mathematics

MDPI

Article

A Privacy-Preserving Authentication Scheme for a Blockchain-Based Energy Trading System

Seunghwan Son [1], Jihyeon Oh [1], Deokkyu Kwon [1], Myeonghyun Kim [1], Kisung Park [2] and Youngho Park [1,*]

[1] School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea; sonshawn@knu.ac.kr (S.S.); j2hnoh@knu.ac.kr (J.O.); kdk145@knu.ac.kr (D.K.); kimmyeong123@knu.ac.kr (M.K.)

[2] Electronics and Telecommunications Research Institute, Daejeon 34129, Republic of Korea; ks.park@etri.re.kr

* Correspondence: parkyh@knu.ac.kr

Abstract: The adoption of renewable energies such as solar power, heat pumps, and wind power is on the rise, and individuals have started generating energy using their own solar panels. In recent years, many blockchain-based energy trading schemes have been proposed. However, existing schemes cannot fully address privacy issues and dependency on energy brokers during energy trading. In this paper, we propose a privacy-preserving authentication scheme for blockchain-based energy traders. An energy user encrypts a request message through lightweight attribute-based encryption, and only energy sellers who have proper attribute keys can decrypt and conduct further processes with the energy user. We analyze the proposed scheme using both informal and formal methods, such as the BAN logic, AVISPA simulation tool, and RoR model. Furthermore, we compare the computational and communication costs of our scheme with related schemes and show that the proposed scheme has competitive performance.

Keywords: access control; lightweight attribute-based encryption (ABE); consortium blockchain; energy trading; mutual authentication

MSC: 68M12

check for updates

Citation: Son, S.; Oh, J.; Kwon, D.; Kim, M.; Park, K.; Park, Y. A Privacy-Preserving Authentication Scheme for a Blockchain-Based Energy Trading System. *Mathematics* **2023**, *11*, 4653. https://doi.org/10.3390/math11224653

Academic Editor: Jan Lansky

Received: 31 October 2023
Revised: 14 November 2023
Accepted: 14 November 2023
Published: 15 November 2023

1. Introduction

With the increasing interest in energy efficiency, smart grid and renewable energies are drawing considerable attention. A smart grid combines information and communication technology as well as power system operation to overcome the disadvantages of the traditional power grid system [1,2]. In traditional power grid systems, the power supply is unidirectional, and it is designed to produce more electricity than required to prepare for higher-than-expected power consumption. Therefore, it is not that efficient and inevitably generates wasted power. Conversely, in smart grid systems, distributed power based on renewable energies is available, and it is bidirectional in power supply. Furthermore, it can monitor energy consumption information to determine energy production and prevent global warming by reducing the use of fossil fuels. Renewable energies include solar power, micro-wind power, heat pumps, and so on [3,4]. These energies can be generated by individuals through solar panels and wind turbines installed in their houses, and they can use the energy by themselves or sell it to others. The realization of energy trading between individuals can reduce the costs associated with time and location-dependent power supply, and energy efficiency can be considerably improved.

The concept of decentralized energy production and peer-to-peer energy trading emerged about years ago [5], yet specific methods and solutions for peer-to-peer energy trading were not discussed much due to technical issues until a few years ago. As the use of smart thermostats, rooftop photovoltaic arrays, and battery energy storage systems grows and individuals' needs to reduce energy costs increase, discussions are underway to realize energy trading. Representatively, with the recent commercialization of electric vehicles, various solutions are being proposed for secure communication between vehicles and charging stations [6,7]. A charging station performs a similar role to a roadside unit in VANETs or an access point in mobile networks. However, P2P energy trading is more complicated because it involves communication between untrusted entities, and transparency, scalability, and reliability must be guaranteed for secure energy trading. Additionally, during the energy trading process, individual privacy must be guaranteed and protected from insider and impersonation attacks.

To resolve the problems, many blockchain-based peer-to-peer energy trading systems have been proposed during the past few years [8–11]. Blockchain technology is a suitable solution for realizing energy trading because it can guarantee the transparency and integrity of stored data [12–17]. However, public blockchains that use proof-of-work or proof-of-stake consensus algorithms have a scalability problem. The existing research solves the scalability problem of blockchain by designing energy brokers to maintain the consortium blockchain. Moreover, energy brokers perform various roles such as identity verification [18–20], matching [21,22], and issuing authentication tokens [23,24] for energy traders. However, existing schemes have the issue that energy traders are highly dependent on energy brokers. The energy broker is an essential entity to facilitate energy trading, but an energy broker can be an individual and can not be considered fully trusted [25]. Therefore, if energy brokers are fully aware of information about energy tradings, such as the location and status of energy users, then privacy issues can arise. To resolve these problems, it is necessary to design a mutual authentication scheme between energy traders, and it is important to consider how an energy trader initiates energy trading with the other party when energy brokers do not match energy users and sellers.

Therefore, we proposed a novel privacy-preserving authentication scheme for a blockchain-based energy trading system. We focused on preserving the privacy of energy users from energy brokers. To achieve this, we applied attribute-based encryption (ABE) to match an energy user and seller. Traditional pairing-based ABE [26] requires lots of computational cost and is difficult to make compatible with blockchain that is based on the Elliptic Curve Cryptosystem (ECC). Therefore, we adopted ECC-based lightweight ABE for the proposed scheme [27]. Compared to traditional ABE, ECC-based ABE does not perform operations that require a high amount of computation, such as bilinear pairing. Individuals have lower computation power than servers and utilizing lightweight ABE enables smooth communication. Furthermore, in the energy trading environment, energy purchasers can encrypt their request messages using ABE and disclose the message only to appropriate sellers. In the proposed scheme, when an energy user sends an energy trading request encrypted with attributes to an energy broker, the energy broker verifies the signature and then transmits the encrypted message to energy sellers. Then, an energy seller who has the proper attributes can decrypt the message and check the requested information. After that, the energy seller sends a response message to the energy user, they authenticate each other, and they can trade energy. The main contributions of this paper are as follows:

- We proposed a new blockchain-based energy trading scheme. We assumed that the energy broker is not a fully trusted entity. Therefore, energy brokers manage the blockchain and act as a middleman between energy traders but do not perform functions such as issuing an authentication token or matching energy traders.
- We adopted lightweight ABE-based access control for energy users. An energy request message of an energy user is encrypted and transmitted to the energy broker, and only energy sellers with the appropriate attributes can confirm the transaction details and respond to the energy buyer. The proposed model adopts ECC-based ABE, which has lower computational costs than pairing-based ABE and is more compatible with blockchain.

- We designed a mutual authentication scheme between energy purchasers and sellers. We analyzed the proposed scheme using informal methods and formal methods, such as the Burrows–Abadi–Needham (BAN) logic [28], the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool [29], and the Real-or-Random (RoR) model [30] and proved that the proposed scheme is correct, has resistance to replay attacks, and guarantees semantic security.

Paper Organization

In Sections 2 and 3, we provide related works and explain the preliminaries, respectively. In Section 4, we demonstrate the proposed system model and provide explanations of entities. In Section 5, we propose a secure authentication protocol for the blockchain-based energy trading system with access control. In Section 6, we informally and formally analyze our scheme, and, in Section 7, we compare the performance of our scheme with other schemes. We conclude this study in Section 8.

2. Related Works

In this section, we introduce recent studies conducted on blockchain-based energy trading systems and key agreement protocols in smart grids.

2.1. Blockchain-Based Energy Trading Systems

In this section, we introduce recent studies conducted on blockchain-based energy trading systems. In 2017, Li et al. [31] proposed blockchain-based energy trading for the industrial Internet of Things (IIoT) environment. They were the first to propose a secure energy trading solution using consortium blockchain, and many subsequent studies have been conducted based on this study. In their scheme, an energy purchaser sends a request to an energy broker. Next, the energy broker verifies the identity of the energy purchaser (EP), generates an authentication token, and sends the token to the EP. Then, the EP can trade the energy with an energy seller using the token. Their method does not guarantee the anonymity of energy purchasers and relies on energy brokers for the authentication process between energy traders. Gai et al. [32] highlighted that Li et al.'s scheme [31] cannot preserve the privacy of EPs. Their scheme mainly focuses on protecting privacy and ensuring the untraceability of EPs by configuring the account generation algorithm and black box operations. However, their scheme still has the problem that energy traders need to authenticate tokens issued by an energy broker to verify the legitimacy of the other party. Li et al. [33] proposed blockchain-enabled energy trading in IIoT environments. In their scheme [33], anonymous authentication was used for the users' privacy protection. Further, attribute-based encryption was used to guarantee fine-grained access control, and a timed commitment-based mechanism was designed for the verifiable fairness of energy trading. However, their scheme [33] has a traceability problem because the public keys of users are transmitted during energy trading. Guan et al. [34] proposed privacy-preserving energy trading using blockchain and ABE. In their scheme [34], Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was used for access control to protect the privacy of transaction initiators, and a credibility-based consensus algorithm was included. However, their scheme [34] does not describe which attribute value is used for encryption or decryption. It cannot guarantee the practicality of the proposed scheme.

