ICEB 2018 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-6-2018

A Heterogeneous Systems Public Key Encryption with Equality Test in Smart City

Rashad Elhabob
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, rashaduestc@gmail.com

Iva Sella
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, ivanasea@gmail.com

Yanan Zhao
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, zynbyxz@gmail.com

Guobin Zhu
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, zhugb@uestc.edu.cn

Hu Xiong
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, xionghu.uestc@gmail.com

Recommended Citation

Elhabob, Rashad; Sella, Iva; Zhao, Yanan; Zhu, Guobin; and Xiong, Hu, "A Heterogeneous Systems Public Key Encryption with Equality Test in Smart City" (2018). *ICEB 2018 Proceedings*. 98.
https://aisel.aisnet.org/iceb2018/98

Elhabob, R., Sella, I., Zhao, Y., Zhu, G. & Xiong, H. (2018). A heterogeneous systems public key encryption with equality test in smart city. In *Proceeding of The 18th International Conference on Electronic Business* (pp. 44-52). ICEB: Guilin, China, December 2-6, 2018

A Heterogeneous Systems Public Key Encryption with Equality Test in Smart City

Rashad Elhabob, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, rashaduestc@gmail.com
Iva Sella, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, ivanasea@gmail.com
Yanan Zhao, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, zynbyxz@gmail.com
Guobin Zhu, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, zhugb@uestc.edu.cn
Hu Xiong*, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, xionghu.uestc@gmail.com

ABSTRACT

Smart cities have been identified as areas which are urbanized and utilize diverse types of electronic data collection sensors that are used to oversee resources and assets efficiently. Smart meters are a unit of smart cities and they collect information about users and their consumption patterns. Consequently, the Internet of Things (IoT) being at a steady evolution has prompted multiple users into having their data collected from smart meters, stored on cloud servers. This is a way of saving costs and time involved in accessing the data. In spite of that, the cloud-assisted IoT faces privacy and security issues. This is as a result of the cloud servers possessing an untrusted nature. Due to this, it is essential for the data accumulated from the smart meters be encrypted hitherto outsourcing it to the cloud server. However, having encrypted data in the cloud server leads to a complication when it comes to accessing the data. For users who are on a different public key system, it becomes illogical for the users to first download the entire data on the cloud in order to access the required data. Therefore to resolve this issue, a heterogeneous systems public key encryption with equality test (HS-PKE-ET) scheme was proposed. The HS-PKE-ET scheme integrates certificateless public cryptography with equality test (CLC-ET) with the public key encryption with equality test (PKI-ET). This scheme allows an authorized cloud server to determine if two encryptions encrypted within heterogeneous systems possess equivalent messages. Basing on the random oracle model, the proposed scheme's security is stated under the bilinear Diffie-Hellman assumption together with the computational Diffie-Hellman assumption. Ultimately the size of storage, computation complexities and properties with other related works are focused on and illustrations indicate our proposed scheme reflects a good performance.

Keywords: Smart grid, cloud, heterogeneous systems equality test.

INTRODUCTION

Based on the challenging new network possibilities, and on steerage competitiveness profits and network improvement e orts, the concept of "smart" cities has seemed. (Batamuliza, 2018.) states that a lot of effort has been put in smart cities to understand and engage in a world that is increasingly connected. This clearly means growth in urban environments in terms of education, healthcare, transportation, etc. Consequently the concept of "smartness" has been embraced in all the aforementioned areas in order to fulfill the demands that have emerged as a result of their growth. Based on the facts given by the communication technologies, the growth of these utilities will result to better, efficient ways of living for their users. The growth of IoT however can be considered to be a booster for the growth of these utilities. And as a result growth of data generated from these utilities is experienced such as data from smart watches, smart healthcare, smart vehicles and so forth. This data therefore requires processing and storage and hence the cloud servers are responsible for these functionalities. They however require a great extent of network resources which culminates to the security and privacy of this data is being compromised. This is because the cloud servers have been rendered insecure putting the security and privacy of users into the limelight. A case in point is where body sensors collect the health status of a user during a workout and upload to the cloud. This information is considered personal and needs to be kept safe. And because of that, users have taken to protect the privacy of their data before storing it to the cloud servers. The continuous growth of such smart devices means a rise in demands for power usage for these devices (Jokar, Arianpoo, & Leung, 2016). And considering that the current power networks cannot fully bare the demands, smart grid has been considered a new solution to this challenge. Smart grid aims at ensuring reliable digital responses to the quickly changing electricity demands and concurrently focusing on providing efficient and reliable power systems. The fact that the smart grid has been put into implementation, just like

