An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities

Xueya Xia1, Sai Ji1,2, Pandi Vijayakumar3, Jian Shen1,4 and Joel J. P. C. Rodrigues5,6

Abstract
Internet of Things devices are responsible for collecting and transmitting data in smart cities, assisting smart cities to release greater potential. As Internet of Things devices are increasingly connected to smart cities, security and privacy have gradually become important issues. Recently, research works on mitigating security challenges of Internet of Things devices in smart cities mainly focused on authentication. However, in most of the existing authentication protocols, the trustworthiness evaluation of Internet of Things devices in smart cities is ignored. Considering the trustworthiness evaluation of Internet of Things devices is an important constituent of data source authentication, in this article, a cloud-aided trustworthiness evaluation mechanism is first designed to improve the credibility of the Internet of Things devices in smart cities. Furthermore, aiming at the problem that the user’s privacy is easy to leak in the process of authentication, an anonymous authentication and key agreement scheme based on non-interactive zero knowledge argument is proposed. The proposed scheme can ensure the privacy preservation and data security of Internet of Things devices in smart cities. The security analysis demonstrates that the proposed scheme is secure under q-SDH problem. The experimental simulation indicates that the performance of the proposal is greatly improved compared with other similar schemes.

Keywords
Smart cities, non-interactive zero knowledge, trustworthiness evaluation, anonymous authentication

Date received: 4 March 2021; accepted: 26 May 2021

Handling Editor: Dr Yanjiao Chen

Introduction
With the continuous increase of population in cities and the formation of new urban agglomerations, the problems caused by urbanization, such as traffic jams, environmental degradation, lack of resources, and the decline of residents’ quality of life, have become increasingly prominent. The concept of smart cities was proposed to realize the sustainable development of the cities.1 Information and communication technologies are showing an increasingly accelerating development trend in the world.2 A series of key technologies, such as 5G network, Internet of Things (IoT), cloud computing, big data analysis, new generation geographic

Corresponding authors:
Pandi Vijayakumar, Department of Computer Science and Engineering, University College of Engineering Tindivanam, Anna University Chennai, Melpakkam 604001, India.
Email: vijibond2000@gmail.com
Jian Shen, School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China.
Email: s_shenjian@126.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
information systems, are gradually carried out from the proposal of the concept to the actual application landing. These technologies give birth to many emerging urban application scenarios and innovative management modes, bringing more opportunities for the construction of smart cities.3

In the architecture of smart cities, the terminal perception layer provides the ability of intelligent perception of the physical environment and realizes the identification, data collection, monitoring, and control of the infrastructure within the scope of the city through sensing devices and sensor networks.4 With the rapid development of IoT and mobile communication technologies, smart meters, smart cameras, wearable embedded devices, smart home appliances, and other terminal devices come into family life. Although a large number of IoT terminal devices provide people with convenient life, they also provide a broader attack platform and environment for attackers.5 As shown in Figure 1, in smart cities, most of the data collected by these IoT devices is sensitive, attackers may eavesdrop or tamper with these data to obtain benefits, which may bring serious consequences. For example, smart meters collect electricity consumption data, which will expose the user’s life behavior track once leaked; wearable embedded devices collect people’s physiological data, which will endanger people’s lives once leaked or tampered in the transmission process. To ensure the security of terminal communication services in smart cities, prevent the data collected by IoT devices from being eavesdropped on or tampered in the process of transmission, and avoid the damage or major security accidents to the business applications of the smart city caused by the leakage and tampering of data content, it is necessary to authenticate the devices and encrypt the transmitted data end-to-end.6,7

**Motivations**

In smart cities, IoT devices are facing a variety of serious security threats, such as replay attack, data tampering attack, device simulation attack, man-in-the-middle attack, and privacy leakage.8 These security threats hinder the development of smart cities. Therefore, security is gradually becoming a key demand in the development of smart cities.9 Device authentication is regarded as one of the basic security services to protect the IoT system in smart cities. It verifies the identity of the IoT devices involved in the communication, so as to provide appropriate access control for these IoT devices.10,11 The key agreement provides end-to-end secure communication for smart cities and ensures the confidentiality and integrity of data in the process of data transmission.12 To mitigate the security challenges in smart cities, we will start with authentication and key agreement to design a protocol suitable for IoT devices with limited computing power.

**Main contributions**

The main contributions of this study can be summarized as follows:

1. A cloud-aided trustworthiness evaluation mechanism is designed. Trustworthiness evaluation
provides reliable authorization basis for identity authentication. However, due to the limited computing and storage resources of IoT devices, the trustworthiness evaluation cannot be completed by itself. Considering the powerful computing resources and storage capacity, cloud server is introduced to evaluate the reliability of IoT devices. The operation center will decide whether to authorize the IoT device according to the trustworthiness level value calculated by the cloud server, so as to achieve mutual trust between the IoT device and the operation center.

2. An anonymous authentication and key agreement protocol with privacy preservation is proposed. A non-interactive zero knowledge (NIZK) scheme is constructed to realize anonymous authentication and key agreement between operation center and IoT devices. As the properties of NIZK, the proposed scheme can protect the data security and privacy of IoT devices in smart cities.

3. Formal security analysis and experimental simulation are presented. Security analysis demonstrates that the proposed protocol can meet many security requirements such as anonymity, privacy preservation, mutual authentication, forward security, and unlinkability. Performance analysis shows that the proposed protocol requires much less time overhead than similar protocols, so the proposed protocol is more suitable for deployment in smart cities.

The remainder of this article is organized as follows: A detailed description of the related work is given in section “Related works.” The system model, security model, and security requirements of the proposed scheme are presented in section “System model, security model and security requirements.” The preliminaries required for the proposed scheme are described in section “Preliminaries.” “The proposed scheme” section elaborates the cloud-aided trustworthiness evaluation mechanism and anonymous authentication process. The section “Security analysis” provides provable security analysis and analysis of the security requirements for the proposed scheme. And the performance analysis of the proposed scheme is presented in the section “Performance analysis.” Finally, we give a conclusion and future work of this article in the section “Conclusion.”

