2^*}(E_2)$ Computes $ID_B^* = ID_{B1} \oplus h(M_A \| M_B \| T_3)$ Computes $N^* = h(M_A \| M_B \| ID_A \| ID_B^* \| T_1)$ Verify $N^* \stackrel{?}{=} N$ Computes $SK_A = h(ID_B \| ID_B^* \| N^* \| M_A \| M_B \| a.b.g \| T_3)$ Hence $SK = SK_A = SK_B$	

- *Send*$(\zeta, messages)$**:** This kind of inquiry is used to replicate active attacks, whereby $\mathcal{A}$ transmit messages to ζ, and obtain response according to the protocol description.
- *EsReveal*(ζ)**:** Provides details on a transient secret maintained by an oracle ζ to $\mathcal{A}$.
- *SKReveal* (ζ)**:** With this inquiry, $\mathcal{A}$ to inform about the session key sorted by ζ.
- *Corrupt*(ζ)**:** $\mathcal{A}$ can obtain the long-term secret characteristics of the oracle ζ by submitting this inquiry.
- *Expire*(ζ)**:** With this query, the Oracle ζ-organized session's session key is eliminated.
- *TestID*(ζ)**:** This query is attempting to verify the SGAK anonymity feature. Upon obtaining the *TestID*(ζ) query, first, a fair coin, c, is flipped; if c = 1, the true identity is given back; if not, a random number is given back.
- *TestSK*(ζ)**:** Assume that the goal of this query is to determine the session key semantic security. Upon obtaining a *TestSK*(ζ) query, first, a fair coin, c, is flipped. If c = 1, the true SK is given back; if not, a randomly generated value of an equivalent length is selected and given back to $\mathcal{A}$.

We define the following security definitions as follows in order to ascertain the semantic security of the SGAK.

- Once both Oracle U_A and U_B have established a similar session key and successfully authenticated each other, they are considered partners.
- If a session and its coordinating session don't reveal anything, then the session is new.
- The advantage of the attackers in breaking the semantic security of the SGAK is stated as Pr(succ.), which indicates the probability of the opponent succeeding in his aim as $Adv_{SGAK}(\mathcal{A}) = |2Pr(succ) - 1|$.
- SGAK remains secure from the adverse model [8] if $Adv_{SGAK}(\mathcal{A}) \leq \varepsilon$ retains.
- In the random oracle framework, SGAK is secure [40], [41], [42] for Theorem 2 and Theorem 3, The oracle is described by us as:
  Reveal: The output string $y = h(x)$ in Oracle provides the unconditional output string over the input string x.

Lemma (Difference Lemma): Assume that S represents the error event between S_1 and S_2, the events of the probability density function, in the following way $S_1 \wedge \neg S \iff S_2 \wedge \neg S$, then $|Pr[S_1] - Pr[S_2]| \leq Pr[S]$.

Theorem 1: If $\mathcal{A}$ is an adversary with polynomial time capabilities against the proposed protocol semantic security, then Q_e execute queries, Q_s send queries, and Q_H hash queries are almost identical $|\mathcal{D}|$ represent the set uniformly distributed cardinality and $Adv_{E_K}^{SE}(\mathcal{A})$ is the advantage of $\mathcal{A}$ against decryption or encryption Enc_K. The advantage of $\mathcal{A}$ in SGAK is provided by

$$Adv_{SGAK}(\mathcal{A}) \leq \frac{(Q_H^2 + Q_S)}{2^{L+1}} + \frac{(Q_S + Q_E)^2}{q} + \frac{2Q_S}{|\mathcal{D}|} + 2Adv_{E_K}^{SE}(\mathcal{A}) + 2Q_H \; max\{Adv_{ECDLP}(\mathcal{A}), Adv_{ECDHP}(\mathcal{A})\}$$

Proof: We introduced the game of sequences to demonstrate the semantic security of SGAK The actual attack begins

with GM_0 and ends with GM_6 is the game where $\mathcal{A}$ has no advantage.

Game GM_0**:** In the ROR model, the attacker $\mathcal{A}$ initiates the first real attack on the suggested scheme in this game. The simulation of *Game* GM_0 is equivalent to the real attack in the random oracle model, we have

$$Adv_{SGAK}(\mathcal{A}) = |2Pr[Succ_0] - 1|. \quad (1)$$

Game GM_1**:** An opponent cannot distinguish between two games since the oracles for the distinct requests are simulated and the subsequent requests result are saved in the lists. Hence, we have

$$Pr[Succ_1] = Pr[Succ_0] \quad (2)$$

Game GM_2**:** The game GM_2 simulates a previous game, with the exception that if a collision arises in the transcripts or hash queries, GM_2 terminates. The birth day paradox indicates that there is a maximum chance of a hash collision $\frac{Q_H^2}{2^{L+1}}$ and probability of collision in the transcript is at most $\frac{(Q_S+Q_E)^2}{2q}$ [43], [44], where L is the hash function length. Therefore, based on difference lemma, we have

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{Q_H^2}{2^{L+1}} + \frac{(Q_S + Q_E)^2}{2q} \quad (3)$$

Game GM_3**:** The G_3 simulation is comparable to GM_2 with the exception that GM_3 shall end if $\mathcal{A}$ accurately predicts the conditions of the verifier without consulting the oracle. Unless the server instance fails with a valid authentication value, GM_3 and the previous game are identical. Therefore,

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{Q_S}{2^L} \quad (4)$$

Game GM_4**:** The proposed protocol session key security is examined in GM_4. The security goal of SGAK is to ensure that $\mathcal{A}$ is unable to achieve the mutual authenticated session key. The purpose of the attacker $\mathcal{A}$ is to compute the session key (SK) for the related Scenario.

Scenario a: (Perfect forward secrecy assumption): $Corrupt(U_A)$ and $Corrupt(U_B)$. In this event assume to be an adversary $\mathcal{A}$ to obtain the secret keys of U_A and U_B i,e. (a, b) and SK, but not theirs temporal secrets.

Scenario b: (Known session specific temporary information attack assumption): $ESReveal(U_A)$ and $ES - Reveal(U_B)$. In this instance, we assume that an adversary $\mathcal{A}$ to obtain the ephemeral secret of U_A and U_B, but not their confidential information.