*Corresponding author

any other technologies, it experiences security and privacy difficulties (Li, Lu, Wang, & Choo, 2016). Devices located from homes, businesses, vehicles to personal gadgets collect information about their users and usage patterns and thereafter upload them to the cloud. As earlier mentioned the information from these devices is confidential and needs to be secured and to ensure this, the data is therefore encrypted before it's uploaded to the cloud servers. And because of this, public-key encryption has proved to be an efficient way to ensure that there is confidentiality. This is achieved by the smart devices using the public key of receivers within the network to encrypt the users' sensitive data before uploading to the cloud server. With this, the data that is uploaded to the cloud is secured. Therefore in cases where an authorized user wants to access this data the user is required to download the data and then use his/her own private key to decrypt the data in order to access it. However this is quite a tiresome and time-consuming process in situations where the data is in huge amounts. With this in consideration, to ensure that a user's information is not disclosed whenever their data is searched; search functionality is supported in the ciphertexts that are stored in the cloud server. This allows for the searchability, with no information related to the ciphertexts being exposed. This idea was first proposed by Boneh *et al.* (2004), where the keyword search function was incorporated into Public Key Cryptography and is known as PKE-KS. However, PKE-KS being able to support search functionality still experiences a drawback where the search function only works for ciphertexts encrypted under the same public key.

To deal with this drawback, Yang *et al.* (2010) presented a scheme known as Public Key Encryption with Equality Test(PKE-ET) where an equality test can not only be performed on ciphertexts encrypted under the same public key but also under different public keys. Consequently a lot of work has been put into improving the equality test scheme such as (Tang, 2011; Ma, Zhang, Huang, & Yang, 2014; Huang et al., 2015; Lee, Ling, Seo, & Wang, 2016a; Ma, Huang, Zhang, & Yang, 2015; Xu et al., 2017).

As a matter of fact, all the above-mentioned schemes have their construction based on the traditional Public Key Infrastructure (PKI). A further look into these schemes by (Ma, 2016) resulted in the idea of PKE-ET being incorporated with Identity-based public key cryptosystem. This brought forth identity-based encryption with outsourced equality test (IBE-ET) that was built on the basis of IBC. The breakthrough in this scheme was that it managed to take a user's identity as their public key hence eliminate certificates found within the PKI. However, the scheme still experiences difficulties as a result of key escrow. Key escrow happens when decryption keys are put in the care of third parties. Here the third parties have access to a user's encrypted data and can access it any time.

Al-Riyami *et al.* (2003) however found a way to deal with the key escrow. He proposed a certificateless public key cryptosystem (CL-PKC) where user private keys were in two parts; one in possession of the user while the other in possession of the key generator center (KGC). This means that the KGC can partially access a user's private key, which is a good thing since the third parties are excluded from accessing users' data. More research led to Qu *et al.* (2018) proposing a new notion where he incorporated CL-PKC with equality test (CL-PKC-ET). An observation into the above-mentioned schemes indicates their homogenous nature, in that they can only be used in environments observing the same public key cryptography. Hence none of them can be considered for a cloud-assisted IoT environment that is heterogeneous. Furthermore, we recognize that currently, no public key encryption scheme with equality test is pertinent in the current environment.

To address this issue, we establish an effective public key encryption scheme that provides a heterogeneous systems equality test (abbreviated as HS-PKE-ET). A typical application scenario using HS-PKE-ET is shown in Figure 1. Within a smart grid environment, the data being conveyed (i.e., between the smart meter and cloud server) requires encryption to guarantee users' privacy. Namely, a public key encryption scheme that efficiently provides equality test in a heterogeneous environment is therefore required hence the public key infrastructure (PKI) and the certificateless public key system are merged. The PKI has proved to be efficient when it comes to achieving user identity authentication and security of data, the customers usually choose to use the PKI system to encrypt data. However, the CLC system has solved the certificate management problems brought by the PKI system and the problem of key escrow within the IBC system, most smart meters choose to use the CLC system to encrypt data. The collected data is encrypted by the smart meter and uploaded to the cloud server. A case in point is a customer wanting to retrieve their information stored on the cloud server (i.e., consumption of electricity on specific days). The customer will have to make use of their secret key to generate trapdoors, which will be forwarded to the cloud server. This cloud server however has been delegated the task of searching the data and then returning the results to the customer. Formerly, performing equality test for customers in different public key systems required them to encrypt the accumulated information using the identity of the smart meter owners. Considering that different smart meters are matched to different identities, it is imperative that customers find identities that match all smart meters. However, this results to substantial overhead and that is where our scheme is incorporated since it diminishes vapid process as it improves the operating efficiency.

Our contribution

This paper nominates a heterogeneous system public key encryption with equality test (HS-PKE-ET) with the integration between (PKE-ET) and (CLC-ET) as the center of attention. We base it on the bilinear pairing design that is depicted for smart grid environment. Our scheme security will be proved under the BDH assumption and the CDH assumption in the random oracle model (ROM). A demonstration of how the scheme will perform shall be illustrated in terms of computation and communication costs incurred through storage size, encryption, decryption, and testing phases.