Related works

In recent years, IoT devices are widely used in various fields of smart cities. Its security has also received great attention.\textsuperscript{13–17} For the secure authentication of IoT devices, scholars have done a lot of research. Now, the related work is sorted out as follows.

In 2014, aiming at security issues of implantable medical devices in wireless body area network environment, Liu et al.\textsuperscript{18} proposed an authentication scheme based on certificateless signature. The scheme is proved to be secure against the existence forgery of adaptive chosen message attack in random oracle model. However, Xiong\textsuperscript{19} pointed out that Liu et al.’s scheme could not resist the public key replacement attack and proposed an extensible certificateless remote authentication protocol with anonymity and forwarding security to solve this problem, but this scheme has the problem of member revocation. To solve this problem, in 2015, Xiong and Qin\textsuperscript{20} proposed a remote authentication scheme which was constructed by incorporating an efficient revocation certificateless encryption scheme for short-term key disclosure and a certificateless signature scheme. The security analysis shows that the scheme satisfies anonymity, key escrow resistance, and revocability. However, Shim\textsuperscript{21} pointed that the scheme was insecure against the adversary who knows a secret value. According to the secret value, the adversary can forge signatures. That is the scheme cannot resist signature forgery attack. In 2021, Wei et al.\textsuperscript{22} proposed an efficient, secure, and privacy-preserving message authentication scheme. The scheme supports IoT devices in smart cities with different encryption systems (whether RSA or ElGamal), and allows offline/online computing, making it more versatile and efficient than previous solutions.

However, the process of identity authentication may reveal users’ privacy. To protect the privacy of users, more and more scholars focus on anonymous authentication. In 2017, Dimitriou and Karame\textsuperscript{23} proposed an anonymous authentication scheme based on the blind signature and the hash chain. Blind signature technology has the characteristic that the signer is invisible to the message signed by him, so as to protect the privacy of the sender. But this scheme cannot trace malicious senders. To solve this problem, Kong et al.\textsuperscript{24} proposed an anonymous authentication scheme based on blind group signature. In this scheme, the group manager can trace the group signatures generated by the group members by using the group private key. But the scheme needs multiple interactions to ensure the security of authentication, resulting in huge computation and communication costs. Aiming at the low efficiency of authentication and resisting load modification attacks on the smart meter, Boyapally et al.\textsuperscript{25} proposed an authentication scheme based on physically unclonable functions (PUF). The scheme uses lightweight cryptographic primitives, which makes the scheme feasible in resource-constrained IoT devices. Vasco et al.\textsuperscript{26} proposed an authentication scheme based on oblivious pseudo random functions (OPRF), and further
proposed a blind anonymous identity-based encryption scheme. The scheme will not disclose to the eavesdropper whether the execution is successful, so as to hide whether the sender’s password is in the receiver’s password set. In addition, the scheme provides a provable security model to capture the security and anonymity of sender and receiver. In most authentication schemes, the evaluation of the credibility of the devices in smart cities is not considered, which makes the authentication schemes lack reliability. Besides, designing a privacy-preserving authentication protocol with low computational and communication overhead is also an urgent problem in smart cities.

**System model, security model, and security requirements**

In this section, the system model, security model, and the security requirements in the proposed scheme are presented. Table 1 lists some of the symbols used in the proposed scheme.

### System model

The system model is shown in Figure 2. First of all, before the IoT device sends registration request to the OC, it needs to collect its own trustworthiness attribute (TA) information and send it to the CS. The CS calculates its trustworthiness level (TL) and returns it to the IoT device. Second, the IoT device signs the TL and sends the report to the OC. To prevent cheating, the OC requests the TL of the device from the CS for comparison. And the authorized tag is granted to the IoT device whose TL falls within its acceptable range. Among them, the CS is semi-trusted, it may deliberately reduce the TL value of the IoT device to prevent the authentication and key agreement between legitimate IoT device and OC; the IoT device is semi-trusted, it may deliberately improve its TL value to cheat the OC; the OC is also semi-trusted, it may be curious about the privacy of data in the IoT device.

![Figure 2. System model.](image-url)

### Security model

We define the security model of the proposed anonymous authentication scheme for smart cities by a game. The game is played by an adversary $A$ (seen as a probabilistic polynomial-time (ppt) Turing machine) and a challenger $C$. Let $\Pi^x_\Omega$ denotes the instance $x$ of a participant $\Omega$, where $\Omega$ is an IoT device or OC. In this game, adversary $A$ sends a series of queries and challenger $C$ answers as follows:

- $h_i(M_i)$: In the query, adversary $A$ sends a hash query about message $M_i$, and challenger $C$ responds this query by randomly picking $R_i \in Z_p^*$ and records the tuple $(M_i, R_i)$ in the list $L_h$.
- Extract $(ID_i)$: In this query, adversary $A$ makes an extract query on identity $ID_i$ of an IoT device. Challenger $C$ answers this query with the authorized tag of that identity.
- Send $(\Pi^x_\Omega, M_i)$: In this query, adversary $A$ makes a send query on message $M_i$. Challenger $C$ executes the protocol according to message $M_i$ and returns the corresponding execution result to adversary $A$.
- Reveal $(\Pi^x_\Omega)$: If challenger $C$ has accepted, adversary $A$ can obtain a session key $K$ on $(\Pi^x_\Omega)$. Otherwise, returns ⊥ to adversary $A$.
- Corrupt $(ID_i)$: In this query, adversary $A$ makes a corrupt query on identity $ID_i$ of an IoT device. Challenger $C$ answers this query with the authorized tag of that identity.
- Test $(\Pi^x_\Omega)$: When adversary $A$ sends the query to $C$, challenger $C$ randomly picks $b \in \{0, 1\}$. If $b = 1$, challenger $C$ outputs a true session key $K$. If $b = 0$, randomly answers an element that has same bits as true session key to adversary $A$.