The existing schemes [31–34] did not give much thought to mutual authentication and access control during energy trading. In this study, we design a secure authentication scheme for the blockchain-based energy trading system with access control.

2.2. Authentications in Smart Grids

In 2018, Li et al. [35] proposed an anonymous authentication scheme between the home area network gateway and the building area network gateway for smart grids. Li et al. [35] formally verified their protocol using ProVerif and asserted that their scheme was secure against various attacks. However, Li et al. did not formally prove the security of their protocol. Wu et al. [36] highlighted that the scheme in [35] could not resist impersonation attacks and was inefficient. Wu et al. proposed an efficient and anonymous scheme using ECC. They asserted that their scheme was more efficient than the other schemes in smart grids. Mahmood et al. [37] proposed an elliptic curve-based authentication scheme for smart grid communication. They claimed that their scheme was efficient and secure against various attacks. However, Abbasinezhad and Nikoogadam [38] proved that the scheme proposed by Mahmood et al. [37] could not prevent known session-specific temporary information attacks and could not guarantee perfect forward secrecy, and they proposed an enhanced scheme in the same environment. Although Abbasinezhad and Nikoogadam asserted that their enhanced scheme was secure, Chen et al. [39] showed that Abbasinezhad and Nikoogadam's scheme could not defend against replay attacks because an adversary could make an entity inaccessible to the network. Chen et al. [39] proposed a pairing-based authentication scheme with improved security. In 2021, Wu et al. [40] found that Chen et al.'s scheme was also vulnerable to known session-specific temporary information and impersonation attacks. Wu et al. proposed a bilinear pairing-based authentication protocol considering various attacks. However, in their scheme [40], the real identity of each entity was transmitted via a public channel, and anonymity and traceability could not be guaranteed.

The existing schemes [35–40] have security issues to adopt in energy trading systems. In this study, we improved these schemes and designed a robust protocol for the energy trading system.

3. Preliminary

In this section, we provide the preliminaries of our scheme.

3.1. Access Tree

We use the access tree defined in [26] as the access structure in our scheme. Let Γ be an access tree; then, the leaf nodes of Γ are attributes, and the non-leaf nodes of Γ are threshold gates. Γ contains the following notations when x is a node of Γ:$(\gamma, t(x), p(x), att(x), i(x), c(x))$. γ is the root node of Γ, $t(x)$ is a threshold value, $p(x)$ is a parent node, $att(x)$ is an attribute, $i(x)$ is an index, and $c(x)$ are child nodes of x. For example, let x be a non-leaf node. Then, if $t(x) = 1$, then x is an OR gate, and, if $t(x) = c(x)$, then x is an AND gate. A user must satisfy the access tree to decrypt the ciphertext encrypted with Γ, and, when the user satisfies Γ, it means that the user has attribute keys that can pass the threshold gate of γ.

3.2. Blockchain

Blockchain can be classified into three types: public, private, and consortium blockchain [41]. Public blockchain includes Ethereum and Bitcoin, which need the consensus of all the network participants to upload transactions to the blockchain. It is completely decentralized, yet it can be difficult to ensure real-time energy tradings. A private blockchain is controlled by a single authority. Compared to a public blockchain, it has better network scalability and efficiency. However, it is centralized and cannot provide transparency because network entities do not participate in the consensus. Consortium blockchains are managed by a number of entities. Compared to the private blockchain, it is decentralized, and, compared to the public blockchain, it can provide network scalability and has better efficiency. Energy trading occurs in a decentralized manner, and a centralized network structure is not suitable. Furthermore, many users will perform energy tradings, and network capacity must be guaranteed. Therefore, we utilize consortium blockchain for secure energy trading in our scheme. In our scheme, the blockchain is managed by energy brokers and records energy trading results.

3.3. Adversary Model

We adopted the Dolev–Yao (DY) adversary model [42] which is widely accepted [43–45] for analyzing the security of an authentication protocol. Under the DY model, an adversary A has the following capabilities.

- A can obtain the messages transmitted through public channels. A can attempt to eavesdrop, modify, or forge the messages.
- A can obtain the smart card of a network user and can extract the stored value via power analysis attacks [46,47].
- A can guess the identity and password to log into the obtained smart card. We assume that A can try to guess the identity and password simultaneously.
- A can attempt diverse attacks such as impersonation, session key disclosure, replay, and Man-in-the-Middle (MITM) attacks.

We also apply the Canetti and Krawczyk (CK) adversary model [48] to analyze the proposed protocol. The CK model considers additional attacks such as ephemeral session random numbers or long-term keys leakage attacks.

4. System Model

We describe the proposed system model. The model comprises four entities: the trusted authority (TA), energy broker (EB), energy user (EU), and energy seller (ES). Figure 1 shows the system model and a detailed description of each entity is provided as follows:

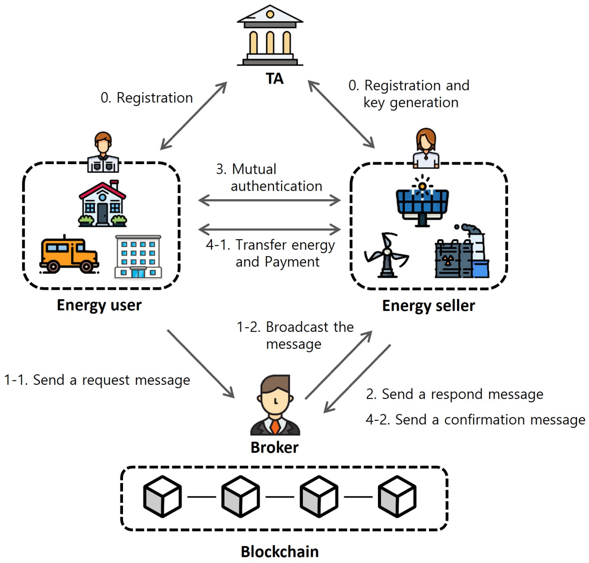

TA
0. Registration
0. Registration and key generation
3. Mutual authentication
4-1. Transfer energy and Payment
Energy user
Energy seller
1-2. Broadcast the message
1-1. Send a request message
2. Send a respond message
4-2. Send a confirmation message
Broker
Blockchain

Figure 1. The proposed blockchain-based energy trading model.

- **TA**: TA initializes the system, registers EBs and EUs, and issues attribute keys for ESs.
- **EB**: An EB acts as an intermediary between energy buyers and sellers and may be an individual or an institution [25]. An EB is not a fully trusted entity. After an EB receives an encrypted message from an EU, the EB verifies the signature of the message and then broadcasts the message to nearby ESs. When an ES receives a confirmation message, the EB verifies the message and uploads the transaction record to the blockchain.
- **EU**: EUs register with the TA to participate in the network. An EU generates an energy request message, which includes wallet address, energy type, demanding amount, price, location, and so on. After that, the encrypted message and the signature for the encrypted message are sent to the EB. The EB can only verify the signature without knowing the detailed information of the request message. Then, the EU mutually authenticates with an ES who has proper attribute keys and conducts energy trading with the ES.

- **ES**: ESs are issued attribute keys when registered with the TA. An ES receives an encrypted energy request message from the nearby EB and can decrypt the message if the ES has the proper attribute keys. After that, the ES conducts mutual authentication with the EU and transmits energy and receives payment. Then, the ES sends a confirmation message, including the EU and ES's signatures, to the EB.