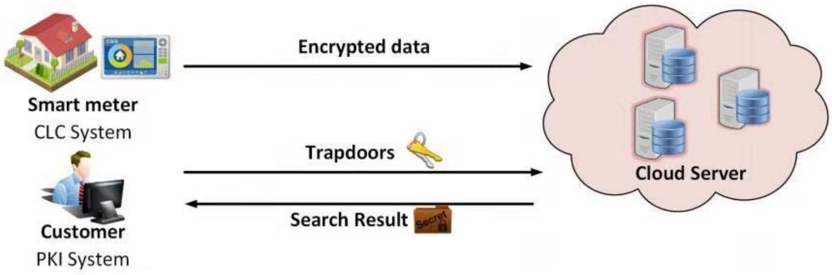

Figure 1: A typical scenario of the smart meter.

RELATED WORKS

Boneh *et al.* (2004) proposed a way of searching the public key encryption scheme by the use of key-words known as Public Key Encryption with Keyword search (PKE-KS). The ciphertexts in this scheme would be run through an equivalence test to determine if the keywords are the same. This is done by a third-party that is considered semi-trusted. The unfortunate issue is that IBE-KS has limitations when it is applied in real-time applications. Yang *et al.* (2010) however solved this limitation by proposing an encryption scheme that incorporated the equality test, not only on ciphertexts encrypted with the same public keys but also with different public keys. This scheme was known as Public Key Encryption with Equality Test (PKE-ET). The advantage of this scheme is that, it is quite flexible since an authorized cloud server has the search functionality hence can search messages to ascertain whether two ciphertexts encrypted with same or different public keys are equivalent. Consequently, (Tang, 2011) proposed a scheme that would enforce authorization on the PKE-ET which was known as fine-grained authorization Public key encryption with equality test (FG-PKE-ET). This scheme made provision for only two users to perform equality test. Nevertheless, there were situations where delegated parties were the only ones required to finish work in practical multi-user settings. Hence a delegated equality test scheme was of importance leading Ma *et al.* (2014) to propose such a scheme, which was known as (PKE-DET). Additionally, Ma *et al.* (2015) improved the PKE-AET by introducing support of flexibility when it came to authorization which was known as PKE-ET-FA. Unfortunately the public key infrastructure has proved to be unreliable when it comes to scalability since the distribution of public keys is unmanageable. New research areas on Identity-based encryption have hence sprouted as shown by (Ma, 2016; Lee, Ling, Seo, & Wang, 2016b; Wu, Zhang, Choo, & He, 2017). This encryption scheme has considered the outsourcing of equality tests in order to make the process more flexible when it comes to certificates management. And despite this encryption souring from key escrow, Lin *et al.* (2016) managed to find a solution by introducing the notion of certificateless public cryptography incorporated with equality test.

DEFINITIONS

Preliminaries

Bilinear Map

Considering two multiplicative cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$, and their prime order is p. g is a generator of $\mathbb{G}_1$. A bilinear map e : $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is required as follows:

1. Bilinearity: $\forall g \in \mathbb{G}_1, \exists a, b \in Z_p^*, e(g^a, g^b) = e(g, g)^{ab}$.

2. Non-degeneracy: $e(g, g) \neq 1$.

Hardness Problems

Establishing our scheme under the Bilinear Diffie-Hellman (BDH) problem and the Computational Diffie-Hellman (CDH) problem, the security of our system is defined. We describe these two hardness problems as follows:

BDH problem. Randomly choose $, b, c \in Z_p^*$, the BDH assumption holds if for any polynomial-time algorithm $\mathcal{A}$ which wants to distinguish the tuple $< g^a, g^b, g^c, e(g, g)^{abc} >$ from $< g^a, g^b, g^c, e(g, g) >$, the advantage is negligible.

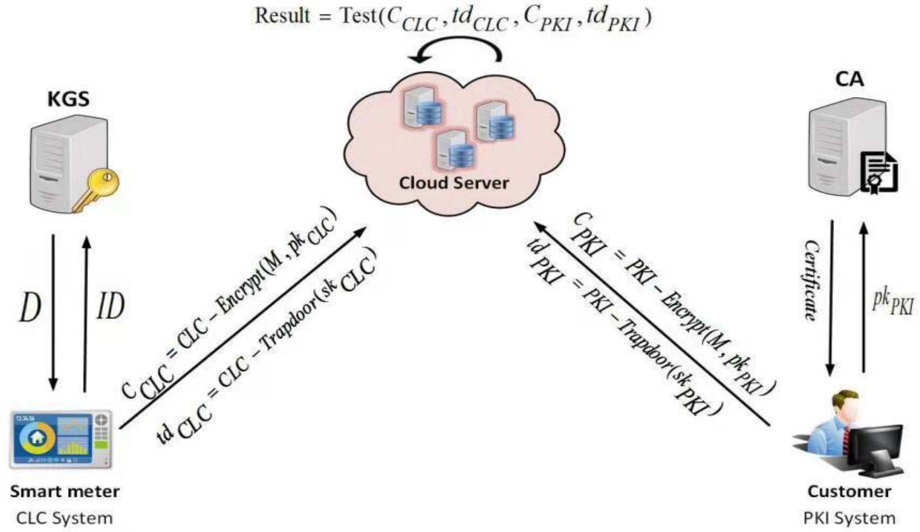
Result = Test(C_{CLC}, td_{CLC}, C_{PKI}, td_{PKI})
KGS
Cloud Server
CA
D
ID
C_{CLC} = CLC – Encrypt(M, pk_{CLC})
td_{CLC} = CLC – Trapdoor(sk_{CLC})
C_{PKI} = PKI – Encrypt(M, pk_{PKI})
td_{PKI} = PKI – Trapdoor(sk_{PKI})
Certificate
pk_{PKI}
Smart meter
CLC System
Customer
PKI System

Figure 2: System Model of HS-PKE-ET.