In the circumstances mentioned above, $\mathcal{A}$ not possible to solve the SK without obtaining the secure hash function value or calculating the ECDLP or ECDHP. Therefore, as long as the ECDHP or ECDLP holds, there is little difference between this game and the previous one. From this, it can be concluded that:

$$|Pr[Succ_4] - Pr[Succ_3]| \leq Q_H \; max\{Adv_{ECDLP}(\mathcal{A}), Adv_{ECDHP}(\mathcal{A})\} \quad (5)$$

Game GM_5**:** The only difference between this game and the previous one is that GM_5 test query ends if $\mathcal{A}$ publishes a *TestID* inquiry to obtain the true identity or sends a query to obtain the password. Thus, we draw the conclusion that

$$|Pr[Succ_5] - Pr[Succ_4]| \leq \frac{Q_S}{|D|} + Adv_{E_K}^{SE}(\mathcal{A}) \quad (6)$$

Game GM_6**:** The simulation of GM_6 is similar GM_5 apart from that *TestSK* query of GM_6 will be coming to an end if $\mathcal{A}$ publish a hash query with $h(ID_A \| ID_B^* \| L_2^* \| MAC_A \| W_A \| W_B \| a.b.P \| T_3)$. Due to, $\mathcal{A}$ utilizing the hash query, to obtain the SK with chance of probability $Q_H^2/2^{L+1}$. Thus, we have

$$|Pr[Succ_6] - Pr[Succ_5]| \leq \frac{Q_H^2}{2^{L+1}} \quad (7)$$

Therefore, without doing a collision resistance hash query with the correct input, $\mathcal{A}$ has no advantage in differentiating the real session key from a random one. $Pr[Succ_6] = 1/2$. We conclude that the theorem is true by summing together all of these probability.

Theorem 2: Assuming that the one-way hash function $h(.)$ closely functions with an oracle, then SGAK is provably safe from an adversary attempting to obtain the ID_i of users U_i.

Proof: The proof of the above theorem 2. We have to generate an attacker $\mathcal{A}$ with the ability to obtain a valid user U_i identities as ID_i. In the proposed security thread model $\mathcal{A}$ able to retrieve all of the sensitive information as ID_i from a legitimate user U_i with the use of an attack known as power analysis [45], [46]. $\mathcal{A}$ executes the algorithm 1 using the Reveal oracle. let $EXP1_{\mathcal{A},SGAK}^{HASH}$ for SGAK. The success probability of $EXP1_{\mathcal{A},SGAK}^{HASH}$ is given as $Succ1 = |Pr[EXP1_{\mathcal{A},SGAK}^{HASH} = 1] - 1|$, as well as this experiment advantage function $Adv1(rt_1, q_R) = max_{\mathcal{A}}\{Succ1\}$, where the maximum is taken over all $\mathcal{A}$ with the number of inquiries I_R made to the Reveal oracle, and the execution time rt_1. $SGAK$ is provably safe from an adversary $\mathcal{A}$ that aims to obtain ID_i, provided $Adv1(rt_1, I_R) \leq \epsilon_1$, for any $\epsilon_1 > 0$. Considering this theory, Only $\mathcal{A}$ can obtain ID_i and win the game if they are able to revert $h(.)$. However, reversing $h(.)$ is a computationally challenging problem. i.e, $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon$, for any $\epsilon > 0$. Hence, we have $Adv1(rt_1, q_R) \leq \epsilon_1$, since $Adv1(rt_1, q_R)$ depends on $Adv_{\mathcal{A}}^{HASH}(t)$. This demonstrates that $SGAK$ is provably safe from an attacker's attempt to ID_i of U_i.

Algorithm 1 $EXP1^{HASH}_{\mathcal{A},SGAK}$

1: Eavesdrop the login request $< ID'_A >$ during the login phase, where $d'_A = h(ID'_A \| X_A)$
2: Call Reveal oracle on input $< ID'_A >$ to retrieve ID_A.
3: **if** $((ID^*_A = ID'_A)$ and $(d'_A = d_A))$ **then**
4: Accept correct request for U_A
5: return (Success)
6: **else**
7: return (Failure)
8: **end if**

Theorem 3: Under the assumption that the one-way secure hash function $h(.)$ closely resembles an oracle, SGAK is provably secure against an attacker in terms of obtaining the session key SK_{ij} among U_i and U_j, the private key of the users, and the ID_i of an authenticated user U_i.

Proof: In order to prove the aforementioned theorem 2, we assume that any $\mathcal{A}$ will be able to access the session key SK_{ij} between U_i and U_j, the private key N of the user, and the ID_i of the authorized users U_i. To execute the fictitious algorithm, $\mathcal{A}$ makes use of the Reveal oracle, let $EXP2^{HASH}_{\mathcal{A},SGAK}$.The success probability for $EXP2^{HASH}_{\mathcal{A},SGAK}$ as $Succ2 = |Pr[EXP2^{HASH}_{\mathcal{A},SGAK} = 1] - 1|$. For the current observation, the advantage function occurs as $Adv2(rt_2, I_R) = max_{\mathcal{A}}(Succ2)$, where the amount of queries I_R submitted to the Reveal oracle and the maximum over all $\mathcal{A}$ with execution time rt_2 are taken into account. The proposed protocol is known as provably secure from an adversary $\mathcal{A}$ for obtaining ID_i, N and SK_{ij}, if $Adv2(rt_2, I_R) \leq \epsilon_2$, for any $\epsilon_2 > 0$. Considering this finding, if $\mathcal{A}$ is able to reverse $h(.)$, then only that person will be able to obtain ID_i with ease, N and SK_{ij} as well as win the game. However, reversing $h(.)$ is computationally challenging. i.e, $Adv^{HASH}_{\mathcal{A}}(t) \leq \epsilon$, for any $\epsilon > 0$. Therefore, we have $Adv2(rt_2, I_R) \leq \epsilon_2$, since $Adv2(rt_2, I_R)$ depends on $Adv^{HASH}_{\mathcal{A}}(t)$. This demonstrates that in order to obtain ID_i, N, and SK_{ij}, the proposed protocol is provably secure from an attacker.

