IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 April 2023, accepted 4 May 2023, date of publication 16 May 2023, date of current version 25 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3276446

RESEARCH ARTICLE

New Constructions of Equality Test Scheme Without Random Oracles

HUIJUN ZHU[1,2], HASEEB AHMAD[3], QINGJI XUE[1,2], TIANFENG LI[1,2], ZIYU LIU[1,2], AND AO LIU[1,2]

[1]Nanyang Institute of Technology, Henan 473000, China
[2]Graphic Image and Intelligent Processing in Henan Province, International Joint Laboratory, Nanyang Institute of Technology, Henan 473000, China
[3]Department of Computer Science, National Textile University, Faisalabad 37610, Pakistan

Corresponding author: Qingji Xue (xue_qj@sina.com)

This work was supported in part by the Projects of Henan Provincial Department of Science and Technology under Grant 212102310297; in part by the National Natural Science Foundation of China (NSFC) under Grant 61972050; in part by the Open Foundation of State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2019-2-17; and in part by the Interdisciplinary Sciences Project, Nanyang Institute of Technology.

ABSTRACT The proliferation of big data has brought exponential amount of increase in data that is being remotely stored around the globe. Thus, making it imperative to secure the remote data through some encryption mechanism to ensure privacy preservation. However, it often becomes difficult to perform operations over the encrypted data. In order to solve this problem, the equality test function based public key encryption (PKEwET) is proposed. PKEwET approach basically allows secure comparison over encrypted data without revealing the underlying data. This work aims to improve Water's scheme while introducing a new functionality. More precisely, equality test is being introduced to Water's scheme so that the encrypted data may be compared without decryption process. To achieve this, an authorization mechanism is being included in which the authorized party uses the trapdoor to test the ciphertext. The scheme is designed under standard model. The security of the proposed scheme is proved with two types of adversaries under the standard model. Finally, the superiority of the proposed scheme in terms of performance is also discussed.

INDEX TERMS Equality test, public key encryption, searchable encryption, standard model.

I. INTRODUCTION

The intensive release of data over the Internet has made it impossible for the people to store and process information in traditional ways. Such tasks are now being performed on remote servers. This dive has raised concerns to ensure security and privacy of remotely stored data. Such concerns are being addressed while presenting cryptographic protocols. However, with the advent of quantum computing and due to its high speed computations, some of the current cryptographic protocols are at the verge of breach. Thus, it is imperative to put forward more secure and privacy preservation techniques. With this aim, this paper presents a bilinear pairing based solution with the equality test in the standard model.

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

II. RELATED WORK

The method of equality test was first proposed by Yang et al [1]. It is a public key encryption (PKE) scheme that allows the performance of equality tests on the encrypted data using different public keys. In 2016, Hyung Tae Lee et al. introduced the computational Diffie Hellman problem (CDH) in the stochastic prediction stochastic model [2]. The chosen ciphertext attacks (CCA) security is implemented by adding message related values as input to the hash function of the encryption algorithm. In the same year, Majid Nateghizad et al. proposed a novel and efficient equality test method [3]. More precisely, by introducing algorithm mutation and an efficient exponential subroutine, data encapsulation is deployed. In 2017, Wang et al. proposed an encryption scheme for authorized equality test on ciphertexts (SEET) [4]. This scheme allows the data owner to authorize the testing stakeholder to compare the ciphertext without