CDH problem. Randomly choose $a, b, c \in Z_p^*$, the CDH assumption holds if for any polynomial-time algorithm $\mathcal{A}$ which wants to distinguish the tuple $< g^a, g^b, g^{ab} >$ from $< g^a, g^b, g^c >$, the advantage is negligible.

System model

Figure 2 illustrates the heterogeneous systems public key encryption with equality test (HS-PKE-ET). The HS-PKE-ET model is made up of five entities: the smart meter, customer, key generation center (KGC), the certificate authority (CA), and a cloud server. Smart meter belongs to the CLC system, while the customer belongs to the PKI system. For the CLC system the smart meter sends its identity to the KGS, and the KGS prompts a corresponding partial secret key (D) and delivers it back to the smart meter. Consequently, on the PKI system side customer communicates with the CA to obtain a certificate signed by the CA. The smart meter and the customer then compute their particular trapdoors denoted by td_{CLC} and td_{PKI} , respectively. Subsequently, the smart meter uses the owner's ID to encrypt the collected data and uploads the encryptions alongside the trapdoor td_{CLC} to the cloud server for storage. When the customer desires to retrieve information, he/she uploads his/her trapdoor td_{PKI} to the cloud server for retrieval. The cloud server now possesses the td_{CLC} and td_{PKI} hence can execute an equivalence test between the CLC system and PKI system.

Security Models

According to (Ma, 2016), one-way chosen-ciphertext attack (OW-CCA) security against the adversary in HS-PKE-ET is defined. For streamlining, **HS-PKE-ET-CLC** to denote the situation that users belong to the CLC system and **HS-PKE-ET-PKI** to denote the situation that users belong to the PKI system are used.

Definition 1. *For the security of* ***HS-PKE-ET-CLC*** *we consider two types of adversaries. Type-1 adversary $\mathcal{A}_1$ cannot retrieve the system's secret master key, but has the ability to replace any user's public key. Type-2 adversary $\mathcal{A}_2$ has no ability to replace a user's public key, but can retrieve the system's master secret key.* ***HS-PKE-ET-CLC****'s security model is expounded by the following two games:*

Game 1: Given a security parameter λ , the game between $\mathcal{A}_1$ and the challenger is defined as follows:

1. *Setup*: The challenger creates the public parameters *PubP* and the master secret key *msk*. Finally, the challenger returns *PubP*.
2. *Phase 1*: The $\mathcal{A}_1$ is permitted to issue the following queries:

- *Partial secret key queries* $< ID_{i>}$: The challenger sends D_i to $\mathcal{A}_1$.
- *Secret key queries* $< ID_{i>}$*:* The challenger sends sk_{CLCi} to $\mathcal{A}_1$.
- *Public key queries* $< ID_{i>}$*:* The challenger sends pk_{CLCi} to $\mathcal{A}_1$.
- *Replace public key queries* $< ID_i, pk'_{CLCi} >$*:* The challenger replaces the public key *pk* of the corresponding user with pk'_i.

- *Decryption queries*$< ID_i, C_i >$: The challenger runs the algorithm CLC-Decrypt (C_i, sk_{CLCi}) where sk_{CLCi} is the secret key corresponding to ID_i. Finally, the challenger gives M_i to $\mathcal{A}_1$.

- *Trapdoor queries*: The challenger creates the trapdoors td_{CLCi} and td_{PKIi} by using *CLC-Trapdoor* and *PKI-Trapdoor* algorithms, respectively. Eventually, the chal-lenger gives td_{CLCi} and td_{PKIi} to $\mathcal{A}_1$.

3. *Challenge:* The challenger randomly chooses the plaintext $M \in G_1^*$ and computes C'= *CLC-Encrypt* (ID_{ch}, M). Finally, the challenger sends C' to $\mathcal{A}_1$ as its challenge ciphertext.

4. *Phase 2*: The challenger's response to $\mathcal{A}_1$ is similar to that in Phase 1 on the grounds that:

- *IDch* is not queried in the *Secret key queries*.

- If the public key associated with ID_{ch} is replaced, the ID_{ch} should not be queried in the *Partial secret key queries*.
- If the public key of the user is replaced, the corresponding identity ID_j should not be queried in the *Secret key queries*.

- $ID_{ch,}C'$ is not inquired in the *Decryption queries*.