B. INFORMAL SECURITY ANALYSIS

This section explains how SGAK can preserve security characteristics and defend against a variety of security attacks. The following is a thorough overview of informal security analysis:

1) MAN-IN-THE-MIDDLE ATTACK

In the proposed SGAK, we used secure hash check conditions and time stamp conditions as $T_i - T_j \leq \bigtriangleup T$ in every step of every phase. In the event that an attacker $\mathcal{A}$ attempts to log in and key exchange phase after break the time-stamp condition then, check the hash conditions $d^*_A \stackrel{?}{=} d_A$ and $N^*_i \stackrel{?}{=} N_i$ which not possible for any $\mathcal{A}$ as hash function is secure, $\mathcal{A}$ can not success in any phase. Hence, SGAK secure against this attack.

Algorithm 2 $EXP2^{HASH}_{\mathcal{A},SGAK}$

1: Eavesdrop the request for login $< ID'_A >$ during the system login phase
2: Call the Oracle to reveal input $< d_A >$ to retrieve ID_A, X_A as $ID'_A, X_A) \leftarrow Reveal(d^*_A)$
3: Computes $d'_A = h(ID'_A \| X_A)$.
4: **if** $(d'_A = d^*_A)$ **then**
5: Calculates $ID_{A1} = ID_A \oplus h(M_A \| PK \| T_1)$, $K_1 = h(PK_B \| X_A \| T_1)$
Encrypted $E_1 = E_{K_1}(ID_{A1}, M_A)$
6: Eavesdrop the authentication request $M_1 = \{E_1, T_1\}$ during the login authentication phase
7: Computes $N = h(M_A \| M_B \| ID^*_A \| ID_B \| T_1)$, $SK_B = h(ID^*_A \| ID_B \| N \| M_A \| M_B \| b.a.g \| T_3)$
8: Eavesdrop the authentication request message $M_2 = \{E_2, T_3\}$ during the authentication phase.
9: **if** $(N^* \stackrel{?}{=} N)$ **then**
10: Get the private key, call the Reveal oracle on Input method, N of U_B as $SK^*_{AB} \leftarrow Reveal(a)$ and $SK^*_{AB} \leftarrow Reveal(b)$.
11: Accept ID'_A, N and SK_{AB} as the original identity ID_A of the U_A, the private key N of the U_B, and the session key SK_{AB} between U_A and U_B.
12: return (Success)
13: **else**
14: return (Failure)
15: **end if**
16: **else**
17: return (Failure)
18: **end if**

2) IMPERSONATION ATTACK

Any $U_{\mathcal{A}}$ get the message $M_1 = \{E_1, T_1\}$ and try to computes $E_1 = E_{K_1}(ID_{A1}, M_A)$ this is not an easy for any opponent because of E_1 contain secrete parameter $K_1 = h(PK_B \| X_A \| T_1), ID_{A1} = ID_A \oplus h(M_A \| PK \| T_1)$ and $M_A = a.g$. Consequently, no attacker can imitate E_1. The $SGAK$ thereby defends against impersonation attacks.

3) REPLAY ATTACK

The most frequent countermeasures for replay attacks are timestamps and random numbers. Even so, both of these are present in SGAK. The time stamp condition verifies as $T_i - T_j \leq \bigtriangleup T$, where $\bigtriangleup T$ is the valid period and $a, b \in Z^*_q$ where q is a huge prime number and a, b are new random numbers.

4) PRIVILEGED INSIDER ATTACK

There is no verifier repository maintained by either interacting parties or third parties in the proposed protocol. Interacting participants utilize their respective secret keys for the authentication process. Hence, SGAK is secure against the stolen verifier and insider attacks.

5) EAVESDROPPING ATTACK

Eavesdropping attacks are mitigated by our proposed protocol, as all parameters are protected by hash algorithms and fresh random numbers in each authentication round. This proactive approach ensures that attackers cannot access any critical parameters or user identities.

6) DENIAL OF SERVICE (DOS) ATTACKS

In SGAK, the U_A does, in fact, initiate the mutual authentication process by inputs his/her ID'_A and then verify the legitimacy by verify $d'_A \stackrel{?}{=} d_A$ where $d'_A = h(ID'_A \| X_A)$. In this process, the system determines that the user is not authorized if the verifying condition is not met. In order to stop DoS attacks, communication is instantly turned off.

7) EPHEMERAL SECURITY LEAKAGE ATTACK

Our proposed protocol safe against ephemeral security leakage attacks by preventing the adversary $\mathcal{A}$ from computing the session key SK without knowledge of both long-term and short-term parameters. The security of the suggested protocol remains intact in both scenarios, where temporary secret parameters or permanent secret parameters are unknown to the attacker.

8) SESSION KEY VERIFICATION AND SECURITY

In the recommended scheme, the user verifies their session key by verifying $N^* \stackrel{?}{=} N$ where $N^* = h(M_A \| M_B \| ID_A \| ID_B^* \| T_1)$ and $N = h(M_A \| M_B \| ID_A^* \| ID_B \| T_1)$ have various secrete parameters. Session key verification and security are thus provided by SGAK.

9) MESSAGE AUTHENTICATION

The message authentication of proposed scheme as follows:

Step 1: U_B receive the message $M_1 = \{E_1, T_1\}$ and verifies $T_2 - T_1 \leq \bigwedge T$ and hash values.

Step 2: U_A obtain the communication message $M_2 = \{E_2, T_3\}$ and verifies $T_4 - T_3 \leq \bigwedge T$ and hash value $N^* \stackrel{?}{=} N$.

Thus, a message secured by constraints for verification, encryption/decryption rule and hash values it is not a guessing essay for any attacker. Thus, *SGAK* protects the message authentication.

10) KNOWN KEY AGREEMENT

SGAK has session key agreement in authentication phase, U_B computes $SK_B = h(ID_A^* \| ID_B \| N \| M_A \| M_B \| b.a.g \| T_3)$ and U_A computes $SK_A = h(ID_B \| ID_B^* \| N^* \| M_A \| M_B \| \ a.b.g \| T_3)$. Thus, $SK = SK_A = SK_B$. Hence, *SGAK* provided known key agreement.