5. Proposed Scheme

The proposed scheme comprises six phases: setup, registration, login, requesting, responding, and confirmation. In the setup phase, the TA generates and publishes system parameters. In the registration phase, the TA registers the EBs, EUs and ESs, generates public keys, creates wallet addresses, and issues smart cards for the EUs and ESs. In the login phase, an EU logs into the network using the smart card issued in the registration phase. In the requesting phase, an EU generates an energy request message, encrypts it using attributes, and sends the message to a nearby EB. Next, the EB verifies the message and broadcasts it to nearby ESs. Then, an ES who has corresponding attribute keys can decrypt the message and can send a response message to the EU. Then, the EU generates a smart contract for energy trading, the ES verifies the contract, and the trading is initiated. A detailed explanation of each step is below, and Table 1 shows the notations of our scheme.

Table 1. Notations and meanings.

Notation	Meaning
EU_j	j-th energy user
ES_k	k-th energy seller
EB_i	i-th energy broker
ID_j, PW_j	identity and password of EU_j
SC_j	smart card of EU_j
C_j	encrypted message of EU_j
$\{s_{j,x}\}_{x=1}^{K}$	EU_j's K wallet addresses
$\{M\}_k$	M is encrypted/decrypted with symmetric key k
Req_j	request message of EU_j
$[M]_s$	M is signed using key s with ECDSA

5.1. Setup

TA inputs security parameter λ; then, an elliptic curve (q, a, b, G, p) is generated. After that, TA selects cryptographic hash function $h(.)$, chooses $s_{TA} \in Z_q^*$, selects attribute universe $\mathbb{A} = \{A_1, ..., A_n\}$, and generates corresponding secret keys $s_1, s_2, ..., s_n \in Z_q^*$. In addition, TA generates $P \in G$ and computes $P_{TA} = s_{TA}.P$ and $P_m = s_m.P$ for all $m \in \{1, 2, ..., n\}$. The network public parameters are $\{G, P, P_{TA}, P_m, q, h(.)\}$, and the secret parameters are $\{s_{TA}, s_m\}$.

5.2. Registration

In the registration phase, TA registers EB_i, EU_j, and ES_k. The registration phase is conducted through a secure channel.

- EB registration: EB_i chooses a unique identity ID_i and sends (ID_i) to TA. After TA receives the message, TA checks whether ID_i is registered, and, if not, TA generates a random number s_i, computes $P_i = s_i.P$, publishes (ID_i, P_i), and sends s_i to EB_i. Then, EB_i keeps s_i secure and also writes permission for the blockchain.
- EU registration: For EU_j registration, EU_j chooses ID_j and PW_j and sends ID_j to TA. Then, TA checks whether ID_j is registered, and, if not, TA generates a fuzzy verifier $2^5 \leq l_j \leq 2^{10}$ and random numbers $\{s_{j,x}\}_{x=1}^{K}$ and stores $(\{s_{j,x}\}_{x=1}^{K}, l_j)$ in smart card SC_j. After that, TA computes $P_{j,x} = s_{j,x}.P$ for all x, which are wallet addresses of EU_j, and sends SC_j to TA. After EU_j receives SC_j, EU_j generates $r_j \in Z_q^*$ and computes $HPW_j = h(ID_j||PW_j||r_j)$, $X_j = r_j \oplus h(ID_j||PW_j)$, $Y_j = \{s_{j,x}\}_{x=1}^{K} \oplus HPW_j$,

and $Auth_j = h(HPW_j||\{s_{j,x}\}_{x=1}^{K})\ (mod\ l_j)$. Then, EU_j stores $(X_j, Y_j, Auth_j)$ in SC_j and deletes $\{s_{j,x}\}_{x=1}^{K}$ from SC_j. EU_j can guarantee anonymity for EB_i by using multiple wallet addresses.

- ES key generation: ES_k chooses ID_k, PW_k, and an access tree Γ_k and sends (ID_k, Γ_k) to TA. Then, for root node γ_k of Γ_k, TA generates a unique polynomial $q_{\gamma_k}(x)$ with order $t(\gamma_k) - 1$. TA sets $q_{\gamma_k}(0) = s_{\gamma_k}$ and chooses other points of $q_{\gamma_k}(x)$ randomly. After that, TA defines other polynomials for other non-leaf nodes z with $q_z(0) = q_{p(z)}(i(z))$. Next, for leaf nodes l of Γ_k, TA computes $D_l = q_l(0)/s_{att(l)}$. Then, the attribute keys for ES_k are $D_k = (D_l = q_l(0)/s_{att(l)}$, and $\forall l$ are leaf nodes of $\Gamma_k)$. This process is only executed the first time when generating attribute keys for Γ_k. After that, TA randomly generates $s_k \in Z_q^*$ and $2^5 \leq l_k \leq 2^{10}$ and computes $P_k = s_k.P$, which is a wallet address of ES_k. Furthermore, TA stores D_k and l_k in SC_k and sends SC_k to ES_k. ES_k generates $r_k \in Z_q^*$ and computes $HPW_k = h(ID_k||PW_k||r_k)$, $A_k = (r_k||s_k) \oplus h(ID_k||PW_k)$, $B_k = D_k \oplus HPW_j$, and $Auth_k = h(HPW_k||D_k||s_k)\ (mod\ l_k)$. ES_k deletes D_k and stores $(A_k, B_k, Auth_k)$ in SC_k. After the ES key generation phase, $P_{\gamma_k} = s_{\gamma_k}.P$ is published, and Γ_k maps to P_k, which is a wallet address of ES_k.

5.3. Login

In the login phase, EU_j inputs ID_j and PW_j to SC_j. Then, SC_j computes $r_j = X_j \oplus h(ID_j||PW_j)$, $HPW_j = h(ID_j||PW_j||r_j)$, and $\{s_{j,x}\}_{x=1}^{K} = Y_j \oplus HPW_j$ and checks $Auth_j \overset{?}{=} h(HPW_j||\{s_{j,x}\}_{x=1}^{K})\ (mod\ l_j)$. If it is equal, EU_j is logged in. ES_k can also be logged in the network in a similar way.

5.4. Requesting

EU_j chooses s_j from $\{s_{j,x}\}_{x=1}^{K}$, computes $P_j = s_j.P$, and generates a current timestamp T_1 and request message $Req_j = (P_j, demand_j, price_j, type_j, loca_j)$. These mean wallet address, demanding amount, price, charging type, and current location, respectively. Then, EU_j generates $a_j \in Z_q^*$, chooses attribute sets Ω_j, and computes $A_j = a_j.P$ and $A_{ij} = a_j.P_i$. After that, EU_j encrypts Req_j with Ω_j using the ECC-based attribute-based encryption [27].

- **Step 1**: EU_j randomly chooses $u_j \in Z_q^*$ and computes $u_j.P_{\gamma_k} = (U_x, U_y)$. If $u_j.P_{\gamma_k} = O$, EU_j chooses another u_j and repeats the process. Then, U_x is used as a symmetric key, and U_y is used to generate message authentication code (MAC).
- **Step 2**: EU_j computes $C_{Req_j} = \{Req_j\}_{U_x}$ and $MAC_{Req_j} = HMAC(Req_j, U_y)$. Furthermore, EU_j computes $C_\omega = u.P_\omega$ for each $\omega \in \Omega_j$.
- **Step 3**: The encrypted message is $C_j = (\Omega_j, C_{Req_j}, MAC_{Req_j}, C_\omega)$. EU_j computes $M_1 = (C_j, P_j) \oplus h(A_{ij})$, generates a signature $Sig_j = [A_j, C_j, T_1]_{s_j}$, and transmits (A_j, M_1, Sig_j, T_1) to EB_i.

After receiving the message, EB_i checks the validity of T_1, computes $A_{ij} = s_i.A_j$ and $(C_j, P_j) = h(A_{ij}) \oplus M_1$, and checks that Sig_j is valid. If it is, EB_i generates a unique request number rn_j, and a random number r_i. Then, EB_i computes $R_i = r_i.P$, $R_{ij} = r_i.P_j$, $M_i = rn_j \oplus h(A_{ij}||R_{ij})$, and $H_i = h(rn_j||R_{ij}||A_{ij}||T_2)$; transmits (R_i, M_i, H_i, T_2) to EU_j; and broadcasts (C_j, rn_j) to energy sellers. EU_j receives the message; checks the validity of T_2, computes $R_{ij} = s_j.R_j$ and $rn_j = M_i \oplus (h(A_{ij}||R_{ij}))$; and checks that $H_i \overset{?}{=} h(rn_j||R_{ij}||A_{ij})$. If it is equal, EU_j keeps rn_j securely.