When the adversary $A$ performs the above queries within a limited period of time, he he makes a guess about the value $b$ and returns $b'$ as his answer. It is defined that adversary $A$ wins the game if he guesses correctly, that is $b' = b$. And it is defined that the

**Table 1. Notations in the proposed scheme.**

| Symbol | Description |
|--------|-------------|
| IoTd   | IoT device  |
| OC     | Operation center |
| CS     | Cloud server |
| TL     | Trustworthiness level |
| $\mu$, $x$, $y$ | The private key of OC, IoTd, CS |
| $U$, $X$, $Y$ | The public key of OC, IoTd, CS |
| $\vartheta$ | The set of trustworthiness attribute information |
| $\zeta_{\text{inst}}(t)$ | The instantaneous TL value for the IoT device at time $t$ |
| $\zeta(t^-)$ | The previous TL value for the IoT device |
| $l$ | The TL value of the IoT device |
| $T$ | The authorized tag for the IoT device |
| $K$ | The session key between IoT device and OC |
advantage of adversary $A$ breaking the authenticated key agreement (AKA) security of the scheme $\Sigma$ as $\text{Adv}_A^\Sigma(E_{AKA}) = |\Pr[b' = b] - \frac{1}{2}|$.

**Definition 1.** q-SDH assumption. With the public parameter $pp = (G, p, g)$ generated by $\text{Gen}(1^k)$, the q-Strong Diffie-Hellman (q-SDH) assumption holds if for all ppt $A$, we have

$$\Pr\left[\begin{array}{l}
pp \leftarrow \text{Gen}(1^k), \mu \stackrel{\$}{\leftarrow} \mathbb{Z}_p : \\
(c, g^{\mu + c}) \leftarrow A(g, g^\mu, \ldots, g^\mu^k)
\end{array}\right] \leq \text{negl}(\kappa)$$

where $c \in \mathbb{Z}_p$.

**Definition 2.** AKA secure. It is defined that the proposed solution is AKA secure if the $\text{Adv}_A^\Sigma(E_{AKA})$ is negligible.

**Security requirements**

In this scheme, the following security goals should be realized:

1. **Mutual authentication**: A malicious adversary will fake a legitimate IoTD to obtain the corresponding services. At the same time, due to the privacy of the data collected and transmitted by the IoTD, the malicious attacker will fake the legitimate OC to request private data. To ensure the security for smart cities, the proposed scheme should achieve mutual authentication.

2. **Session key agreement**: To ensure the data security in smart cities, the proposed scheme should achieve session key agreement. Session key can provide guarantee for subsequent data security communication between IoTD and other communicating parties.

3. **Privacy preservation**: The data in the IoTD have high privacy. Once the data are leaked, it will cause serious consequences. To protect the privacy of data in IoTD, the proposed scheme should achieve privacy preservation, that is, any unauthorized entities cannot get the data in plaintext, and the authorized third parties cannot disclose the user’s privacy according to the accepted data.

4. **Perfect forward security**: To protect the data security, the designed scheme need satisfy perfect forward security, that is, although the attacker obtains the current session key, he cannot recover the previous session keys.

5. **Resistance of other attacks**: What is more, the proposed protocol should be able to resist multiple attacks. Such as replay attack, man in the middle attack, forgery attack, and so on.

**Preliminaries**

In this section, a basic definition of the cryptographic primitives required for the proposed protocol is given.

**$\Sigma$-Protocol**

Let $R = \{(s, w)\}$ be a binary relation, where $s$ is a statement owned by both the prover and verifier, and $w$ is a witness that only the prover has. A three-move interaction protocol $\pi = (a, c, z)$ between a prover $P$ and a verifier $V$ is a $\Sigma$-protocol for relation $R$ if the following three properties hold:

1. **Completeness**: If $P$ inputs a statement $s$ and a witness $w$, and $s, w$ satisfy the relation $R$, then $V$ always accepts $P$.

2. **Special soundness**: Given two accepting transcripts $(a, c, z), (a', c', z')$ for any statement $s$, where $c \neq c'$, there exists a PPT algorithm $\text{Extr}$ can calculate the witness $w$ which satisfies the relation $R$.

3. **Special honest verifier zero knowledge**: On input $s$ and a challenge $c$, there exists a PPT algorithm $\text{Simu}$ can output a transcript with the same probability distribution as transcripts in the real world. Formally speaking, for every $s$ and $w$ that satisfy the relation $R$ and every $c \in \{0, 1\}^k$ it holds that

$$\{\text{Simu}(s, c)\} = \{<P(s, w), V(s, c)>\}$$

where $\text{simu}(s, c)$ denotes the simulated transcript, and $<P(s, w), V(s, c)>$ represents the real output transcript.

**NIZK arguments**

None-interactive zero-knowledge proofs (NIZKs) make a prover $P$ to prove a statement $s$ satisfies the relation of $R = \{(s, w)\}$ without interacting with the verifier $V$ in zero-knowledge. A pair of PPT algorithms $(P, V)$ for a language $L \in \text{NP}$ is a NIZK argument system if the following properties hold:

1. **Completeness**: For any statement $s \in L(|s| = \kappa)$ and the corresponding witness $w$, it has

$$\Pr\left[y \leftarrow \{0, 1\}^{|\log(\kappa)|}; \pi \leftarrow P(y, s, w) : V(y, s, \pi) = 1\right] = 1$$
2. **Soundness**: If \( s \not\in L \), then for any \( \mathcal{P} \), the following probability is negligible:

\[
\Pr\left[ y \leftarrow \{0,1\}^{\beta \log(k)}; \pi \leftarrow \mathcal{P}(y,s) : V(y,s,\pi) = 1 \right] \leq \text{negl}(k)
\]

3. **Zero-knowledge**: There is a PPT simulator \( \mathcal{S} \), such that any \( s \in L \) and the corresponding witness \( w \), the following two distributed computations are indistinguishable:

\[
\Pr[\gamma \leftarrow \{0,1\}^{\beta \log(k)}; \pi \leftarrow \mathcal{P}(\gamma,s,w) : V(\gamma,s,\pi)]
\]

\[
\Pr[(\gamma,\pi) \leftarrow \mathcal{S}(s) : (\gamma,s,\pi)] \leq \text{negl}(\kappa)
\]

A NIZK argument can be constructed by transforming a \( \Sigma \)-Protocol using Fiat–Shamir heuristic.\(^2\)

**The proposed scheme**

In this section, we will demonstrate the proposed scheme in detail from the following phases. The detailed process of anonymous authentication and key agreement is shown in Figure 3.