11) USER ANONYMITY

In authentication phase U_A sends anonymous identity $ID_{A1} = ID_A \oplus h(M_A \| PK \| T_1)$ and encrypted in $E_1 = E_{K_1}(ID_{A1}, M_A)$ where $K_1 = h(PK_B \| X_A \| T_1)$. Similarly U_B sends his/her anonymous identity $ID_{B1} = ID_B \oplus h(M_A \| M_B \| T_3)$ to U_A and encrypted in $E_2 = E_{K_2}(ID_{B1}, N, M_B)$ with the help of $K_2 = h(M_A \| T_3 \| ID_A^*)$. Thus, our proposed protocol maintain user anonymity.

12) DATA CONFIDENTIALITY

One method of protecting data from adversaries is data confidentiality. The data confidentiality of data are as follows:

Step 1: U_A encrypt $E_1 = E_{K_1}(ID_{A1}, M_A)$ with the help of $K_1 = h(PK_B \| X_A \| T_1)$. After that U_B decrypt $(ID_{A1}, M_A) = D_{K_1^*}(E_1)$ with the help of $K_1^* = h(PK_B \| X_A \| T_1)$.

Step 2: U_B encrypt $E_2 = E_{K_2}(ID_{B1}, N, M_B)$ with the help of $K_2 = h(M_A \| T_3 \| ID_A^*)$. After that U_A decrypt $(ID_{B1}, N, M_B) = D_{k_2^*}(E_2)$ with the help of $K_2^* = h(M_A \| T_3 \| ID_A)$.

Let if $\mathcal{A}$ collect all information during communication, then he/she decrypt the message, which can not be possible for $\mathcal{A}$ as there are verifying conditions with hash values.

13) KEY FRESHNESS

The session key in the suggested protocol has a time stamp and a new random number that are unique for each session during the authentication process. The uniqueness of these parameter confirm the unique key for each session. The key freshness attribute of SGAK is thus confirmed by the unique key for every session.

14) UNTRACEABILITY

Cryptographic protocols provide untraceability if it has two properties (i) $\mathcal{A}$ fails to distinguish the original identity of users. (ii) $\mathcal{A}$ is unable to determine whether two distinct sessions that were started at different times are associated with the same user. Thus, SGAK keeps both of those properties.

15) PERFECT FORWARD SECRECY

By including perfect forward secrecy, the protocol further strengthens its commitment to security. In order to ensure that adversaries could not compute the session key for sessions in the past or future, even in the event that the long-term keys of both parties were compromised, the ephemeral secrets of users a, b play an important role in the computation of the session key. The confidentiality of previous or upcoming sessions is not compromised by compromising the long-term keys of the communicating parties because these secrets are unique to each session and are never reused. Further, In SGAK, U_A and U_B determine the session key by $SK_A = h(ID_B \| ID_B^* \| N^* \| M_A \| M_B \| a.b.g \| T_3)$ and $SK_B = h(ID_A^* \| ID_B \| N \| M_A \| M_B \| b.a.g \| T_3)$. Here, SK_A and SK_B includes requirements for verification with $a.b.g$. Due to the difficulty of the ECDLP computation, even if an opponent manages to estimate users private keys, they are unable to compute SK and hence cannot guess the session

key of the users. Hence, SGAK is able to maintain perfect forward secrecy.

V. PERFORMANCE ANALYSIS

Here, we offer in-depth examination and evaluation of the suggested protocol with previous research. The comparison of comparable [6], [7], [11], [14], [15], [16], [17], [18], [20], [21], [22], [47] schemes and SGAK performance analysis finished with four subsections. Namely Comparison of the security and functionality features, computational, communication costs comparison and energy consumption comparison. The conclusion of performance analysis demonstrates that in smart grid network proposed protocol compared to other protocols SGAK provides higher security and efficiency.

A. COMPARISON OF THE SECURITY AND FUNCTIONALITY FEATURES

In Table 3, we summarize security analysis of SGAK and those scheme which are available in literature [6], [7], [11], [14], [15], [16], [17], [18], [20], [21], [22], [47]. While related protocols are vulnerable to different types of security attacks due to different security flaws. It can be notice that Wu and Zhou [11] does not stand with A_{MI}, A_{UA}, A_{SK}, A_{PR} and A_{IN}. Sule et al. [16] does not maintain A_{UA}, A_{ST}, A_{ME}, A_{FA}, A_{DO} and A_{IN} Mahmood et al. [17] scheme does not maintain A_{UA}, A_{DA}, A_{ME}, A_{IM}, A_{SK}, A_{DO}, A_{IN}, A_{ST}, A_{FA}. Li et al. [18] scheme does not maintain A_{UA}, A_{DA}, A_{ST} and A_{IN}. While Mahmood et al. [6] protocol fails against A_{UA}, A_{IM}, A_{IN}, A_{ST}. Odelu et al. [15] scheme does not maintain A_{DA}, A_{ME}, A_{IM}, A_{DO}, A_{IN}, A_{ST} and A_{FA}. He et al. [47] scheme does not maintain A_{DA}, A_{ME}, A_{IM}, A_{DO}, A_{IN}, A_{ST} and A_{FA}. Mood and Nikooghadam [20] does not provided A_{UA}, A_{IM}, A_{DO} and A_{IN}. Tsai and Lo [14] does not maintain A_{DO}, A_{IN}, A_{ST} and A_{FA}. Wazid et al. [22] does not provided A_{IN}, A_{L1}, A_{L2} and A_{FS}. Abbasinezhad-Mood and Nikooghadam [7] does not provided A_{UA}, A_{DA}, A_{DO}, A_{L1} and A_{L2}. Braeken et al. [21] does not provided A_{UA}, A_{DA}, A_{IN}, A_{FA}, A_{L1} and A_{L2}.