5.5. Responding

If ES_k has the proper attribute keys, ES_k can decrypt C_j according to the following procedure.

- **Step 1**: For each leaf node l of Γ_k and $\omega = att(l)$, ES_k computes

$$\begin{aligned} D(C_j, D_k, l) &= D_l.C_\omega \\ &= q_l(0).s^{-1}_{att(l)}.u.P_{att(l)} \\ &= q_l(0).s^{-1}_{att(l)}.u.s_{att(l)}.P \\ &= q_l(0).u.P \end{aligned}$$

- **Step 2**: For each non-leaf node z, let $c(z)$ be a set of child nodes of z, $c^{'}(z)$ be an arbitrary subset of $c(z)$ with $t(z)$ nodes, and $c^{''}(z)$ be a set of indexes $\forall o \in c^{'}(z)$. Then, ES_k computes

$$\begin{aligned} D(C_j, D_k, z) &= \sum_{o \in c^{'}(z)} \Delta_{i(o),c^{''}(z)}(0).D(C_j, D_k, v) \\ &= \sum_{o \in c^{'}(z)} \Delta_{i(o),c^{''}(z)}(0).q_o(0).k.G \\ &= \sum_{o \in c^{'}(z)} \Delta_{i(o),c^{''}(z)}(0).q_z(i(o)).k.G \\ &= q_z(0).k.G \end{aligned}$$

ES_k recursively repeats these processes and can finally obtain $D(C_j, D_k, \gamma_k) = q_{\gamma_k}(0).u_j.P = (U_x, U_y)$. Then, ES_k can obtain $Req_j = \{C_{Req_j}\}_{U_x}$ and can check the integrity of the message using MAC_{Req_j}. After that, ES_k generates $a_k \in Z_q^*$ and a timestamp T_1; computes $a_k.P = A_k$, $a_k.P_j = A_{kj}$, $M_2 = h(A_{kj}||Req_j)$, and $M_3 = a_k + M_2.s_k$; and transmits (A_k, M_3, T_1). EU_j receives the message and checks the validity of T_1; computes $A_{kj} = A_k.s_j$, $M_2 = h(A_{kj}||Req_j)$, and $P_k = M_2^{-1}(M_3.P - A_k)$; checks $M_3.P \overset{?}{=} A_k + M_2.P_k$; and retrieves P_k from the blockchain. After that, EU_j generates timestamp T_2 and $k_j \in Z_q^*$; computes $K_j = k_j.P$, $K_{jk} = k_j.P_k$, $D_{jk} = s_j.P_k$, $M_4 = h(K_{jk}||Req_j||D_{jk})$, $M_5 = k_j + M_4.s_j$, $H_1 = h(rn_j||s_i.P_j)$, $M_6 = k_j + H_1.s_j$, and $SK = h(K_{jk}||D_{jk})$; and sends (K_j, M_5, T_2) to ES_k. ES_k receives the message; checks the validity of T_2; computes $K_{jk} = a_k.K_j$, $D_{jk} = s_k.P_j$, and $M_4 = h(K_{jk}||Req_j||D_{jk})$; checks $M_5.P \overset{?}{=} K_j + M_4.P_j$; and computes $SK = h(K_{jk}||D_{jk})$. Then, SK can be used for further communication, and EU_j and ES_k trade energy. When the energy trading finishes, EU_j transmits M_6 to ES_k encrypting it using SK. The mutual authentication in the responding phase is summarized in Figure 2.

5.6. Confirmation

For the trading confirmation, ES_k generates T_5, $x_k \in Z_q^*$, and a verification message Ver_k; computes $X_k = x_k.P$, $E_k = X_k + K_j$, $M_7 = M_6 + x_k + H_2.s_k$, $H_2 = h(s_k.P_i||rn_j||T_5)$, and $M_8 = M_6 + x_k + H_2.s_k$; and transmits $(E_k, M_7, M_8, rn_j, T_5)$ to EB_i. Ver_k includes P_k and the trading results. Then, EB_i retrieves P_j using rn_j and computes $H_1 = h(rn_j||s_i.P_j)$, $H_2 = h(s_i.P_k||rn_j||T_5)$, and $M_7.P \overset{?}{=} E_k + H_2.P_k + H_1.P_j$. If they are equal, EB_i considers that the trading is finished successfully because the signatures of both EU_j and ES_k are verified, and Ver_k is uploaded to the blockchain. Then, energy users can check the transaction records of Es_k in the later energy trading process.

ES_k		EU_j
Obtains Req_j Generates $a_k \in Z_q^*$ and T_3 Computes $A_k = a_k.P$ $A_{kj} = a_k.P_j$ $M_2 = h(A_{kj}\|\|Req_j\|\|T_3)$ $M_3 = a_k + M_2.s_k$		
	$\xrightarrow{(A_k, M_3, T_3)}$	
		Checks validity of T_3 Computes $A_{kj} = s_j.A_k$ $M_2 = h(A_{kj}\|\|Req_j\|\|T_3)$ $P_k = M_2^{-1}(M_3.P - A_k)$ Retrieves P_k from the blockchain Checks $M_3.P \overset{?}{=} A_k + M_2.P_k$ Generates $k_j \in Z_q^*$ and T_4 Computes $K_j = k_j.P$ $K_{jk} = k_j.P_k$ $D_{jk} = s_j.P_k$ $H_1 = h(rn_j\|\|s_j.P_i)$ $M_6 = k_j + H_1.s_j$ $SK = h(K_{jk}\|\|D_{jk})$
	$\xleftarrow{(K_j, M_5, T_4)}$	
Checks validity of T_4 Computes $K_{jk} = a_k.K_j$ $D_{jk} = s_k.P_j$ $M_4 = h(K_{jk}\|\|Req_j\|\|D_{jk}\|\|T4)$ Checks $M_5 \overset{?}{=} K_j.M_4.P_j$ Computes $SK = h(K_{jk}\|\|D_{jk})$		
	$\xleftrightarrow{Trade\ Energy}$	

Figure 2. Mutual authentication between ES_k and EU_j.

6. Security Analysis

We provide an informal analysis of the proposed scheme under the DY and CY model and a formal analysis using the BAN logic, RoR model, and the AVISPA simulation tool.

6.1. Informal Analysis

In this subsection, we show that the proposed scheme has resistance to various attacks. We assume that an adversary A tries security attacks based on the assumptions we described in Section 3.3.

6.1.1. Smart Card Stolen Attack

A can steal SC_j and can extract the stored values through a side-channel attack. Then, A can obtain $(X_j, Y_j, Auth_j)$. However, these values are masked using ID_j and PW_j. Therefore, A cannot know any information about EU_j and cannot generate any messages using these values. Therefore, the proposed scheme is secure even if SC_j is stolen.

6.1.2. Offline Guessing Attack

A can steal a smart card of EU_j and can try to find ID_j and PW_j. Let ID_j^A and PW_j^A be guessed values by A that are input to SC_j. Then, SC_j computes $r_j^A = X_j \oplus h(ID_j^A||PW_j^A)$, $HPW_A = h(ID_j^A||PW_j^A||r_j^A)$, and $\{s_{j,k}^A\}_{k=1}^K = Y_j \oplus HPW_j^A$. After that, SC_j checks $Auth_j \overset{?}{=} h(HPW_j^A||\{s_{j,k}^A\}_{k=1}^K)\ (mod\ l)$, and, if it is equal, SC_j generates a request message and sends it to EB_i. In this case, it can be equal even if ID_j^A and PW_j^A are not equal to ID_j and PW_j because $Auth_j$ is masked with a fuzzy verifier l_j. When the bit lengths of ID_j and PW_j are set to 128 bits, the total guessed bit length is 256 bits. Therefore, even if A successfully logs into SC_j, the probability that ID_j^A and PW_j^A are correct is $\frac{2^{10}}{2^{256}}$, which is negligible.

6.1.3. Impersonation Attack

A fails to guess ID_j and PW_j but still can try to impersonate EU_j or ES_k and send a request message. However, A cannot generate a legitimate signature Sig_j in the requesting phase or M_3 in the responding phase because A cannot obtain the secret key of EU_j or ES_k without knowing the identity and password of network participants. If the signature is not correct, the message would be considered illegitimate by the other party, and A cannot perform further communication.