**Setup**

In this scheme, each IoTD maps its information to a specific and unique identity \( ID \). By executing the Setup algorithm, the public parameters as generated as follows:

1. First, on input security parameter \( \kappa \), the OC outputs a three-tuple \( (G,p,g) \), where \( G \) is a multiplicative group of prime \( p \) generated by \( g \).
2. Second, the OC randomly picks \( \mu \in \mathbb{Z}_p^* \) as its private key and calculates \( U = g^\mu \) as its public key. The IoTD randomly selects \( x \in \mathbb{Z}_p^* \) as its private key and calculates \( X = g^x \) as its public key. And the CS picks random value \( y \in \mathbb{Z}_p^* \) as its private key and calculates \( Y = g^y \) as its public key.
3. Finally, the OC chooses cryptographic hash functions \( h_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*, \ h_2 : \{0,1\}^\kappa \rightarrow \mathbb{Z}_p^* \), where \( \kappa \) is the length of session key, and publishes public parameters \( (G,p,g,U,X,Y,h_1,h_2) \).

**Trustworthiness level computation**

Pouryazdan et al.\(^3\) proposed a vote-based trustworthiness management system. The detailed process of trustworthiness level computation is presented in their scheme. This method is also used in the proposed scheme. Before IoTD sends registration to OC, it needs to ask the CS to calculate its TL value, the detailed process is given below:

1. First, the IoTD collects a set of attribute values which can reflect its reliability, and sends the set
to the CS. The set is \( \theta = \{a_1, a_2, a_3, \ldots, a_m\} \), where \( \theta \) stands for the set of trustworthiness attribute information and \( a_1, a_2, a_3, \ldots, a_m \) stands for different parameters collected by sensors about IoTD.

2. Second, when receiving the set \( \theta \), the CS computes the instantaneous TL value for the IoTD by the equation as follows

\[
\zeta_{\text{inst}}(t) = \frac{\sum_{i=1}^{m} a_i \alpha_i}{m}
\]

Because the importance of each attribute is different, we use weight \( \alpha_i \) to measure the \( i \)th set \( \theta \). Based on the instantaneous TL value, the TL value is calculated as follows

\[
\zeta(t) = \left(1 - \frac{\delta}{\theta \cdot (1 + \Delta t)}\right) \cdot \zeta_{\text{inst}}(t) + \frac{\delta}{\theta \cdot (1 + \Delta t)} \cdot \zeta(t^-)
\]

where \( \delta \) represents the proportion of TL value at time \( t^- \) in the calculation of TL value at time \( t \). \( \Delta t \) denotes time interval between \( t \) and \( t^- \). \( \theta \) denotes the annealing rate of TL values previously calculated as time changing.

1. Third, the CS encrypts the TL value \( l \) of the IoTD with public key \( X \) and sends it to the IoTD.

**Authorized tags generation**

Data storage and processing on the CS is secure, but there is a situation that the CS deliberately reduces the TL value \( l \) of an IoTD to prevent the successful registration of legitimate applicants. To prevent this, IoTDC needs to sign on the value \( l \) to prove that the assessment is acceptable. If the value \( l \) is not within its acceptable trustworthiness level range, it will be rejected. If there is no confirmation from IoTDC, the TL value assessment is invalid.

When receiving the TL value \( l \), the IoTDC picks a random number \( b \in \mathbb{Z}_p \) and signs it by the following equations if it accepts the value

\[
\begin{align*}
v_1 &= (g^b \mod p) \mod q \\
v_2 &= \left[ b^{-1}(h_1(l) + xv_1) \right] \mod q
\end{align*}
\]

Encrypted the value \( l \) by the public key of OC, then sends the ciphertext, the signature \( (v_1, v_2) \) and identity \( ID \) to the OC.

Upon receiving the data package, the OC decrypts using its private key and acquires \( l \). Then it calculates \( w = (v_2)^{-1} \mod q, u_1 = [h_1(l)w] \mod q, u_2 = v_1w \mod q \), and \( \omega = [(g^uX^v) \mod p] \mod q \). Checks whether \( \omega = v_1 \) holds. If the verification is successful, the OC will send the identity \( ID \) to the CS and ask the CS to return the TL value \( l \) of the \( ID \). If the value returned is the same as the value sent by IoTDC, and the value \( l \) shows that the IoTDC is trustworthy, the OC will compute \( k = h_1(ID) \) and generate a tag \( T = g^{xv} \) for the IoTDC, where \( l \in \mathbb{Z}_p \setminus \{-\mu\} \). To prove the validity of the tag, the OC also needs to send a NIZK proof \( \pi \leftarrow \text{NIZK} \{ \mu : T^\mu = T^{-\lambda}g \land g^\mu = U \} \) to the IoTDC. The detailed process is described below:

1. First, the OC picks a random number \( r \in \mathbb{Z}_p \), and sets \( R_1 = T^r, \ R_2 = g^r \), then computes \( c = h_2(g, U, \lambda, T, R_1, R_2) \) and \( z = r + c \mu \mod p \). After that, the OC outputs a proof \( \pi = (c, z) \) and sends \( (T, \pi) \) to the IoTDC through secure channel.

2. Second, when the IoTDC receives \( (T, \pi) \) from OC, it computes \( \lambda = h_1(ID) \) and computes the following equations to verify the proof

\[
\begin{align*}
R'_1 &= T^z + \alpha g^{-c} \\
R'_2 &= g^z U^{-c} \\
c' &= h_2(g, U, \lambda, T, R'_1, R'_2)
\end{align*}
\]

Checks whether \( c' = c \) holds. If this equation holds, the tag will be stored in IoTDC for subsequent authentication.

**Session key agreement**

This phase can be divided into the following steps:

Step 1: The OC randomly selects a number \( m \in \mathbb{Z}_p^* \) and computes \( M = g^m \). Then the OC signs message \( M \) with private key \( \mu \) and generates a signature \( \sigma_1 \). It sends \( (M, \sigma_1) \) to the IoTDC.