B. COMPARISON OF THE COMPUTATION COST

We calculate the computational cost of SGAK in this instance and compare it to comparable methods [6], [7], [11], [14], [15], [16], [17], [18], [20], [21], [22], [47], Table 4, provides an illustration and evaluation. The configuration of the system is 2.0 GB RAM and Pentium Dual core E2200 2.20 GHz processor computation cost of various cryptographic operations are [7], [48]. T_{HO}: execution of hash operation $\cong$ 0.0023 ms, T_P: time for bilinear pairing $\cong$ 5.811 ms, T_{PM}: time for point multiplication $\cong$ 2.226 ms, T_{ME}: time for modular exponentiation $\cong$ 3.85 ms, T_{PKED}: public key encryption or decryption execution time $\cong$ 3.85 ms, T_{HMAC}: time for HMAC operation $\cong$ 0.0046 ms, T_F: execution of fuzzy extraction operation $\cong$ 2.226 ms, T_{ESED}: symmetric encryption/decryption execution time $\cong$ 0.0046 ms, T_{PA}: time for point addition $\cong$ 0.0288 ms.

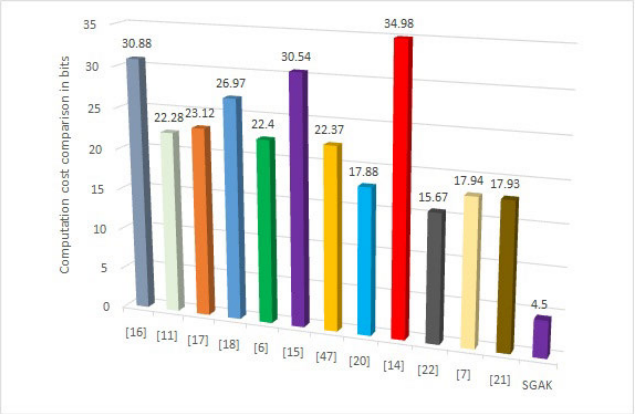

FIGURE 3. A comparison of the computation cost.

In SGAK, U_A side perform two symmetric encryption/decryption, one elliptic curve point multiplication and six one way secure hash function i.e $2T_{ESED} + T_{PM} + 6T_{HO}$ which takes execution time $\cong$ 2.25 ms. On the other side U_B perform two symmetric encryption/decryption, one elliptic curve point multiplication and seven one way secure hash function i.e $2T_{ESED}+T_{PM}+7T_{HO}$ which takes approximately execution time $\cong$ 2.25 ms. Thus, total execution time to perform these operation in proposed protocol is $\cong$ 4.50 ms. Similarly, the other related protocols [6], [7], [11], [14], [15], [16], [17], [18], [20], [21], [22], [47] takes 30.80, 22.28, 23.12, 26.97, 22.40, 30.54, 22.37, 17.88, 34.98, 15.67, 17.94 and 17.93 ms respectively. The computation cost of SGAK is 4.5 ms which is much less than other existing schemes in same environment. The average gross computational cost of all protocols other than the suggested protocol is found to be in order to better understand its advantage $\cong$ 22.11 *ms*. The suggested protocol overall computational cost is less than the mean of other protocol costs for $\frac{22.11-4.5}{22.11} \cong 79.64\%$ The comparison of the computation cost is displayed in Table 4. The efficiency of SGAK and other related frameworks in terms of computation cost given in Figure 3.

C. COMPARISON OF THE COMMUNICATION COST

We show the evaluation and comparison of communication costs with related protocols in Table 5. The communication costs of different cryptographic elements, taken as generated random number takes 128 bits, identifier takes 64 bits, time-stamp takes 32 bits, ECC encryption/decryption takes 320 bits, ECC point takes 320 bits and secure hash function takes 256 bits.

The performance evaluation and comparison of SGAK with the comparative protocol shown in Figure 4. The communication overhead of SGAK computes as, if U_A sends $\{E_1, T_1\}$. It takes $320 + 32 \cong 352$ bits. Further, U_B sends $\{E_2, T_3\}$ to U_A, it also consumed 352 bits. Thus, the total overhead of SGAK is 704 bits in overall communication. Similarly, other related protocols such as [6], [7], [11], [14], [15], [16], [17], [18], [20], [21], [22], and [47] used

TABLE 3. Comparison security and functionality features.

Security Attack	[11]	[16]	[17]	[18]	[6]	[15]	[46]	[20]	[14]	[22]	[7]	[21]	Proposed
A_{MI}	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
A_{RP}	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
A_{UA}	×	×	×	×	×	✓	✓	×	✓	✓	×	×	✓
A_{DA}	✓	✓	×	×	✓	×	×	✓	✓	✓	×	×	✓
A_{ME}	✓	×	×	✓	✓	×	×	✓	✓	✓	✓	✓	✓
A_{IM}	✓	✓	×	✓	×	×	×	×	✓	✓	✓	✓	✓
A_{SK}	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
A_{DO}	×	×	×	✓	✓	×	×	×	×	✓	×	✓	✓
A_{PR}	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
A_{IN}	×	×	×	✓	×	×	×	×	×	×	✓	×	✓
A_{ST}	✓	×	×	×	×	×	×	✓	×	✓	✓	✓	✓
A_{FA}	×	×	×	×	✓	×	×	✓	×	✓	✓	×	✓
A_{L1}	×	×	×	×	×	×	×	×	×	×	×	×	✓
A_{L2}	×	×	×	×	×	×	×	×	×	×	×	×	✓
A_{FS}	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓

Observation $\Longrightarrow$ × : doesn't stop the attack and ✓ : Stop the attack.
A_{UA} : User anonymity, A_{DA} : Data confidentiality, A_{ME} : Message authentication, A_{MI} : Man in the middle attack, A_{DO} : Denial of service attack, A_{PR} : Provision of key agreement, A_{IM} : Impersonation attack, A_{ST} : Stolen verifier attack, A_{RP} : Replay attack, A_{SK} : Session key agreement, A_{IN} : Insider attack, A_{FA} : Fails to protection session key, A_{L1} : Low communication cost, A_{L2} : Low computation cost, A_{FS} : Formal security.

TABLE 4. A comparison of costs of computation.