6.1.4. Mutual Authentication

The mutual authentication is performed in the responding phase between ES_k and EU_j. In the first message, ES_k sends (A_k, M_3, T_1) to EU_j. Then, EU_j computes A_{kj} using a secret key, computes $P_k = M_2^{-1}(M_3.P - A_k)$, and checks $M_3.P \overset{?}{=} A_k + M_2.P_k$. Then, EU_j can authenticate ES_k. After that, EU_j sends (C_j, M_5, M_6, T_2) to ES_k. Similarly, ES_k checks $M_5.P \overset{?}{=} C_j + M_4.P_j$ and can authenticate EU_j.

6.1.5. Anonymity and Untraceability

In the proposed scheme, transmitted messages through a public channel do not include a public key or the identity of EU_j. Furthermore, A has no way to track EU_j through values obtained from transmitted messages without knowing a secret value such as a secret key or an identity. Therefore, the proposed scheme can provide anonymity and untraceability of EU_j.

6.1.6. Denial of Services (DoS) Attack

A can attempt to paralyze the network by transmitting messages indiscriminately. A can generate a request message, response message, or confirmation message. In our scheme, every message includes a timestamp and message digest value using the timestamp, and, therefore, A cannot reuse messages to paralyze the network. Furthermore, A cannot generate a legitimate message arbitrarily because the messages are masked with the secret key of the message sender. Therefore, the proposed scheme has resistance to DoS attacks.

6.1.7. Perfect Forward Secrecy

When the network is compromised or A succeeds in obtaining the long-term keys of the network, A can try to calculate the session keys of previous sessions. In the attack scenario, A can obtain s_j and s_k, which are the secret keys of EU_j and ES_k, respectively. In our scheme, the session key is $SK = h(C_{jk}||D_{jk})$. However, A can not calculate C_{jk} without knowing c_j and a_k, and these values are temporal keys used only once in each session. Therefore, the proposed scheme can guarantee perfect forward secrecy.

6.1.8. Ephemeral Session Random Number Leakage Attack

In this attack scenario, we assume that A has obtained the session random numbers c_j and a_k and try to calculate $SK = h(C_{jk}||D_{jK})$. A can obtain $C_{jk} = c_j.A_k$. However, A cannot know s_j or s_k, which are the long-term secret keys of EU_j and ES_k, respectively. Therefore, A cannot succeed in calculating SK, and the proposed scheme has resistance to ephemeral session random number leakage attacks.

6.1.9. Privileged Insider Attack

If A is a privileged insider in the network, A can obtain the message of EU_j from the registration phase and try logging into other networks impersonating EU_j. However, in the proposed scheme, EU_j only transmits ID_j and does not send a password-related value. This means that A fails to log into other networks disguising themselves as EU_j. Therefore, the proposed scheme is secure against the privileged insider attack.

6.1.10. Access Control

The proposed scheme adopted lightweight ECC-based ABE to provide access control for EU_j. Each EU_j encrypts its request message using attribute keys, and only ES_k, who has the proper attribute sets, can decrypt the message and send a response message to EU_j. Therefore, EU_j can preserve its privacy from EB_i and can present its message only to a valid ES_k.

6.2. Formal Proof Using BAN-Logic Analysis

We conduct BAN-logic analysis [28], which is a widely accepted verification method [49–51] of an authentication protocol. Then, we set goals and assumptions, describe idealized forms, and perform implementation of the BAN logic analysis. First, we demonstrate the basic rules of the BAN logic. If the above condition holds, the below condition is true. Table 2 presents the notations used in our scheme.

1. Message meaning rule (MMR):

$$\frac{\eta_1 \Big| \equiv \eta_1 \overset{K}{\leftrightarrow} \eta_2, \quad \eta_1 \lhd \{\kappa_1\}_K}{\eta_1 | \equiv \eta_2 | \sim K}$$

2. Nonce verification rule (NVR):

$$\frac{\eta_1 | \equiv \#(\kappa_1), \quad \eta_1 | \equiv \eta_2 \Big| \sim \kappa_1}{\eta_1 | \equiv \eta_2 | \equiv \kappa_1}$$

3. Jurisdiction rule (JR):

$$\frac{\eta_1 | \equiv \eta_2 | \Longrightarrow \kappa_1, \quad \eta_1 | \equiv \eta_2 | \equiv \kappa_1}{\eta_1 \Big| \equiv \kappa_1}$$

4. Belief rule (BR):

$$\frac{\eta_1 \Big| \equiv (\kappa_1, \kappa_2)}{\eta_1 \Big| \equiv \kappa_1}$$

5. Freshness rule (FR) :

$$\frac{\eta_1 \Big| \equiv \#(\kappa_1)}{\eta_1 \Big| \equiv \#(\kappa_1, \kappa_2)}$$

Table 2. Notations of BAN-logic.

Notation	Description
η_1, η_2	two principals
κ_1, κ_2	two statements
$\eta_1 | \equiv \kappa_1$	η_1 believes κ_1
$\eta_1 | \sim \kappa_1$	η_1 once said κ_1
$\eta_1 \Rightarrow \kappa_1$	η_1 controls κ_1
$\eta_1 \lhd \kappa_1$	η_1 receives κ_1
$\#\kappa_1$	κ_1 is fresh
$\{\kappa_1\}_K$	κ_1 is encrypted with K
$\eta_1 \overset{K}{\leftrightarrow} \eta_2$	η_1 and η_2 have shared key K

6.2.1. Goals

The following goals have to be achieved to prove the correctness of the proposed scheme.

Goal 1: $EU_j| \equiv ES_k \overset{SK}{\longleftrightarrow} ES_k$

Goal 2: $EU_j| \equiv ES_k| \equiv EU_j \overset{SK}{\longleftrightarrow} ES_k$

Goal 3: $ES_k| \equiv EU_j \overset{SK}{\longleftrightarrow} ES_k$

Goal 4: $ES_k| \equiv EU_j| \equiv EU_j \overset{SK}{\longleftrightarrow} ES_k$

6.2.2. Assumptions

The assumptions of our scheme are as follows.

A_1: $EU_j| \equiv \#(T_3)$

A_2: $ES_k| \equiv \#(T_4)$

A_3: $EU_j| \equiv ES_k \Rightarrow (EU_j \overset{A_{kj}}{\longleftrightarrow} ES_k)$

A_4: $ES_k| \equiv EU_j \Rightarrow (EU_j \overset{C_{jk}}{\longleftrightarrow} ES_k)$

A_5: $EU_j| \equiv (EU_j \overset{A_{kj}}{\longleftrightarrow} ES_k)$

A_6: $ES_k| \equiv (EU_j \overset{C_{jk}}{\longleftrightarrow} ES_k)$

6.2.3. Idealized Forms

The idealized forms of our scheme are as follows.

Msg_1 : $ES_k \rightarrow EU_j : \{P_k, M_2, T_3\}_{A_{kj}}$

Msg_2 : $EU_j \rightarrow ES_k : \{C_j, M_4, T_4\}_{C_{jk}}$

6.2.4. BAN Logic Implementation

We implement the BAN logic of the proposed scheme as follows. We show that the proposed scheme is correct through Steps 11 and 12.