5. *Guess*: $\mathcal{A}_1$ outputs M' , and wins if $M' = M$. The advantage of $\mathcal{A}_1$ in the game above is defined as follows:

$$Adv_{HS-PKE-ET,A}^{OW-CCA,HS-PKE-ET-CLC}(\lambda) = Pr[M = M']$$

Game 2: Provided with a security parameter λ, the game between $\mathcal{A}_1$ and the challenger is expounded as follows:

1. *Setup*: The challenger generates the public parameters *PubP* and master secret key *msk*. Finally, the challenger gives *PubP* and the *msk* to $\mathcal{A}_2$.

2. *Phase 1*: $\mathcal{A}_2$ issues queries as in **Game 1**, except the *Partial secret key queries* and the *Replace public key queries* are not allowed to issue in this game.

3. *Challenge*: The challenger randomly picks the plaintext $M \in G_1^*$ and computes C' = *CLC-Encrypt* (ID_{ch}, M). Finally, the challenger gives C' to $\mathcal{A}_2$ as its challenge cipher-text.

4. *Phase 2*: The challenger's response to $\mathcal{A}_2$ is similar to that in *Phase 1* on grounds that:
   - ID_{ch} is not queried in the *Secret key queries*.
   - (ID_{ch}, C^*) is not queried in the *Decryption queries*.

5. *Guess*: $\mathcal{A}_2$ outputs M' , and wins if $M' = M$. Therefore, $\mathcal{A}_2$ advantage in the game is:

$$Adv_{HS-PKE-ET,A}^{OW-CCA,HS-PKE-ET-CLC}(\lambda) = Pr[M = M']$$

Definition 2. *For the security of* **HS-PKE-ET-PKI** *scheme, we said the* **HS-PKE-ET-PKI** *has OW-CCA property if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following game.*

1. *Setup*: The challenger uses as input security parameters λ. Then, the challenger accords the system parameters to $\mathcal{A}$ and retains the *msk* secret.
2. *Phase 1*: $\mathcal{A}$ is allowed to inquire as follows:
   - *Key generation queries <i>:* The challenger sends sk_{PKIi} to $\mathcal{A}$.
   - *Decryption queries<i,C$_i$>:*The challenger runs *PKI-Decrypt* (C_i, sk_i) algorithm and sends the plaintext M to $\mathcal{A}$.
   - *Trapdoor queries <i>:* The challenger creates the trapdoors td_{CLCi} andtd_{PKIi} by using *CLC-Trapdoor* and *PKI-Trapdoor* algorithms, respectively. Finally, the challenger sends td_{CLCi} and td_{PKIi} to $\mathcal{A}$.

3. *Challenge*: The challenger arbitrary chooses a plaintext $M \in G_1^*$ and computes C' = *PKI-Encrypt*(pk'_{PKI}, M). In addition, the challenger creates a trapdoor td_{PKI} associated with sk'_{PKI} by using *PKI-Trapdoor* algorithm. Finally, the challenger sends (C', td_{PKI}) to $\mathcal{A}$.

4. *Phase 2*: In this phase, the response of C to $\mathcal{A}$ is similar to the one obtained in *Phase 1*. The following constraints are considered.
   - $< pk' >$ is not requested in the *key generation queries*.
   - $< pk', C' >$ is not requested in the *decryption queries*.

5. *Guess*: $\mathcal{A}$ outputs $M' \in G_1^*$, and wins if $M = M'$. The advantages of $\mathcal{A}$ in the game above is defined as follows:

$$Adv_{HS-PKE-ET,A}^{OW-CCA,HS-PKE-ET-PKI}(\lambda) = Pr[M = M']$$

CONSTRUCTION

The concrete constructions of heterogeneous systems public key encryption with equality test are instituted in this section.

1. *Setup*: Provided a security parameter λ, the algorithm runs as follows:
   - Generate the pairing parameters: two groups G_1, G_2 of prime order p and an admissible bilinear map e: $\mathbb{G}_1 \text{x} \mathbb{G}_1 \rightarrow G_2$ .Then choose a random generator $g \in \mathbb{G}_1$.
   - Choose cryptographic hash functions:
     $H_1: \{0,1\}^* \rightarrow, H_2: G_2 \rightarrow G_1, H_3: G_2 \rightarrow \{0,1\}^{n_1+n_2}, where\ n_1 = |G_1| and\ n_2 = |Z_p^*|$
   - Randomly choose $(s_1, s_2) \in Z_p^*$, then set $g_1 = g^{s1}$ and $g_2 = g^{s2}$. The *CLC-PKG* publishes system parameters $< p, G_1, G_2, e, g, g_1, g_2, H_1, H_2, H_3 >$ and keeps the master secret key $(s_{1,}s_2)$ secret.