	U_A	U_B	Computational Cost(ms)
Sule et al. [16]	$2T_{ME} + 2T_{PKED} + T_{HMAC} \cong 15.40$	$2T_{ME} + 2T_{PKED} + T_{HMAC} \cong 15.40$	$\cong 30.80$
Wu and Zhaou [11]	$6T_{PM} + T_{ESED} + T_{HO} \cong 13.36$	$4T_{PM} + T_{ESED} + 4T_{HO} \cong 8.92$	$\cong 22.28$
Mahmood et al. [17]	$3T_{ME} + 2T_{ESED} + T_{HO} + T_{HMAC} \cong 11.56$	$3T_{ME} + 2T_{ESED} + T_{HO} + T_{HMAC} \cong 11.56$	$\cong 23.12$
Li et al. [18]	$3T_{ME} + 3T_{HO} \cong 11.56$	$4T_{ME} + 3T_{HO} \cong 15.41$	$\cong 26.97$
Mahmood et al. [6]	$5T_{PM} + 2T_{PA} + 4T_{HO} \cong 11.2$	$5T_{PM} + 2T_{PA} + 4T_{HO} \cong 11.2$	$\cong 22.40$
Odelu et al. [15]	$3T_{PM} + T_{PA} + 6T_{HO} + T_{ME} \cong 10.57$	$2T_{PM} + T_{PA} + 6T_{HO} + 2T_P + T_{ME} \cong 19.97$	$\cong 30.54$
He et al. [46]	$4T_{PM} + T_{PA} + 5T_{HO} \cong 8.94$	$6T_{PM} + 2T_{PA} + 6T_{HO} \cong 13.43$	$\cong 22.37$
Mood and Nikooghadam [20]	$4T_{PM} + T_{PA} + 5T_{HO} \cong 8.94$	$4T_{PM} + T_{PA} + 5T_{HO} \cong 8.94$	$\cong 17.88$
Tsai and Lo [14]	$4T_{PM} + T_{PA} + 5T_{HO} + T_{ME} \cong 12.79$	$3T_{PM} + 2T_P + 5T_{HO} + T_{ME} + T_{PA} \cong 22.19$	$\cong 34.98$
Wazid et al. [22]	$4T_{PM} + 2T_{PA} + 5T_{HO} \cong 8.97$	$2T_{PM} + 8T_{HO} + T_F \cong 6.7$	$\cong 15.67$
Mood and Nikooghadam [7]	$4T_{PM} + 2T_{PA} + 4T_{HO} \cong 8.97$	$4T_{PM} + 2T_{PA} + 4T_{HO} \cong 8.97$	$\cong 17.94$
Braeken et al. [21]	$4T_{PM} + T_{PA} + T_{ESED} + 5T_{HO} \cong 8.95$	$4T_{PM} + 2T_{PA} + T_{ESED} + 7T_{HO} \cong 8.98$	$\cong 17.93$
SGAK	$2T_{ESED} + T_{PM} + 6T_{HO} \cong 2.25$	$2T_{ESED} + T_{PM} + 7T_{HO} \cong 2.25$	$\cong 4.50$

TABLE 5. A comparison of the cost of communication.

	Communication cost in bits	Number of messages
Sule et al. [16]	4416	3
Wu and Zhaou [11]	2656	4
Mahmood et al. [17]	4768	2
Li et al. [18]	2752	2
Mahmood et al. [6]	1792	2
Odelu et al. [15]	3840	3
He et al. [46]	1664	3
Mood and Nikooghadam [20]	1440	3
Tsai and Lo [14]	3520	3
Wazid et al. [22]	1536	3
Mood and Nikooghadam [7]	1792	3
Braeken et al. [21]	1280	3
SGAK	704	2

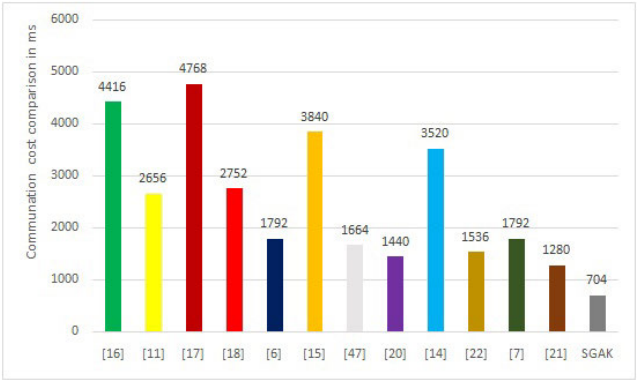

FIGURE 4. A comparison of the cost of communication.

4416, 2556, 4768, 2756, 1792, 3840, 1664, 1440, 3520, 1536, 1792 and 1280 bits respectively. The communication cost of SGAK is 704 bits which is much less than other existing schemes in same environment. The average gross communication cost of all protocols other than the suggested protocol is found to be in order to better understand its advantage ≅2473.85. The suggested protocol overall computational cost is less than the mean of other protocol costs for $\frac{2473.85-704}{2473.85} \cong 71.54\%$. The efficiency of SGAK and other related frameworks in terms of communication cost given in Figure 4.

D. ENERGY CONSUMPTION

The communication system uses energy during its implementation, which is referred to as energy consumption. It is

measured in millijoule (mJ). Based on [49] it is determined as $EC_{et} = TC2 * P_p$, where P_p is the maximal processing power, $TC2$ is the total computational cost, and EC_{et} is the consumed energy. Table 6, shows the total energy consumption of our designed protocol and other related protocols. The smart grid authentication technique proposed in this paper has the potential to correctly minimize energy consumption when compared to other existing schemes. The proposed protocol uses very less energy than alternative protocols, as shown in energy consumption Figure 5. This protocol can be seen as highly practical for the SG environment because of the limitations of computing speed, bandwidth, and other resources of the devices deployed in the user side of the smart grid communication system. Through theoretical and experimental analysis, as well as a comparison with alternative authentication protocols in a smart grid environment, it is demonstrated that the proposed protocol offers a significant performance and security advantage.

TABLE 6. Evaluation of energy consumption.