Step 1: EU_j receives Msg_1.

$$S_1 : EU_j \triangleleft \{P_k, M_2, T_3\}_{A_{kj}}$$

Step 2: We can obtain S_2 by applying the MMR using S_1 and A_5.

$$S_2 : EU_j| \equiv ES_k| \sim (P_k, M_2, T_3)$$

Step 3: We can obtain S_3 by applying the FR using A_1 and S_2.

$$S_3 : EU_j| \equiv \#(P_k, M_2, T_3)$$

Step 4: We can obtain S_4 by applying the NVR using S_2 and S_3.

$$S_4 : EU_j| \equiv ES_k| \equiv (P_k, M_2, T_3)$$

Step 5: We can obtain S_5 by applying the BR to S_4.

$$S_5 : EU_j| \equiv ES_k| \equiv P_k$$

Step 6: ES_k receives Msg_2.

$$S_6 : ES_k \triangleleft \{C_j, M_4, T_4\}_{C_{jk}}$$

Step 7: We can obtain S_7 by applying the MMR using S_6 and A_6.

$$S_7 : ES_k| \equiv EU_j| \sim (C_j, M_4, T_4)$$

Step 8: We can obtain S_8 by applying the FR to A_2.

$$S_8 : ES_k| \equiv \#(C_j, M_4, T_4)$$

Step 9: We can obtain S_9 by applying the NVR using S_7 and S_8.

$$S_9 : ES_k| \equiv EU_j| \equiv (C_j, M_4, T_4)$$

Step 10: We can obtain S_{10} by applying the BR to S_9.

$$S_{10} : ES_k| \equiv EU_j| \equiv C_j$$

Step 11: EP_j can compute $SK = h(C_{jk}||s_j.P_k)$, and ES_k can compute $SK = h(C_{jk}||s_k.P_j)$ using the obtained values. Therefore, we obtain S_{11} and S_{12}.

$$S_{11} : EU_j| \equiv ES_k| \equiv (EU_j \overset{SK}{\longleftrightarrow} ES_k) \quad \textbf{(Goal 2)}$$

and

$$S_{12} : ES_k| \equiv EU_j| \equiv (EU_j \overset{SK}{\longleftrightarrow} ES_k) \quad \textbf{(Goal 4)}$$

Step 12: We obtain S_{13} and S_{14} by applying the JR using S_{11} and A_3, and S_{12} and A_4, respectively. Then, the BAN logic's implementation is complete.

$$S_{13} : EU_j| \equiv (EU_j \overset{SK}{\longleftrightarrow} ES_k) \quad \textbf{(Goal 1)}$$

and,

$$S_{14} : ES_k| \equiv (EU_j \overset{SK}{\longleftrightarrow} ES_k) \quad \textbf{(Goal 3)}$$

6.3. RoR Model

We perform the Real-or-Random model [30] to prove the session key security of the proposed scheme. Table 3 summarizes the queries and their descriptions of the RoR model.

Table 3. Queries and their descriptions.

Query	**Description**
$Execute(p_i, p_j)$	This query represents an eavesdropping attack carried out by A. A can obtain messages transmitted between p_i and p_j during execution of the mutual authentication protocol.
$Corrcut(p_i)$	This query represents A stealing the smart card of a legitimate user and extracting the stored value using a power analysis attack.
$Send(p, M)$	This query represents active attacks, in which A can modify eavesdropped messages, send a message M to an instance p, and can receive a response message.
$Hash$	This query represents A conducting a one-way hash operation using the eavesdropped or modified messages.
$Test(p)$	We assume that there is an unbiased coin c. When A executes the *Test* query, c is flipped, and, if the result is the tail, then a random number is given to A. If the result is the head, then the session key is given to A. A guesses whether the given value is the session key or a random number. If the probability that A answers correctly is significantly higher than $\frac{1}{2}$, the session key cannot guarantee the semantic security.

Let $Adv(A)$ be an advantage function of A in which A succeeds in distinguishing the session key and a random number. Then, we can show that the proposed scheme can guarantee the semantic security of the session key by proving the following equation:

$$Adv(A) \leq \frac{q_h^2}{|H|} + \frac{2q_s}{2^{246}} \tag{1}$$

where q_h, q_s, $|H|$ are, respectively, the number of executed *Hash* queries, the number of executed *Send* queries, and the range space of a hash output. A plays the game G_0, G_1, G_2, and G_3. The number of queries that A can execute increases as the game progresses. At the end of each game, A performs the *Test* query, and we calculate the advantage function that A passes the *Test* query.

- G_0: In G_0, we assume that A cannot perform any query. Let $P[A_{G_0}^{Succ}]$ be a probability that A succeeds in guessing correctly when $Game_0$ ends. Then, the advantage function can be defined as the following:

$$Adv(A) = |2P[A_{G_0}^{Succ}] - 1| \tag{2}$$

- G_1: A performs the *Execute* query in G_1. In the proposed scheme, A can obtain (A_k, M_3, T_3) and (K_j, M_5, T_4) from a public channel. Then, A cannot guess any information about SK because the obtained values from the public channel are not used to calculate SK. Therefore, the probability that A guesses correctly when G_1 is not changed is as follows:

$$P[A_{G_1}^{Succ}] = P[A_{G_0}^{Succ}] \tag{3}$$

- G_2: A can execute the *Send* and *Hash* queries to guess SK. A can arbitrarily generate a message or re-use it. However, each message contains a timestamp and the message digest, and A cannot generate a legitimate message. In order for A to win the game, A has the only way to find a hash collision to compromise SK, and the following equation is induced:

$$|P[A_{G_2}^{Succ}] - P[A_{G_1}^{Succ}]| \leq \frac{q_h^2}{2|H|} \tag{4}$$

- G_3: A can execute the *Corrupt* query and extracts the stored values of SC_j. In this scenario, A must guess the correct ID_j and PW_j to generate a legitimate message disguising itself as EU_j. Even if A succeeds in logging into SC_j, the probability that the guessed identity and password are correct is $\frac{2^{10}}{2^{256}} = \frac{1}{2^{246}}$. If the generated message is not correct, EB_i revokes SC_j from the network. Next, A must succeed to guess ID_j and PW_j within q_h attempts. Then, the following equation can be induced:

$$|P[A_{G_3}^{Succ}] - P[A_{G_2}^{Succ}]| \leq \frac{q_s}{2^{246}} \tag{5}$$

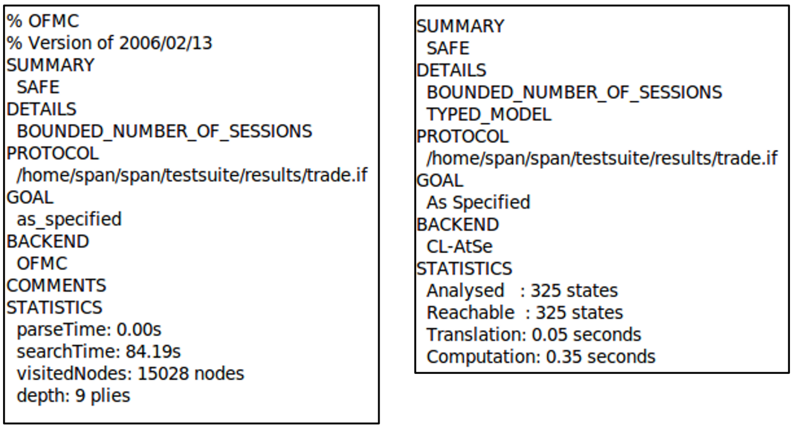
Based on the above equations, we can obtain the following equation using the triangle inequality:

$$
\begin{aligned}
\frac{1}{2}Adv(A) &= |P[A^{Succ}_{G_0}]] - \frac{1}{2}| \\
&= |P[A^{Succ}_{G_0}] - P[A^{Succ}_{G_3}]| \\
&\leq P[A^{Succ}_{G_0}] - P[A^{Succ}_{G_1}]| \\
&\quad + |P[A^{Succ}_{G_1}] - P[A^{Succ}_{G_2}]| \\
&\quad + |P[A^{Succ}_{G_2}] - P[A^{Succ}_{G_3}]| \\
&\leq \frac{q_h^2}{2|H|} + \frac{q_s}{2^{246}}
\end{aligned}
\tag{6}
$$

Finally, the proof is completed, and the advantage of A to win the game is negligible.

6.4. AVISPA Simulation

We simulated the proposed scheme using the AVISPA simulation tool [29]. The AVISPA simulation tool can verify resistance to replay attacks or Man-in-the-Middle (MITM) attacks of an authentication protocol by checking the freshness and secrecy of transmitted messages during the authentication process. We wrote the proposed method in the HLPSL language [52] and simulated it with the "On-the-Fly Model Checker (OFMC) [53]" and "Constraint Logic-based Attack Searcher (CL-AtSe)" [54] models. The execution results are shown in Figure 3, and the proposed scheme is safe under the two models. Therefore, we formally verify that our scheme has resistance to replay and MITM attacks.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/trade.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 84.19s
 visitedNodes: 15028 nodes
 depth: 9 plies
```

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/trade.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed   : 325 states
 Reachable  : 325 states
 Translation: 0.05 seconds
 Computation: 0.35 seconds
```

Figure 3. Simulation results of the proposed scheme under OFMC and CL-AtSe models.