Step 2: When the IoTDC receives \( (M, \sigma_1) \) from OC, it verifies the validity of the signature \( \sigma_1 \) by OC’s public key \( U \). If it passes, the IoTDC randomly selects a number \( n \in \mathbb{Z}_p^* \) and computes \( N = g^n \). The IoTDC needs to send message \( N \) to the OC. To show its legal identity and maintain its anonymity, the IoTDC produces a proof \( \sigma_2 \). In particular, the IoTDC chooses a random number \( a \in \mathbb{Z}_p^* \) and computes \( A = T^a \). After that, the IoTDC selects random number \( r_1, r_2 \in \mathbb{Z}_p \) and calculates the following equations to generate a proof \( \sigma_2 \)

\[
\begin{align*}
\Phi &= A^{-r_1} g^{r_2} \\
k &= h_2(g, A, \Phi, N, r) \\
s_1 &= r_1 + k \lambda \mod p \\
s_2 &= r_2 + ka \mod p
\end{align*}
\]
The IoTDF generates proof $\sigma_2 = (k, s_1, s_2)$ and calculates the session key $K = h_2(M, \sigma_1, N, \sigma_2, M^o)$. Finally, the IoTDF sends $(A, N, \sigma_2, t)$ to the OC.

Step 3: When the OC receives $(A, N, \sigma_2, t)$ from the IoTDF, it first checks the freshness of the timestamp $t$. If the timestamp has already been used, which means that an adversary launched a replay attack during the data transmission, the packet is ignored. Otherwise, the OC parses $\sigma_2$ into $(k, s_1, s_2)$ and calculates the following equations to verify the validity of the proof

\[
\Gamma = A^k \\
\Phi' = A^{-k} \Gamma^{-k} g_j^{k'} \\
k' = h_2(g, A, \Phi', N, t)
\]

If $k = k'$ does not hold, it means message $N$ is modified by an adversary in the course of data transmission or the IoTDF is not an authorized legal entity, the OC will ignore the packet. Otherwise, it means message $N$ is coming from a legitimate entity. Then the OC can successfully share the session key $K = h_2(M, \sigma_1, N, \sigma_2, M^w)$ with the IoTDF.

**Security analysis**

**Provable security**

Through the above security model, a formal security analysis is given in this subsection as follows:

**Theorem 1.** If the $q$-SDH assumption holds in $\mathbb{G}$, then no ppt adversary $A$ against the proposed authentication scheme can forge an authorized tag to pass the OC’s verification with non-negligible probability.

**Proof.** If there exists an adversary $A$ can forge an authorized tag that successfully passes the verification by the OC with non-negligible probability $\varepsilon$, then we can prove that there exists a challenger $C$ can solve the $q$-SDH problem with non-negligible probability.

Given a $q$-SDH instance $(g, g_1, \ldots, g_n) \in (\mathbb{G}^*)^q + 1$ for some unknown $\mu \in \mathbb{Z}_p^*$, $C$ aims to output $(c, g_{\mu+c})$ for some $c \in \mathbb{Z}_p \setminus \{-\mu\}$. $C$ chooses a string $ID'$ as the target IoTDF’s identity. Then $C$ randomly picks $\lambda_1, \lambda_2, \ldots, \lambda_{q-1} \in \mathbb{Z}_p$. Let

\[
f(x) = \prod_{j=0}^{q-1}(x + \lambda_j) = \sum_{j=0}^{q-1} g_j x^j \\
 f'(x) = \frac{f(x)}{(x + \lambda_j)} = \prod_{j=0}^{q-1}(x + \lambda_j) = \sum_{j=0}^{q-2} b_j x^j
\]

Using the tuple and technique of Boneh-Boyen, $C$ can compute

\[
g' = \prod_{j=0}^{q-1} (g_j^{a_j}) = g'^{(\mu)} \\
U = \prod_{j=1}^{q} (g_j^{a_j-1}) = g'^{(\mu)} = (g'^r)\mu \\
T_i = \prod_{j=0}^{q-2} g_j^{b_j} = g^{(\mu)} = (g'^{\frac{1}{(q+1)^2}}) = g'^{\frac{1}{(q+1)^2}}
\]

Finally, $C$ maintains list $L_{Ex} = \{\{\lambda, T_i\}\}^{q-1}$ as authorized tags and responses tuples $(G, p, g, U)$ to $A$. $C$ answers $A$’s queries as follows:

$h_i(M_j)$-Query: Challenger $C$ maintains a list $L_{h_i} = \{M_j, R_j\}$, where $j = 1, 2$. When $A$ sends a hash query, $C$ checks if $(M_j, R_j)$ has exists in $L_{h_i}$. If it exists, returns the tuple. Otherwise, $C$ randomly picks $R_j \in \mathbb{Z}_p$, records the tuple $(M_j, R_j)$ in the list $L_{h_i}$ and returns $R_j$ to $A$.

Extract $(ID_0)$-Query: If $ID_0 = ID^*$, $C$ outputs $\perp$ to $A$. Otherwise, returns $(\lambda_i, T_i)$ according list $L_{Ex}$.

Send $(ID_j, M_j)$-Query: Challenger $C$ checks if $ID_j = ID^*$ first. If so, $C$ aborts the game. Otherwise, $C$ answers this query according the following results:

- When $A$ makes a query on $(\Pi_3^0, \text{start})$, $C$ randomly picks number $a, n$, computes $N = g^a$ and $A = T^\alpha$. And picks two random number $r_1, r_2 \in \mathbb{Z}_p$, computes $\Phi = A^{-\alpha} g^{r_2}$, $k = h_2(g, A, \Phi, N, t)$, $s_1 = r_1 + k \lambda$ mod $p$, $s_2 = r_2 + ka$ mod $p$ since $C$ knows authorized tag $(\lambda, T)$. Then $C$ sends $(A, N, \sigma = (s_1, s_2, t))$ to $A$.

- When $A$ makes a query on $(\Pi_3^0, \text{auth})$, $C$ first verifies the freshness of time $t$, and checks the correctness of $\sigma$ according to the message generated by $(\Pi_3^0, \text{start})$. If $\text{auth}$ is not valid then $C$ aborts it. Otherwise, $C$ answers $A$ according to the execution of scheme as $C$ knows authorized tags of these IoTDFs.