2. *CLC-PKG*: To generate public and secret key, this algorithm works as follows:
   - *Generate partial secret key*: Given a string $ID \in \{0,1\}^*$:
     – Compute $h_{ID} = H_1(ID) \in \mathbb{G}_1$
     – Compute partial secret key $D = (D_1, D_2) = (h_{ID}^{s_1}, h_{ID}^{s_2})$, where (s_1, s_2) is the master secret key.
   - *Assign secret value*: The algorithm uses as inputs PubP and D. It chooses $x \in Z_p^*$ randomly then returns *x* as a secret value.
   - *Assign secret key*: The algorithm uses as inputs *PubP*, *D*, and *x*. It computes $sk = (sk_1, sk_2) = (D_1^x, D_2^x)$.
   - *Assign public key*: The algorithm uses as inputs *PubP* and a secret value *x*. It returns public key
     $pk = (X, pk_1, pk_2) = (g^x, g_1^x, g_2^x)$.

3. *IBC-Trapdoor*: This algorithm takes as input *sk* of a user in the CLC system and outputs a trapdoor $td_{CLC} = sk_1 = D_1^x$.

4. *PKI-KG*: A user in the PKI system chooses two arbitrary numbers $\theta, \beta \in Z_p^*$,and computes $(sk, pk) = ((\theta, \beta), (g^\theta, g^\beta))$

5. *PKI-Trapdoor*: This algorithm utilizes as input *sk* of a user in the PKI system and outputs a trapdoor $td_{PKI} = \theta$

6. *CLC-Encrypt*: This algorithm proceeds as follows:
   - Take the message $M \in \mathbb{G}_1^*$, the identity ID, and the public key $pk = (X, pk_1, pk_2)$ as inputs.
   - Verify that if $pk = (X, pk_1, pk_2) \in \mathbb{G}_1^*$ and $e(X, g_1) = e(pk_{1,}g)$ and $e(X, g_2) = e(pk_2, g)$. If these verifications pass, perform the encryption. Otherwise, terminate the encryption.
   - Compute $h_{ID} = H_1(ID) \in \mathbb{G}_1^*$.
   - Pick two arbitrary numbers $(r_1, r_2) \in Z_p^*$.
   - Compute $C = (C_1, C_2, C_3, C_4)$, where $C_1 = g^{r_1}, C_2 = g^{r_2}, C_3 = M^{r_1} \cdot H_2(e(h_{ID}, pk_1)^{r_1}), and\ C_4 = (M||r_1) \oplus H_3(e(h_{ID}, pk_2)^{r2})$.

7. *CLC-Decrypt*: The algorithm uses as inputs a ciphertext *C* and a secret key *sk*. It returns the plaintext *M* by working as follows.
   - Compute $C_4 \oplus H_3(e(sk_2, C_2)) = C_4 \oplus H_3(e(sk_2, C_2)) = C_4 \oplus H_3\left(e(D_2^{xID}, g^{r_2})\right) = C_4 \oplus H_3(e(h_{ID}, g_2^{xID})^{r_2}) = (M||r_1)$
   - Verify if $C_1 = g^{r_1}$ and $\frac{C_3}{M^{r_1}} = H_2(e(sk_1, C_1))$.
   - If both verifications pass, return *M*. Otherwise, return the symbol $\perp$.

8. *PKI-Encrypt*: It utilizes as inputs a message M and the public key pk of a user in the PKI system. Then, it chooses two random numbers $(r_1, r_2) \in Z_P^*$ and computes

$C = (C_1, C_2, C_3, C_4)$, where

$C_1 = g^{r_1}, C_2 = g^{r_2}, C_3 = M^{r_1} \cdot H_2(g^{\theta r_1}), and\ C_4 = (M||r_1) \oplus H_3\ (g^{\beta r_2})$

9. *PKI-Decrypt*: It takes as inputs a ciphertext C and secret key sk of a user in the PKI system. Then, gives back the plaintext M by computing $M||r_1 \leftarrow C_4 \oplus H_3(C_2^{\beta})$, and then verifies both $C_1 = g^{r_1}$ and $\frac{C_3}{M^{r_1}} = H_2\ (C_1^{\theta})$. In the event that both verifications pass, it returns M else, it returns the symbol $\perp$.

10. *Test* $(C_i, td_{CLC}, C_j, td_{PKI})$: Let U_i and U_j be two users of heterogeneous systems. Let U_i be a user in the CLC system and U_j be a user in the PKI system. Let $C_i = (C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})$ and $C_j = (C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4})$ be the ciphertexts of U_i andU_j, respectively. The Test algorithm for heterogeneous systems works as follows:

$$\begin{aligned} R_i &= \frac{C_{i,3}}{H_2(e(td_{CLC}\ ,\ C_{i,1}))} \\ &= \frac{M_i^{r_{i,1}} \cdot H_2(e(h_{ID,i}\ ,\ pk_{i,1})^{r_{i,1}})}{H_2(e(sk_{i,1}\ ,\ C_{i,1}))} \\ &= \frac{M_i^{r_{i,1}} \cdot H_2(e(h_{ID,i}\ ,\ g_1^{x_i})^{r_{i,1}})}{H_2(e(D_{i,1}^{x_i}\ ,\ g^{r_{i,1}}))} \\ &= \frac{M_i^{r_{i,1}} \cdot H_2(e(h_{ID,i}\ ,\ g_1^{x_i})^{r_{i,1}})}{H_2(e(h_{ID,i}\ ,\ g_1^{x_i})^{r_{i,1}})} \\ &= M_i^{r_{i,1}} \end{aligned}$$