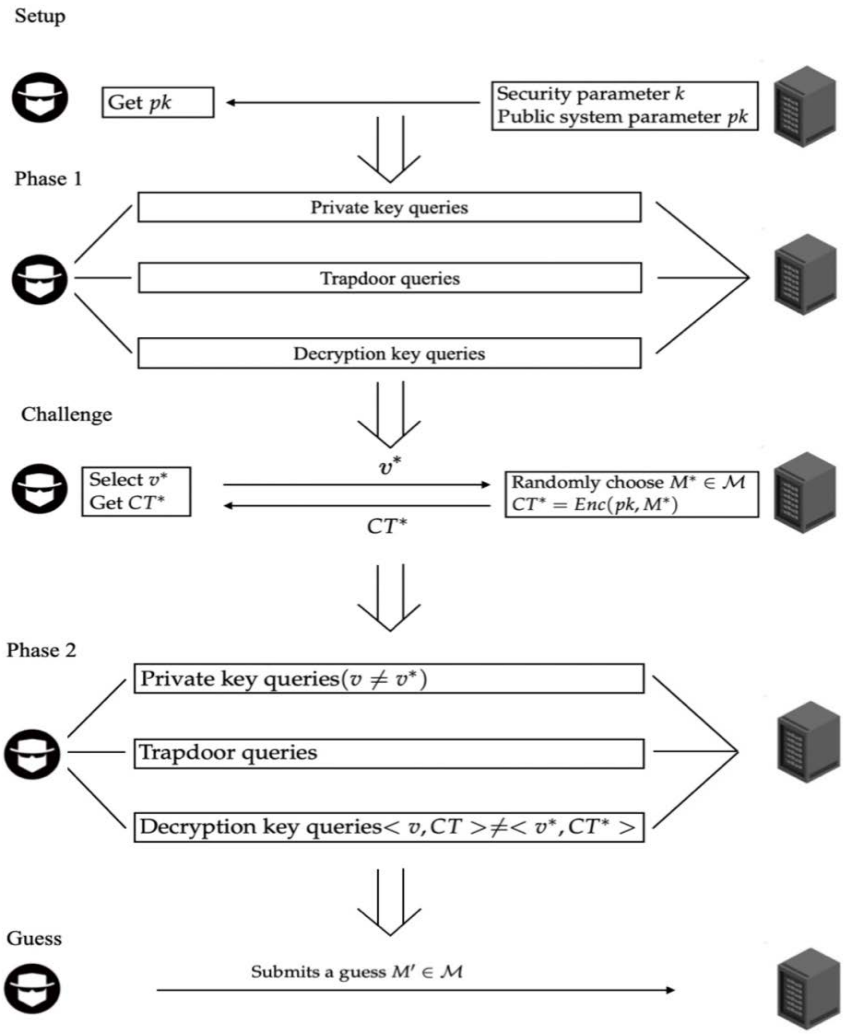

FIGURE 1. OW-ID-CCA security model.

understanding the ciphertext data. In 2018, Sun et al. proposed the concept of attribute hidden predicate encryption equation test (AH-PE-ET) by introducing the concepts of attribute-based and equality test [5]. This inherits the advantages of predicate encryption and allows universal access control. Thus, the ciphertext and key are associated with the descriptive attribute x and the Boolean function f respectively. The ciphertext can be decrypted only when x returns true. Nabeil Eltayieb et al. proposed a fine-grained attribute-based encryption supporting equality test (FGABEET) [6]. The scheme allows the cloud server to execute two ciphertext encrypts of the same message encrypted with the same access policy or with different access policies. In addition, cloud servers may also perform equivalent test operations. Thus, the user don't need to know anything about messages encrypted under any access policy. Lin et al. proposed a general public key encryption with equality test (PKEETP) construction method [7]. This method can be easily extended to identity based settings. In addition, the authors also proposed a new protocol language, called signcryption with equality test (SCET). Compared with traditional PKEET, SCET provides both confidentiality and authentication.