Reveal $(\Pi_3^0)$-Query: $C$ outputs $\perp$ if $\Pi_3^0$ is not accepted. Otherwise, returns the session key according list $L_{Ex}$.

Corrupt $(ID_0)$-Query: $C$ searches list $L_{Ex} = \{\{\lambda, T_i\}\}^{q-1}$ and then outputs corresponding result to $A$.

Test $(\Pi_3^0)$-Query: $C$ chooses random element that has the same bit length as the true session key and sends to $A$.

Finally, $A$ outputs a forgery $(\lambda^*, T^*)$, $C$ sets $(\lambda, T) = (\lambda^*, T^*)$. If $(\lambda, T)$ is a successful forgery, that is, $(\lambda, T) \notin \{\{\lambda, T_i\}\}^{q-1}$ and $A^{\mu + \lambda} = g'$. Let $f(x) = f'(x)(x + \lambda) + \theta$ for some $\theta \in \mathbb{Z}_p^*$, and write $f'(x) = \sum_{j=0}^{q-2} b_j x^j$.

\[T = (g'^r)^{\frac{1}{(q+1)^2}} = g'^{\frac{r(\lambda + \theta)}{q+1}} = g'^{(\mu)} = (g'^{\frac{1}{(q+1)^2}})^{\frac{r}{q+1}} + \theta \frac{r}{q+1} \]

If $\lambda$ can solve the $q$-SDH problem. Let $E_1$ denotes the event that $C$ aborts the send-Query, $E_2$ denotes the event that $A$ forgives an authorized tag. Then the advantage that challenger $C$ solves the $q$-SDH problem is

\[\Pr[E_1 \land E_2] = \Pr[E_1] \Pr[E_2|E_1] = \varepsilon \left( \frac{1}{q^2} \right)^q = \frac{1}{(q+1)^2} \]
As the advantage that $C$ solves the q-SDH problem is non-negligible, which conflicts with the reality. Thus, the proposed scheme is AKA secure.

**Analysis of the security requirements**

In this subsection, we will show that proposed protocol meets all the security requirements mentioned above. The security analysis is shown as follows.

*Mutual authentication*. When the IoTTD sends a registration request to the OC, the OC will assign authorized tag for it who has high trustworthiness level value. And the OC generates a proof $\pi = (c, z)$ to prove that the tag comes from a legal entity. The IoTTD authenticates the validity of the tag from OC by $R_1^t = T^z + \alpha g^c$, $R_2^t = g^{Uz} c$, and $c' = h_3(g, U, \lambda, T, R_1^t, R_2^t)$. Besides, before to send message $N$, each IoTTD uses its authorized tag to produce a proof for that message. Upon receiving a message report, the OC verifies that the message $N$ is from a legitimate IoTTD by $\Gamma = A^t$, $\Phi = A^{-1} \Gamma^{t^k} g^b$, and $k' = h_2(g, A, \Phi, N, t)$. The soundness of NIZK makes sure that only who has an authorized tag can be accepted by the OC. Thus in this phase, the OC can authenticate the IoTTD. The mutual authentication can be guaranteed in the proposed scheme. What is more, the message report $(N, t)$ is hashed by $k = H_2(g, A, \Phi, N, t)$, if a malicious adversary $A$ modifies the IoTTD’s message report, the OC will discover it and refuse the message report. Therefore, the authentication and data integrity are both assured in the proposed scheme.

*Session key agreement*. As $K = h_2(M, \sigma_1, N, \sigma_2, M^n)$ and $K = h_2(M, \sigma_1, N, \sigma_2, N^m)$, the IoTTD and OC can calculate a session key with same value. Then they can use the session key for secure communication. Besides, the proposed scheme has been proved AKA secure under q-SDH problem. Therefore, the proposed scheme support secure session key agreement.

*Privacy-preserving*. Only entities with session keys $K = h_2(M, \sigma_1, N, \sigma_2, N^m)$ can decrypt the data report from IoTTD, which makes any unauthorized entities can’t get the data in plaintext. What is more, the zero knowledge of NIZK makes sure that the OC cannot link the accepted message $N$ to a specific IoTTD. As the authorized tag $T_i$ is randomized by a random number in the way of $A_i = T_i^n$, the randomized tag $A_i$ belongs to an IoTTD takes different ways when performing a new round of key agreement, leading to the privacy protection of IoTTD and the resistance to dictionary attacks. Although the session key is leaked, the malicious adversary $A$ acquires data report in the form of plaintext. As we have randomize the tag by a dynamic random number, and the zero knowledge property also ensures that no one can retrieve useful information about IoTTD’s identity from the tag, so the adversary $A$ cannot link this report to a specific IoTTD. Therefore, the privacy preservation can be guaranteed in this scheme.

**Perfect forward security**. If the adversary intercepts the report $(M, \sigma_1)$ and $(A, N, \sigma_2 = (k, s_1, s_2, t))$ transmitted between the IoTTD and OC during authentication phase, he cannot compute a session key because he cannot solve DL problem. Furthermore, even the current session key is leaked, it will not affect the security of the previous session communication, then this protocol provides forward security. Since the current session key is calculated as $K = h_2(M, \sigma_1, N, \sigma_2, N^m)$. Even if the current session key is compromised by an adversary, as the random number $m$ is dynamically updated with every session, it will not impact the secrecy of past session keys. Thus, the proposed scheme satisfies forward security.

**Resistance of other attacks.** As this protocol injects a timestamp $t$ during message transmission, any malicious behavior that wants to launch a replay attack will be detected. As mutual authentication is guaranteed in the key agreement process, the proposed protocol can resist man-in-the-middle attacks. Besides, we have proved that no ppt adversary can forge a valid tag to pass the OC’s verification under q-SDH problem, so the proposed authentication scheme can be resistance of forgery attack.

**Performance analysis**

In this section, first, a comparison about features of the proposed scheme with those of other schemes is given. Second, the communication overhead of the proposed scheme is analyzed. Finally, the computational cost is discussed and the time cost of authorized tag generation and session key exchange is described.