$$\begin{aligned} R_j &= \frac{C_{j,3}}{H_2(C_{j,1}^{td_{PKI}})} \\ &= \frac{M_j^{r_{j,1}} \cdot H_2(g^{\theta r_{j,1}})}{H_2(g^{\theta r_{j,1}})} \\ &= M_j^{r_{j,1}} \end{aligned}$$

The **Test** algorithm returns 1 if $e(C_{i,1},\ R_j) = e(C_{j,1}, R_i)$. Otherwise, it returns the symbol $\perp$.

SECURITY ANALYSIS

In this segment, the security of the **HS-PKE-ET** scheme is presented. The basic notion of security proof is similar to the scheme in (Al-Riyami & Paterson, 2003) and (Huang et al., 2015).

Theorem 1: Presuming that H_1, H_2, H_3 are random oracles and assume that the BDH problem is hard. Therefore, our **HS-PKE-ET-CLC** is OW-CCA secure. Significantly, assume there is a **Type-1 adversary** $\mathcal{A}_1$ that has advantage $\varepsilon_1(\lambda)$ against the **HS-PKE-ET-CLC**. Assume that $\mathcal{A}_1$ makes q_{pk} public key queries, q_{sk} secret key queries, q_{psk} partial secret key queries, q_t trapdoor queries, q_{rpk} replace public key queries, q_{dec} decryption queries, q_{H_2} hash queries to H_2, and q_{H_3} hash queries to H_3. Thus, we have an algorithm $\mathcal{B}_1$ which breaks BDH problem with advantage at least $\varepsilon_1(\lambda)/e(q_{sk} + q_{psk} + q_t + 1).\ q_{H_3}$.

Theorem 2: Presuming that H_1, H_2, H_3 are random oracles and assume that the BDH problem is hard. Therefore, our **HS-PKE-ET-CLC** is OW-CCA secure. Significantly, assume there is a **Type-2 adversary** $\mathcal{A}_2$ that has advantage $\varepsilon_2(\lambda)$ against the **HS-PKE-ET-CLC**. Assume that $\mathcal{A}_2$ makes q_{pk} public key queries, q_{sk} secret key queries, q_t trapdoor queries, q_{dec} decryption queries, q_{H_2} hash queries to H_2, and q_{H_3} hash queries to H_3. Thus, we have an algorithm $\mathcal{B}_2$ which breaks BDH problem with advantage at least $\varepsilon_2(\lambda)/e(q_{sk} + q_t + 1).\ q_{H_3}$.

Theorem 3*:* HS-PKE-ET-PKI is OW-CCA secure against the adversary $\mathcal{A}$ if CDH problem is intractable.

Proof: Assume that $\mathcal{A}$ is an adversary, who is permitted to make q_K key generation queries, decryption queries, q_T trapdoor queries, q_{H_2} hash queries to H_2, and q_{H_3} hash queries to H_3. The algorithm $\mathcal{B}$ emulates certain games, dominates oracle O_K, O_D, O_T, O_{H_2}, and O_{H_3}, and then utilizes the advantage of $\mathcal{A}$ to break CDH problem if $\mathcal{A}$ breaks **HS-PKE-ET-PKI**. Consequently, a sequence of hybrid games are presented for verification of the security of our scheme. Due to the limited number of pages, the interested readers can refer to (Al-Riyami & Paterson, 2003) and (Huang et al., 2015) for more details.

PERFORMANCE ANALYSIS

In Table 1, the computation cost and communication cost of the proposed **HS-PKE-ET** scheme and the schemes in (Yang et al., 2010), (Ma, Huang, et al., 2015), (Ma, 2016), (Lin et al., 2016), and (Qu et al., 2018) are compared.

Table 1: Comparison

Schemes	|PK|	|SK|	|CT|	Enc	Dec	Test	H-ET
(Yang et al., 2010)	$\mathbb{G}$	$2Z_p$	$3\mathbb{G}+Z_p$	3Exp	3Exp	2Pair	No
(Ma et al., 2015)	$3\mathbb{G}$	$3Z_p$	$5\mathbb{G}+Z_p$	6Exp	5Exp	2Pair+2Exp	No
(Ma, 2016)	$2\mathbb{G}$	$2Z_p$	$4\mathbb{G}+Z_p$	6Exp	2Pair+2Exp	4Pair	No
(Lin et al., 2016)	$2\mathbb{G}$	$2Z_p$	$5\mathbb{G}+Z_p$	6Exp	2Pair+2Exp	4Pair	No
(Qu et al., 2018)	$2\mathbb{G}$	$2Z_p$	$5\mathbb{G}+Z_p$	5Exp	2Pair+2Exp	4Pair	No
HS-PKE-ET	$2\mathbb{G}$	$2Z_p$	$3\mathbb{G}+Z_p$	5Exp	2Pair+2Exp	3Pair+1Exp	Yes

Legends: |PK|, |SK|, and |CT|: size of public key, size of secret key, size of and ciphertext, respectively; Enc, Dec, and Test: the computation complexity of encryption, decryption, and test algorithms; Exp: an exponentiation operation; Pair: pairing operation; H-ET: the scheme that provides heterogeneous equality test.