Protocols	Evaluation of energy consumption (in mJ)
Sule et al. [16]	$30.80 * 10.88 = 335.104$
Wu and Zhaou [11]	$22.28 * 10.88 = 242.4064$
Mahmood et al. [17]	$23.12 * 10.88 = 251.5456$
Li et al. [18]	$26.97 * 10.88 = 293.4336$
Mahmood et al. [6]	$22.40 * 10.88 = 243.712$
Odelu et al. [15]	$3.54 * 10.88 = 332.2752$
He et al. [46]	$22.37 * 10.88 = 243.3856$
Mood and Nikooghadam [20]	$17.88 * 10.88 = 194.5344$
Tsai and Lo [14]	$34.98 * 10.88 = 380.5824$
Wazid et al. [22]	$15.67 * 10.88 = 170.4896$
Mood and Nikooghadam [7]	$17.94 * 10.88 = 195.1872$
Braeken et al. [21]	$17.93 * 10.88 = 195.0784$
SGAK	$4.5 * 10.88 = 48.96$

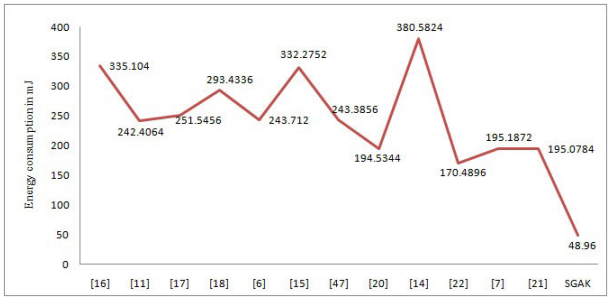

FIGURE 5. Evaluation of energy consumption.

VI. CONCLUSION

This paper presented a secure and efficient protocol for SG communication that is lightweight, anonymous and authenticated by using elliptic curve cryptography. It offers secure communication in a smart grid environment and is resistant to well known security attacks. We have confirmed the security of our proposed protocol and showed that it provides stronger security than the current authenticated and key agreement protocols by using both formal and informal security analysis. The presented protocol achieves high volume of security with minimum computational cost and communication cost in comparison with other existing protocols. The proposed protocol takes a minimum executing time of ≈4.5 msec for completing the entire login session establishment, and it requires only 704 bits as communication overhead. The computational cost is reduced to ≈79.64%, cost of communication is reduced ≈71.54% and energy consumption reduced to ≈79.65%, compared to the other existing authentication protocols. Our proposed protocol provides a robust security for communication but also offers opportunities for further research and application in the secure communication technologies. This research article provides open avenues for future direction for designing a secure authentication for SG communication system by using ring signature, blockchain, lattice based cryptography with post quantum mechanism.

REFERENCES

[1] H. Zheng, "Research on low-carbon development path of new energy industry under the background of smart grid," *J. King Saud Univ., Sci.*, vol. 36, no. 3, Mar. 2024, Art. no. 103105.

[2] M. A. Rahman, M. R. Islam, M. A. Hossain, M. S. Rana, M. J. Hossain, and E. M. Gray, "Resiliency of forecasting methods in different application areas of smart grids: A review and future prospects," *Eng. Appl. Artif. Intell.*, vol. 135, Sep. 2024, Art. no. 108785.

[3] O. Majeed Butt, M. Zulqarnain, and T. Majeed Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network," *Ain Shams Eng. J.*, vol. 12, no. 1, pp. 687–695, Mar. 2021.

[4] R. E. Brown, "Impact of smart grid on distribution system design," in *Proc. IEEE Power Energy Soc. Gen. Meeting, Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–4.

[5] M. M. Fouda, Z. Md. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[6] 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.

[7] 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.

[8] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Austria: Springer, 2001, pp. 453–474.

[9] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 196–201.

[10] H. Nicanfar and V. C. M. Leung, "Password-authenticated cluster-based group key agreement for smart grid communication," *Secur. Commun. Netw.*, vol. 7, no. 1, pp. 221–233, Jan. 2014.

[11] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

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

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

[14] 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.

[15] 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.

[16] R. Sule, R. S. Katti, and R. G. Kavasseri, "A variable length fast message authentication code for secure communication in smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, pp. 1–6.

[17] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Comput. Electr. Eng.*, vol. 52, pp. 114–124, May 2016.

[18] 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.

[19] V. Kumar, A. A. Khan, and M. Ahmad, "Design flaws and cryptanalysis of elliptic curve cryptography-based lightweight authentication scheme Design flaws and cryptanalysis of elliptic curve cryptography-based lightweight authentication scheme," in *Proc. Adv. Data Sci., Secur. Appl. (ICDSSA)*, pp. 169–179.

[20] 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, 2018.

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

[22] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, 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, Jul. 2019.

[24] K. Yasunaga and K. Yuzawa, "On the limits of computational fuzzy extractors," *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 605, Oct. 2014.

[25] A. A. Khan, V. Kumar, and M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 3, pp. 698–705, Mar. 2022.

[26] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for Internet of Things-enabled smart grid systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021.

[27] S. H. Baghestani, F. Moazami, and M. Tahavori, "Lightweight authenticated key agreement for smart metering in smart grid," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4983–4991, Sep. 2022.

[28] Y. Li, "An improved lightweight and privacy preserving authentication scheme for smart grid communication," *J. Syst. Archit.*, vol. 152, Jul. 2024, Art. no. 103176, doi: 10.1016/j.sysarc.2024.103176.

[29] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications," *Secur. Commun. Netw.*, vol. 2019, Mar. 2019, Art. no. 3263902.

[30] D. Dey, S. Chandra, and N. Ghosh, "HessianAuth: An ECC-based distributed and efficient authentication mechanism for 6LoWPAN networked IoT devices," in *Proc. 24th Int. Conf. Distrib. Comput. Netw.*, Jan. 2023, pp. 227–236.

[31] K. A. Farrea, Z. Baig, R. R. M. Doss, and D. Liu, "Provably secure optimal homomorphic signcryption for satellite-based Internet of Things," *Comput. Netw.*, vol. 250, Aug. 2024, Art. no. 110516.

[32] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[33] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr., V. Y. Pillitteri, T. L. Brewer, N. T. Golmie, D. H. Su, A. C. Eustis, D. Holmberg, and S. T. Bushby, "NIST framework and roadmap for smart grid interoperability standards, release 3.0," NIST, Gaithersburg, MD, USA, Tech. Tech. Rep. NIST SP 1108r3, 2014, doi: 10.6028/nist.sp.1108r3.

[34] A. Kumari, M. Yahya Abbasi, V. Kumar, and A. A. Khan, "A secure user authentication protocol using elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 521–530, May 2019.

[35] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, pp. 1–16, Dec. 2010.

[36] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 259–277, Feb. 2006.