**Features comparison**

In this subsection, the comparison between the proposed scheme, revocable and scalable certificateless remote authentication (RSCR)\(^{20}\), threshold-based anonymous identification (TAI)\(^{32}\), and conditionally anonymous ring signature (CRS)\(^{33}\) is given. As displayed in Table 2, only the proposed scheme can satisfy all of these features. By generating NIZK proofs, the proposed scheme satisfies the mutual authentication and privacy-preserving. As the hash function is collision resistant, the data integrity is guaranteed in the proposed scheme. As the q-SDH assumption holds in $G$, the proposed scheme can resist forgery attack. Also,
because it satisfies the mutual authentication, it can resist man-in-middle attacks, so the proposed scheme supports secure session key agreement. The detailed explanation is presented in section “Security analysis.” Besides, because the proposed scheme is relatively small in communication and computational overhead compared with other similar schemes, so the proposed scheme achieves scalability.

Communication overhead
To show the superiority of the proposed scheme, other similar schemes are compared with the scheme. It is assumed that the number of IoTDs is \( n \). First, the communication cost of the authorized tags that are distributed to the IoTD is analyzed. The tag issued by the OC is in the shape of \( T \parallel c \parallel z \) and its size is \( |G| + 2|Z_p^*| \), in which \( |G| \) represents the length of element in \( G \), \( |Z_p^*| \) represents the length of element in \( Z_p^* \). Besides, the communication cost of message report for key agreement that is generated by the IoTD and sent to the OC is discussed. The message report for the IoTD is in the shape of \( A \parallel k \parallel s_1 \parallel s_2 \parallel N \parallel r \) and its size is \( 2|G| + 3|Z_p^*| + |r| \), where \( |r| \) represents the length of timestamp. We compare the proposed scheme with other similar schemes TAI and CRS in terms of the communication cost from the IoTD to the OC. The result is shown in Figure 4. Because in CRS, each device needs the public keys of all other peer devices to participate to achieve its anonymity, so its overhead increases as the number of devices increases. In addition, because the proposed protocol only needs a shorter proof to complete identity authentication when generating zero-knowledge proofs, the proposed protocol has less communication overhead compared to similar scheme TAI that uses zero-knowledge to complete anonymous authentication.

Computational complexity
In this subsection, we denote \( H \) as hash operation, \( P \) as weil pairing operation, \( E \) as modular exponentiation operation and \( M \) as modular multiplication operation.

Then the computational complexity of authorized tag generation at the OC side is \( 2H + 3E + M \), the tag authentication at the device side is \( 2H + 4E + 3M \), the zero knowledge proof generation at the IoTD side is \( H + 3E + 3M \), and the proof authentication at the OC side is \( H + 4E + M \). The proposed scheme and the compared schemes are simulated on pairing-based cryptography (PBC) library to compare their performance. Execution time demonstrates the complexity of the proposal, which can be evaluated by time cost of the tag authentication and zero knowledge proof generation at the IoTD side, authorized tag generation and proof authentication at the OC side. First, we compare the time cost of the two phases at the OC. It can be seen from Figures 5 and 6 that the time of tag generation and proof authentication at the OC.

Table 2. Features comparison.

| Schemes          | The proposed scheme | RSCR | TAI | CRS |
|------------------|---------------------|------|-----|-----|
| Mutual authentication | ✓       | ✗     | ✓   | ✗   |
| Session key agreement | ✓       | ✗     | ✗   | ✗   |
| Privacy-preserving | ✓       | ✓     | ✓   | ✓   |
| Unforgeability    | ✓       | ✗     | ✓   | ✗   |
| Data integrity    | ✓       | ✓     | ✗   | ✓   |
| Scalability       | ✓       | ✓     | ✓   | ✗   |

Figure 4. IoTD to OC communication cost.

Figure 5. Time cost of OC for tag generation.

Table 2.
Authentication in these proposals increase linearly with the number of IoTDs, but the time cost on these two phases in the proposed scheme is much less than the time required for the TAI and CRS. This is because, the schemes TAI and CRS require more expensive operations than the proposed scheme, such as pairing operations. Then, we compare the time cost of the tag authentication and zero knowledge proof generation at the IoTD side with other similar schemes. The computational complexity of tag authentication phase in TAI is $2P + 2M$, in CRS is $2P + E + nM$. And The computational complexity of zero knowledge proof generation phase in TAI is $2H + P + 3E + 8M$, in CRS is $(4n - 1)E$. From Figures 7 and 8, we can see that with the number of IoTDs increases, the time cost of tag authentication and zero knowledge proof generation in the proposed scheme and in TAI both keep constant, but the the proposed scheme has better performance than the TAI. The time cost of these two phases in CRS increases linearly with the number of IoTDs, that is, because the IoTD needs to use other peer devices’ public keys to generate its signature.

Therefore, from the perspective of practicability, the proposed scheme is more applicable to smart cities.

**Conclusion**

In this article, we first propose a cloud-aided trustworthiness evaluation mechanism. According to the trustworthiness evaluation calculated by CS, the OC decide whether to authorize tag to IoTD, hence mutual trust between IoTD and OC is guaranteed in the proposed scheme. In addition, an efficient anonymous authentication and key agreement scheme based on non-interactive zero knowledge is proposed. Based on this scheme, the OC can authenticate the validity of IoTD without revealing its identity, hence privacy preservation of IoTD is guaranteed in the proposed scheme. And the session key prevents attackers acquiring data in plaintext, hence data security of IoTD is guaranteed in the proposed scheme. Security analysis indicates that the proposal can satisfy many security properties, such as anonymity, privacy preservation, mutual authentication, forward security, and unlinkability. The result of performance evaluation demonstrates that the proposal is more suitable for deployment in smart cities.

However, how to seek a balance between privacy protection and regulation is a problem worthy of discussion in the data security protection of the smart city. In the future, we will study how to design a revocation mechanism which can revoke malicious entities while keeping the anonymity of legitimate entities in smart cities.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.
**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is supported by the National Natural Science Foundation of China under Grant Nos U1836115, 61672295, 61922045, 61672290, and 61877034; the National Science Foundation of Jiangsu Province under Grant No. BK20181408; the Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing University of Posts and Telecommunications under Grant No. DSIIP1901; the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004; the CICAEET fund; and the PAPD fund. Besides, this work is also supported by FCT/MCTES through national funds and when applicable co-funded EU funds under the Project UIDB/50008/2020; and by the Brazilian National Council for Scientific and Technological Development—CNPq, via Grant No. 313036/2020-9.