7. Performance Analysis

We compare the proposed authentication protocol with the existing protocols suggested in smart grid environments. We show that the proposed protocol has comparable performances compared to the existing schemes in this section.

7.1. Computational Cost

We compared the computational costs generated during the mutual authentication of the proposed scheme with existing schemes [35–40]. For the comparison, we referred [55], which measured various operations used in authentication protocols. The notation of each operation and the time cost are as follows:

- T_{bp}: Execution time for a bilinear pairing operation $\cong$ 5.811;
- T_{mul}: Execution time for a point scalar multiplication operation $\cong$ 2.226 ms;
- T_{add}: Execution time for a point addition operation $\cong$ 0.0288 ms;
- T_{mtp}: Execution time for a map-to-point hash function $\cong$ 12.418 ms;
- T_{exp}: Execution time for a modular exponentiation $\cong$ 3.85 ms.

The computational cost comparison of the proposed scheme and the existing schemes are summarized in Table 4. The proposed scheme has higher costs than [35,37,38] and lower costs than [36,39,40]. Comprehensively, the proposed protocol is competitive compared to existing protocols. However, as demonstrated in Section 7.3, the proposed scheme can provide superior security to existing schemes.

Table 4. Computational cost comparison.

Scheme	Operations	Total Execution Time (ms)
Li et al. [35]	$8T_{exp} + 2T_{mul}$	35.252
Wu et al. [36]	$9T_{exp} + 2T_{mul} + T_{add}$	39.1308
Mahmood et al. [37]	$10T_{mul} + 4T_{add}$	22.3752
Abbasinezhad et al. [38]	$8T_{mul} + 4T_{add}$	17.9232
Chen et al. [39]	$2T_{bp} + 7T_{mul} + 2T_{mtp} + 2T_{add}$	52.0976
Wu et al. [40]	$2T_{bp} + 11T_{mul} + 2T_{mtp} + 2T_{add}$	61.0016
Proposed scheme	$17T_{mul} + 6T_{add}$	38.0148

7.2. Communication Cost

We compared the communication cost of the proposed scheme and the existing schemes [35–40]. We assume that M_1 and M_2 are transmitted messages, a hash output is 256 bits, a point on the elliptic curve is 320 bits, the identity is 128 bits, and the timestamp is 32 bits. In the scheme of [35], M_1 is (C_1, C_2, C_3, t_i), and M_2 is (C_4, C_5, C_6, t_j). These messages include three ECC points, three hash outputs, and two timestamps. The total communication cost is 960 + 768 + 64 = 1792 bits. In the scheme of [36], M_1 is (A, C, t_i), and M_2 is (B, D, t_j). These messages include two ECC points, two hash outputs, an identity, and two timestamps. The total communication cost is 640 + 512 + 128 + 64 = 1344 bits. In the scheme of [37], M_1 is $(X_i, Y_i, K_{ip}, ID_i, t_i)$ and M_2 is $(X_j, Y_j, K_{jp}, ID_j, t_j)$. These messages include six ECC points, two identities, and two timestamps. The total communication cost is 1920 + 256 + 64 = 2240 bits. In the scheme of [38], M_1 is (id_A, R_A, WT_A), M_2 is (id_B, R_B, V_B, WT_B), and M_3 is (id_A, V_A). These messages include two ECC points, three hash outputs, three identities, and two timestamps. The total communication cost is 960 + 768 + 384 + 64 = 2176 bits. In the scheme of [39], M_1 is $(id_i, R_{in}, R_{i1}, R_{si}, T_1)$, and M_2 is $(id_j, R_{jn}, R_{j1}, h_j)$. These messages include five ECC points, a hash output, two identities, and a timestamp. The total communication cost is 1680 + 256 + 256 + 32 = 2224 bits. In the proposed scheme, the first message is (A_k, M_3, T_1), and the second message is (C_j, M_5, M_6, T_2). These messages include two ECC points, three hash outputs, and two timestamps. Therefore, the total communication cost is 640 + 768 + 64 = 1472 bits. Table 5 shows a comparison of the communication costs. The proposed scheme has the lowest communication cost as compared to other schemes.

Table 5. Communication cost comparison.

Scheme	Total Communication Cost
Li et al. [35]	1792 bits
Wu et al. [36]	1344 bits
Mahmood et al. [37]	2240 bits
Abbasinezhad et al. [38]	2176 bits
Chen et al. [39]	2224 bits
Wu et al. [40]	2880 bits
Proposed	1472 bits

7.3. Security Features

We compare the security features of the proposed scheme with the existing schemes introduced in Section 2.2. We consider the following security features: A1—"resistance to offline guessing attack", A2—"resistance to impersonation attack", A3—"providing mutual authentication", A4—"preservation of user anonymity", A5—"preservation of user untraceability", A6—"resistance to DoS attack", A7—"preservation of perfect forward secrecy", A8—"resistance to ephemeral session random number leakage attack", and A9—"consideration of access control". The proposed scheme can provide these security features, as demonstrated in Section 6.1. However, the existing schemes [35–40] do not consider or cannot satisfy some of the features. Table 6 shows that the proposed scheme is more robust than existing schemes.

Table 6. Security features comparison.

Features	[35]	[36]	[37]	[38]	[39]	[40]	Proposed
A1	O	O	O	O	O	O	O
A2	X	O	O	O	X	O	O
A3	X	O	O	O	X	O	O
A4	O	O	X	X	X	X	O
A5	O	O	X	X	X	X	O
A6	O	O	O	O	O	O	O
A7	–	O	X	O	O	O	O
A8	O	X	X	X	O	O	O
A9	–	–	–	–	–	–	O

X: Insecure. O: Secure. –: Not considered.

8. Conclusions

In this paper, we designed a privacy-preserving mutual authentication scheme between energy traders in a blockchain-based energy trading system. We adopted lightweight ABE to provide access control of energy request messages for energy users and proposed a key agreement scheme between energy traders without the participation of an energy broker. The proposed scheme reduces the dependency on energy brokers, realizes a decentralized energy trading model, and preserves the privacy of energy users. We analyzed the proposed scheme using informal and formal methods and demonstrated that the proposed scheme has resistance to various security attacks, guarantees the correctness of authentication, and provides session key security. We compared the computational and communication costs and security features of the proposed scheme with related schemes, and we showed that our scheme has competitive performance and superior security to related schemes. Overall, the proposed scheme is better than existing schemes and can be suitable for real energy trading environments. In future work, we plan to implement the proposed scheme through experiments to verify the practicality of our scheme.

Author Contributions: Conceptualization, S.S.; software, D.K.; investigation, S.S. and K.P.; methodology, S.S. and D.K.; validation, M.K.; formal analysis, S.S. and J.O.; writing—original draft preparation, S.S.; writing—review and editing, J.O., K.P. and Y.P.; supervision, Y.P.; funding acquisition, Y.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education under grant 2020R1I1A3058605.

Data Availability Statement: Data are contained within the article.

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

References

1. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
2. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
3. Parag, Y.; Sovacool, B.K. Electricity market design for the prosumer era. *Nat. Energy* **2016**, *1*, 16032. [CrossRef]
4. Fischer, D.; Madani, H. On heat pumps in smart grids: A review. *Renew. Sustain. Energy Rev.* **2017**, *70*, 342–357. [CrossRef]
5. Hiremath, R.B.; Shikha, S.; Ravindranath, N.H. Decentralized energy planning; modeling and application—A review. *Renew. Sustain. Energy Rev.* **2007**, *11*, 729–752. [CrossRef]
6. Abdallah, A.; Shen, X. Lightweight authentication and privacy-preserving scheme for V2G connections. *IEEE Trans. Veh. Technol.* **2017**, *3*, 2615–2629. [CrossRef]