In 2019, Zhang et al. proposed an identity based encryption approach and used it to design an efficient CCA2 security PKE scheme [8]. The scheme proposed by Wang et al. enables the sender to encrypt and sign messages simultaneously [9]. The proposed scheme specifies a testing stakeholder to perform equality tests on ciphertext. Wu et al. proposed pairing-free identity-based encryption scheme with authorized equality test [10]. Li et al. proposed an identity-based encryption with equality test supporting flexible authorization(IBEE-FA) [11]. In addition, it supports testing whether two ciphertext encrypted under different keys encapsulate the same messages or not. Hyung Tae Lee et al. employed an identity-based two-tier hierarchical encryption scheme for their universal construction [12]. The scheme

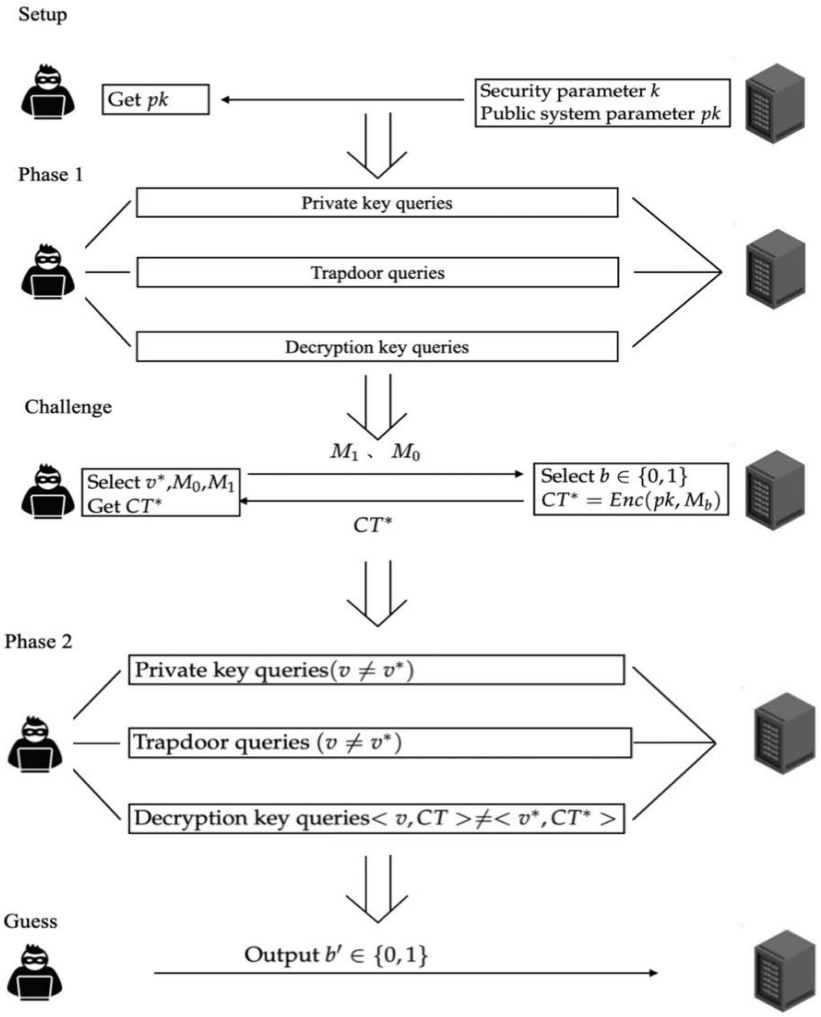

FIGURE 2. IND-ID-CCA security model.

can selectively resist the chosen plaintext attack. Ling et al. introduced group mechanism into PKEET for the first time and proposed a new primitive, group public key encryption with equality testing [13]. PKEET can resist attacks where a tester can guess a message offline and recover it from the given ciphertext.