**ORCID iDs**

Xueya Xia [https://orcid.org/0000-0002-1194-9444](https://orcid.org/0000-0002-1194-9444)
Pandi Vijayakumar [https://orcid.org/0000-0001-5451-8946](https://orcid.org/0000-0001-5451-8946)

**References**

1. Shen M, Tang X, Zhu L, et al. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J* 2019; 6(5): 7702–7712.
2. Xie J, Tang H, Huang T, et al. A survey of blockchain technology applied to smart cities: research issues and challenges. *IEEE Commun Surv Tut* 2019; 21(3): 2794–2830.
3. Hammi B, Khatoun R, Zeadally S, et al. IoT technologies for smart cities. *IET Netw* 2018; 7(1): 1–13.
4. Alavi AH, Jiao P, Buttler WG, et al. Internet of things-enabled smart cities: state-of-the-art and future trends. *Measurement* 2018; 129: 589–606.
5. Hui TKL, Sherratt RS and Sánchez DD. Major requirements for building smart homes in smart cities based on internet of things technologies. *CST* 2017; 76: 358–369.
6. Vijayakumar P, Azees M, Chang V, et al. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *Cluster Comput* 2017; 20(3): 2439–2450.
7. Lee CC, Hwang MS and Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans Ind Electron* 2006; 53(5): 1683–1687.
8. Ning H, Liu H and Yang LT. Aggregated-proof based hierarchical authentication scheme for the internet of things. *IEEE Trans Parall Distrib Syst* 2015; 26(3): 657–667.
9. Gharaibeh A, Salahuddin MA, Hussini SJ, et al. Smart cities: a survey on data management, security, and enabling technologies. *IEEE Commun Surv Tut* 2017; 19(4): 2456–2501.
10. Vijayakumar P, Azees M, Kannan A, et al. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Trans Intell Transp Syst* 2016; 17(4): 1015–1028.
11. Chen CT and Lee CC. A two-factor authentication scheme with anonymity for multi-server environments. *Secur Commun Netw* 2015; 8: 1608–1625.
12. Mir O, Weide TVD and Lee CC. A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems. *J Med Syst* 2015; 39(9): 89.
13. Wei F, Zeadally S, Vijayakumar P, et al. An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles. *IEEE Trans Intell Transp Syst*. Epub ahead of print 7 July 2020. DOI: 10.1109/TITS.2020.2998775.
14. Gope P, Gheraibia Y, Kabir S, et al. A secure IoT-based modern healthcare system with fault-tolerant decision making process. *IEEE J Biomed Health Inform* 2021; 25(3): 862–873.
15. Azees M, Vijayakumar P and Deboarh LJ. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans Intell Transp Syst* 2017; 18(9): 2467–2476.
16. Manickam P, Shankar K, Perumal E, et al. Secure data transmission through reliable vehicles in vanet using optimal lightweight cryptography. In: Hassaniene A and Elhosny M (eds) *Cybersecurity and secure information systems*. Cham: Springer, 2019, pp.193–204.
17. Vijayakumar P, Chang V, Deborah LJ, et al. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Fat Gener Comput Syst* 2018; 78: 943–955.
18. Liu J, Zhang Z, Chen X, et al. Certificateless remote anonymous authentication schemes for wireless body area networks. *IEEE Trans Parall Distrib Syst* 2014; 25(2): 332–342.
19. Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. *IEEE Trans Inform Foren Sec* 2014; 9(12): 2327–2339.
20. Xiong H and Qin Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Trans Inform Foren Sec* 2015; 10(7): 1442–1455.
21. Shim KA. Comments on “revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks.” *IEEE Trans Inform Foren Sec* 2018; 15: 81–82.
22. Wei J, Phuong TVX and Yang G. An efficient privacy preserving message authentication scheme for internet-of-things. *IEEE Trans Ind Inform* 2021; 17(1): 617–626.
23. Dimitriou T and Karame GO. Enabling anonymous authorization and rewarding in the smart grid. *IEEE Trans Depend Secure Comput* 2017; 14(5): 565–572.
24. Kong W, Shen J, Vijayakumar P, et al. A practical group blind signature scheme for privacy protection in smart grid. *J Parall Distrib Comput* 2020; 136: 29–39.
25. Boyapally H, Mathew P, Patranabis S, et al. Safe is the new smart: PUF-based authentication for load modification-resistant smart meters. *IEEE Trans Depend Secure Comput*. Epub ahead of print 6 May 2020. DOI: 10.1109/TDSCE.2020.2992801.
26. Vasco MIG, Pozo ALPD and Soriente C. A key for John Doe: modeling and designing anonymous password-authenticated key exchange protocols. *IEEE Trans Depend Secure Comput* 2021; 18: 1336–1353.

27. Boneh D and Boyen X Short signatures without random oracles. In: *Proceedings of the EUROCRYPT 2004*, Interlaken, 2–6 May 2004, pp.56–73. Berlin: Springer.

28. Zhao Y, Deng RH, Zang B, et al. Practical zero-knowledge arguments from protocols. In: *Proceedings of the international workshop on internet and network economics*, Hong Kong, China, 15–17 December 2005, pp.288–298. Berlin: Springer.

29. Fiat A and Shamir A. How to prove yourself: practical solutions to identification and signature problems. In: *Proceedings of the conference on the theory and application of cryptographic techniques*, Santa Barbara, CA, 11–15 August 1986, pp.186–194. Berlin: Springer.

30. Pouryazdan M, Kantarci B, Soyata T, et al. Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing. *IEEE Access* 2016; 4: 529–541.

31. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput* 1997; 26(5): 1484–1509.

32. Sui Z, Niedermeier M and de Meer H. TAI: a threshold-based anonymous identification scheme for demand-response in smart grids. *IEEE Trans Smart Grid* 2016; 9(4): 3496–3506.

33. Zeng S, Jiang S and Qin Z. An efficient conditionally anonymous ring signature in the random oracle model. *Theor Comput Sci* 2012; 461: 106–114.