7. Saxena, N.; Choi, B.J. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. *IEEE Trans. Inf. Forensics Secur*. **2016**, *11*, 1438–1452. [CrossRef]
8. Wang, N.; Zhou, X.; Lu, X.; Guan, Z.;Wu, L.; Du, X.; Guizani, M. When energy trading meets blockchain in electrical power system: The state of the art. *Appl. Sci.* **2019**, *9*, 1561. [CrossRef]
9. Al-Saif, N.; Ahmad, R.W.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Omar, M.A. Blockchain for electric vehicles energy trading: Requirements, opportunities, and challenges. *IEEE Access* **2021**, *9*, 156947–156961. [CrossRef]
10. Aloqaily, M.; Boukerche, A.; Bouachir, O.; Khalid, F.; Jangsher, S. An energy trade framework using smart contracts: Overview and challenges. *IEEE Netw*. **2020**, *34*, 119–125. [CrossRef]
11. Kim, M.; Lee, J.; Oh, J.; Park, K.; Park, Y.; Park, K. Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers. *Appl. Energy* **2022**, *322*, 119445. [CrossRef]
12. Guo, Y.; Zhang, C.; Wang, C.; Jia, X. Towards Public Verifiable and Forward-Privacy Encrypted Search by Using Blockchain. *IEEE Trans. Dependable Secur. Comput*. **2023**, *20*, 2111–2126. [CrossRef]
13. Hu, S.S.; Cai, C.J.; Wang, Q.; Wang, C.; Luo, X.; Ren, K. Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization. In Proceedings of the IEEE Conference on Computer Communications (Infocom 2018), Honolulu, HI, USA, 16–19 April 2018. [CrossRef]
14. Cai, C.; Weng, J.; Yuan, X.; Wang, C. Enabling Reliable Keyword Search in Encrypted Decentralized Storage with Fairness. *IEEE Trans. Dependable Secur. Comput*. **2018**, *18*, 131–144.
15. Wang, M.; Guo, Y.; Zhang, C.; Wang, C.; Huang, H.; Jia, X. MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain. *IEEE Trans. Serv. Comput*. **2023**, *16*, 436–451. [CrossRef]
16. Yu, S.; Park, Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. *IEEE Internet Things J*. **2022**, *9*, 20214–20228. [CrossRef]
17. Park, K.; Lee, J.; Das, A.K.; Park, Y. BPPS:Blockchain-enabled privacy-preserving scheme for demand response management in smart grid environments. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20* , 1719–1729. [CrossRef]
18. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.M. Towards collective energy Community: Potential roles of microgrid and blockchain to go beyond P2P energy trading. *Appl. Energy* **2022**, *314*, 119003. [CrossRef]
19. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.M. P2P energy trading: Blockchain-enabled P2P energy society with multi-scale flexibility services. *Energy Rep*. **2022**, *8*, 3614–3628. [CrossRef]
20. Faisal, J.; Naeem, I.; Shabir, A.; Dohyeun, K. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. *IEEE Access* **2021**, *9*, 39193–39217.
21. Dong, J.; Song, C.; Liu, S.; Yin, H.; Zheng, H.; Li, Y. Decentralized peer-to-peer energy trading strategy in energy blockchain environment: A game-theoretic approach. *Appl. Energy* **2022**, *325*, 119852. [CrossRef]
22. Chen, Y.; Li, Y.; Chen, Q.; Wang, X.; Li, T.; Tan, C. Energy trading scheme based on consortium blockchain and game theory. *Comput. Stand. Interfaces* **2023**, *84*, 103699. [CrossRef]
23. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput*. **2016**, *15*, 840–852. [CrossRef]
24. Zhang, X.; Jiang, S.; Liu, Y.; Jiang, T.; Zhou, Y. Privacy-preserving scheme with account-mapping and noise-adding for energy trading based on consortium blockchain. *IEEE Trans. Netw. Serv. Manag*. **2021**, *19*, 569–581.
25. Tesfamicael, A.D.; Liu, V.; Mckague, M.; Caelli,W.; Foo, E. A design for a secure energy market trading system in a national wholesale electricity market. *IEEE Access* **2020**, *8*, 132424–132445. [CrossRef]
26. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October 2006; pp. 89–98. [CrossRef]
27. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112. [CrossRef]
28. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *ACM Trans. Comput. Syst*. **1990**, *8*, 18–36. [CrossRef]
29. Vigano, L. Automated security protocol analysis with the AVISPA tool. *Electron. Notes Theor. Comput. Sci*. **2006**, *155*, 61–86. [CrossRef]
30. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the 8th International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Volume 3386, pp. 65–84. [CrossRef]
31. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform*. **2017**, *14*, 3690–3700. [CrossRef]
32. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
33. Li, M.; Hu, D.; Lal, C.; Conti, M.; Zhang, Z. Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things. *IEEE Trans. Ind. Inform*. **2020**, *16*, 6564–6574. [CrossRef]
34. Guan, Z.; Lu, X.; Yang, W.; Wu, L.; Wang, N.; Zhang, Z. Achieving Efficient and Privacy-Preserving Energy Trading Based on Blockchain and ABE in Smart Grid. *J. Parallel Distrib. Comput*. **2021**, *147*, 34–45. [CrossRef]

35. Li, X.; Wu, F.; Kumari, S.; Xu, L.; Sangaiah, A.K.; Choo, K.K.R. A provably secure and anonymous message authentication scheme for smart grids. *J. Parallel Distrib. Comput.* **2019**, *132*, 242–249.
36. Wu, L.B.; Wang, J.; Zeadally, S.; He, D.B. Anonymous and efficient message authentication scheme for smart grid. *Secur. Commun. Netw.* **2019**, *2019*, 4836016. [CrossRef]
37. Mahmood, K.; Chaudhry, S.A.; Naqvi, H.; Kumari, S.; Li, X.; Sangaiah, A.K. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Gener. Comput. Syst.* **2018**, *81*, 557–565. [CrossRef]
38. Abbasinezhad-Mood, D.; Nikooghadam, M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Futur. Gener. Comput. Syst.* **2018**, *84*, 47–57. [CrossRef]
39. Chen, Y.; Martínez, J.F.; Castillejo, P.; López, L. A bilinear map pairing based authentication scheme for smart grid communications: Pauth. *IEEE Access* **2019**, *7*, 22633–22643. [CrossRef]
40. Wu, T.Y.; Lee, Y.Q.; Chen, C.M.; Tian, Y.; Al-Nabhan, N.A. An enhanced pairing-based authentication scheme for smart grid communications. *J. Ambient Intell. Human. Comput.* **2021**, 1–13. [CrossRef]
41. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
42. Dolev, D.; Yao, A.C.-C. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–207.
43. Chattaraj, D.; Bera, B.; Das, A.K.; Saha, S.; Lorenz, P.; Park, Y. Block-CLAP: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8092–8107. [CrossRef]
44. Kim, M.; Yu, S.; Lee, J.; Park, Y.; Park, Y. Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors* **2020**, *20*, 2913. [CrossRef]
45. Yu, S.; Lee, J.; Park, Y.; Park, Y.; Lee, S.; Chung, B. A secure and efficient three-factor authentication protocol in global mobility networks. *Appl. Sci.* **2020**, *10*, 3565. [CrossRef]
46. Chattaraj, D.; Bera, B.; Das, A.K.; Rodrigues, J.J.; Park, Y. Designing fine-grained access control for software-defined networks using private blockchain. *IEEE Internet Things J.* **2021**, *9*, 1542–1559.
47. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397. [CrossRef]
48. Canetti, R.; Krawczyk, H. Analysis of key-exchange protocols and their use for building secure channels. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 453–474.
49. Son, S.; Park, Y.; Park, Y. A secure, lightweight, and anonymous user authentication protocol for IoT environments. *Sustainability* **2021**, *13*, 9241. [CrossRef]
50. Ryu, J.; Oh, J.; Kwon, D.; Son, S.; Lee, J.; Park, Y.; Park, Y. secure ECC-based three-factor mutual authentication protocol for telecare medical information system. *IEEE Access* **2022**, *10*, 11511–11526.
51. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors* **2021**, *21*, 1488.
52. Von Oheimb, D. The high-level protocol specification language HLPSL developed in the EU project AVISPA. In Proceedings of the 3rd APPSEM II (Applied Semantics II) Workshop (APPSEM'05), Frauenchiemsee, Germany, 12–15 September 2005; pp. 1–17.
53. Basin, D.; Moedersheim, S.; Vigano, L. OFMC: A symbolic model checker for security protocols. *Int. J. Inf. Secur.* **2005**, *4*, 181–208.
54. Turuani, M. The CL-Atse protocol analyser. *Term Rewrit. Appl.* **2006**, 277–286.
55. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1005–1023.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.