[37] W. Stallings, *Cryptography and Network Security*, 4th ed., Chennai, India: Pearson, 2006.

[38] A. A. Khan, V. Kumar, J. Srinivas, S. Kumari, and M. K. Gupta, "RAKS: Robust authentication and key agreement scheme for satellite infrastructure," *Telecommun. Syst.*, vol. 81, no. 1, pp. 83–98, Sep. 2022.

[39] V. Kumar, S. Jangirala, and M. Ahmad, "An efficient mutual authentication framework for healthcare system in cloud computing," *J. Med. Syst.*, vol. 42, no. 8, p. 142, Aug. 2018.

[40] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Adhoc Sensor Wireless Netw.*, vol. 21, no. 1, p. 121, 2014.

[41] A. K. Das, N. R. Paul, and L. Tripathy, "Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem," *Inf. Sci.*, vol. 209, pp. 80–92, Nov. 2012.

[42] V. Odelu, A. K. Das, and A. Goswami, "A secure effective key management scheme for dynamic access control in a large leaf class hierarchy," *Inf. Sci.*, vol. 269, pp. 270–285, Jun. 2014.

[43] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, and M. U. Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 1–15, Jan. 2017.

[44] S. H. Islam, "Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 78, no. 3, pp. 2261–2276, Nov. 2014.

[45] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, 1999, pp. 388–397.

[46] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[47] 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.

[48] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014.

[49] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012.

AKBER ALI KHAN received the M.Sc. (Tech.) degree in industrial mathematics with computer application from the Department of Mathematics, Jamia Millia Islamia, New Delhi, India, and the Ph.D. degree in mathematics from Jamia Millia Islamia, in 2021. Currently, he is an Assistant Professor with the Department of Applied Sciences and Humanities, IIMT College of Engineering, Greater Noida, Uttar Pradesh, India. He has qualified Faculty Aptitude Test (FATE-2016) in mathematical science with a grade A, conducted by AKTU, Uttar Pradesh. He has authored or co-authored dozens of research papers in reputed international journals and conferences, including SCI/SCIE, Scopus, and Web of Science. Also, he has co-authored books titled *Applied Mathematics-I* and *Applied Mathematics-II* for diploma engineering courses. His research interests include cryptography, with a particular focus on the design and analysis of authentication protocols for secure communication. His current research interests include authentication protocols for secure communications, smart grid security and privacy, V2G security and privacy, blockchain, elliptic curve cryptography, optimization, and applied mathematics. He is a Lifetime Member of the MathTech Thinking Foundation (MTTF). He served as a Reviewer of reputed journals, such as *Journal of Systems Architecture*, IEEE Access, *Electrical Power and Energy Systems*, *Cybernetics and Systems*, *Transactions on Emerging Telecommunications Technologies*, *Peer-to-Peer Networking and Applications*, *Scientific Reports*, *Telecommunication Systems*, *Cluster Computing*, *Signal, Image and Video Processing*, and *Journal of Super Computing*.

VINOD KUMAR received the Master of Philosophy degree in mathematics from Chaudhary Charan Singh University, Meerut, India, the Master of Technology degree in computer science and data processing from Indian Institute of Technology Kharagpur, Kharagpur, India, and the Ph.D. degree in elliptic curve cryptography (ECC)-based authentication protocols in cloud computing from the Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi, India. He qualified for the CSIR National Eligibility Test (NET) in mathematical sciences, in 2011. In 2011, he also qualified for the Graduate Aptitude Test in Engineering (GATE) in mathematics. He has over nine years of experience in teaching, research, and industry in the fields of mathematics, information security, and related fields. He is currently an Assistant Professor with the Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi, India. He has supervised five M.Tech. scholars in the area of security and optimization. He is a Lifetime Member of the Operational Research Society of India (ORSI), India, and the MathTech Thinking Foundation (MTTF), India. He has received the ''Recognition/Reviewer Certificate Award'' from many reputed journals. He has presented 28 research papers and given talks at conferences and workshops. He has authored or co-authored 52 research papers in reputed international journals and conferences, such as IEEE, Elsevier, Springer, Wiley, and Taylor and Francis. Also, he has co-authored a book titled *Elementary Real Analysis*. He received the Best Paper Award 2022 titled ''RSEAP: RFID-Based Secure and Efficient Authentication Protocol for Vehicular Cloud Computing'' from Q1 and SCIE journal *Vehicular Communications* (Elsevier), with an impact factor is 6.7. He has also served as a reviewer for many renowned journals. He has been associated with many conferences as a TPC member and the session chair.

RAMAKANT PRASAD received the B.Sc. degree (Hons.) in mathematics from the Science College, Patna, in 2002, the M.Sc. degree in mathematics from Indian Institute of Technology Delhi, in 2005, the M.Tech. degree in computer science and data processing from Indian Institute of Technology Kharagpur, in 2008, and the joint M.Sc. degree in financial mathematics from the University of Edinburgh and Heriot-Watt University, in 2016. Currently, he is an Assistant Professor (Selection Grade) with the Gargi College, University of Delhi, India. His research interests include cryptography and applied mathematics.

M. JAVED IDRISI received the M.Sc. degree in mathematics from Jamia Millia Islamia (a Central University of India), New Delhi, India, in 2008, and the Ph.D. degree in mathematics from Maharshi Dayanand University, Rohtak, India, in 2015. He is currently an Associate Professor with the Department of Mathematics, College of Natural and Computational Science, Mizan-Tepi University, Tepi Campus, Ethiopia. He has more than seven years of post-Ph.D. teaching experience at the university level. Till date, he has authored a total of 33 research articles, out of which 15 research articles are published in SCI-listed journals (Springer and Elsevier) and the rest are in Scopus and peer-reviewed journals. He has also authored two books titled *Applied Mathematics-I* and *Applied Mathematics-II* for diploma engineering courses. He is a reviewer of several SCI and Scopus-indexed journals. His research interests include mathematical modeling, differential equations, astronomy, astrophysics, cryptography, satellite security and privacy, and network security and privacy. He is a Lifetime Member of the International Association of Engineers (IAENG), Hong Kong, China; the Centre for Fundamental Research in Space Dynamics and Celestial Mechanics, New Delhi, India; and the MathTech Thinking Foundation, Punjab, India.