CONCLUSION

We nominate an efficient equality test for heterogeneous systems in this paper. The nature of the heterogeneity in our scheme allows for a cloud server to accomplish an equivalence test between ciphertexts that have been encrypted under the PKI system and CLC system. Furthermore, we have reduced our scheme's security proof to the standard Bilinear Di e-Hellman assumption and computational Diffie-Hellman assumption by basing it on the random oracle model. Our speculative analysis and simulations from experiments indicate our scheme's practicability and suitability in comparison to other related works. Future works include expansion of the heterogeneous equality test to make provision for users to delegate a cloud server rights to execute equality test employing different types of authorizations.

ACKNOWLEDGMENT

This work was supported in part by the 13th Five-Year Plan of National Cryptography Development Fund for Cryptographic Theory of China under Grant MMJJ20170204, in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2016J091, the Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, and in part by the Natural Science Foundation of China under Grants U1401257, 61472064 and 61602096.

REFERENCES

[1] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., .Shi, H. (2005). Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In Crypto (Vol. 3621, pp. 205–222).

[2] Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In Asiacrypt (Vol. 2894, pp. 452–473).

[3] Baek, J., Safavi-Naini, R., & Susilo, W. (2008). Public key encryption with keyword search revisited. Computational Science and Its Applications–ICCSA 2008, 1249–1259.

[4] Batamuliza, J. (2018). Certificateless secure anonymous key distribution scheme for smart grid. International Journal of Computer Applications (Vol. 180 – No.24).

[5] Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. In International conference on the theory and applications of cryptographic techniques (pp. 506–522).

[6] Huang, K., Tso, R., Chen, Y.-C., Rahman, S. M. M., Almogren, A., & Alamri, A. (2015). Pke-aet: public key encryption with authorized equality test. The Computer Journal, 58(10), 2686–2697.

[7] Jokar, P., Arianpoo, N., & Leung, V. C. (2016). A survey on security issues in smart grids. Security and Communication Networks, 9(3), 262–273.

[8] Lee, H. T., Ling, S., Seo, J. H., & Wang, H. (2016a). Cca2 attack and modification of huang et al.s public key encryption with authorized equality test. The Computer Journal, 59(11), 1689–1694.

[9] Lee, H. T., Ling, S., Seo, J. H., & Wang, H. (2016b). Semi-generic construction of public key encryption and identity-based encryption with equality test. Information Sciences, 373, 419–440.

[10] Li, B., Lu, R., Wang, W., & Choo, K.-K. R. (2016). Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Transactions on Information Forensics and Security, 11(11), 2415–2425.

[11] Lin, X. J., Yan, Z., Zhang, Q., & Qu, H. (2016). Certificateless public key encryption with equality test. IACR Cryptology ePrint Archive, 2016, 1129.

[12] Lynn, B. (2013). The Stanford pairing based crypto library. Privacy Preservation Scheme for Multicast Communications in Smart Buildings of the Smart Grid, 324.

[13] Ma, S. (2016). Identity-based encryption with outsourced equality test in cloud computing. Information Sciences, 328, 389–402.

[14] Ma, S., Huang, Q., Zhang, M., & Yang, B. (2015). Efficient public key encryption with equality test supporting flexible authorization. IEEE Transactions on Information Forensics and Security, 10(3), 458–470.

[15] Ma, S., Zhang, M., Huang, Q., & Yang, B. (2015). Public key encryption with delegated equality test in a multi-user setting. The Computer Journal, 58(4), 986–1002.

[16] Qu, H., Yan, Z., Lin, X.-J., & Zhang, Q. (2018). Certificateless public key encryption with equality test.

[17] Tang, Q. (2011). Towards public key encryption scheme supporting equality test with fine-grained authorization. In Australasian conference on information security and privacy (pp. 389–406).

[18] Wu, L., Zhang, Y., Choo, K.-K. R., & He, D. (2017). Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Generation Computer Systems, 73, 22–31.

[19] Xu, Y., Wang, M., Zhong, H., Cui, J., Liu, L., & Franqueira, V. N. (2017). Verifiable public key encryption scheme with equality test in 5g networks. IEEE Access.

[20] Yang, G., Tan, C. H., Huang, Q., & Wong, D. S. (2010). Probabilistic public key encryption with equality test. In Cryptographers track at the rsa conference (pp. 119–131).