In 2020, Wang et al. removed authorized duplicate data by flexibly removing encrypted data [14]. More precisely, the users can optimize their storage space by delegating their equality tests. This may enable the constrained users and mobile devices to be more efficient. Abdelrhman Hassan et al. proposed a certificateless PKE with authorized equality test (CLPKEAET) [15]. In details, the CLPKEAET scheme, authorizes cloud servers to check the equivalence of two different passwords composed of the same message. In the random oracle model (ROM), the construction of bilinear pairing is incorporated in the underlying scheme. The scheme is proved to be safe under the improved bilinear Diffie-Hellman assumption. In 2021, Lin et al. proposed a scheme of identity based encryption with equality test and date stamp-based authorization mechanism (IBEET-DBA) [16]. In the primitive, the data owner can control the effectiveness of the trap by embedding a date stamp in the trap. Cloud servers can only get correct equivalents on ciphertext generated during the trap door validity period. In 2022, Shen et al. proposed an efficient and verifiable group public key encryption algorithm with an equality test structure without bilinear pairs [17]. The scheme is based on the basic observation that two points determine a straight line. In 2023, Hanshu Hong and Zhixin Sun propose the paradigm of Conditional Public Key Encryption and Equality Testing (CPKEET) [26]. This paradigm allows a user to perform ciphertext testing only if he holds a valid certificate generated by the specified issuer server.

A. OUR CONTRIBUTIONS

Though the Water's scheme is classical and practical, but it may be improved for more recent applications while

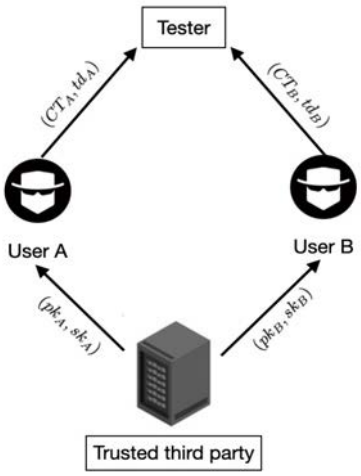

FIGURE 3. System model.

introducing equality test [insert citation of Water's scheme here]. To bridge this gap, an improved scheme is proposed in this paper. The improved scheme may be incorporated in various scenarios including Internet of Things, Cloud Services and Internet of Vehicles etc. The major contributions of this work are summarized as follows:

- In order to make it more practicle, the paper introduces equality test to Waters's scheme. More precisely, the paper proposes Identity-based encryption with equality test based on standard model. (IBEwET-S).
- To prove the security of IBEwEST scheme, two types of attackers are introduced that have different permissions.
- More precisely, for first type of attacker with the trapdoor, the scheme can resist one-way against chosen-ciphertext attack selective-ID (OW-ID-CCA) security. While for the attacker without trapdoor option, the scheme can resist indistinguishable against chosen-ciphertext attack selective-ID (IND-ID-CCA) security.
- Through theoretical deduction, performance of the IBEwET-S scheme is verified. Our scheme is more efficient and practical as compared to other schemes supporting equality test based on standard model.

B. OUTLINE OF THIS PAPER

The rest of this article is structured as follows: In Section III, the preliminary knowledge is introduced. The system models and the security models are discussed in Section IV and V, respectively. Section VI describes the details of the proposed algorithm. Section VII provides security proof of the proposed scheme. In Section VIII, the efficiency of the algorithm is evaluated experimentally. Finally, we summarize the work in Section IX.

III. PRELIMINARIES

A. BILINEAR MAP

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of prime order p. Suppose that g is a generator of $\mathbb{G}_1$. A bilinear map e:$\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ satisfies the following properties:

Bilinear: For any $g \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$, $e(g^a, g^b) = e(g, g)^{ab}$.

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

Computable: There is an efficient algorithm to compute $e(g, g)$ for any $g \in \mathbb{G}_1$.

B. DECISIONAL BILINEAR DIFFIE-HELLMAN(DBDH) ASSUMPTION

In this algorithm, the challenger picks $a, b, c, z \in Z_p^*$ and flips coin $coin \in \{0, 1\}$ randomly.

- If $coin = 0$, $\mathcal{S}$ outputs $(g, g^a, g^b, g^c, e(g, g)^z)$.
- Otherwise, $\mathcal{S}$ outputs $(g, g^a, g^b, g^c, e(g, g)^{abc})$.

Then, the adversary $\mathcal{A}$ gives a guess of $coin$.

C. CONSISTENCY

For the consistency property, these algorithms must satisfy the following three conditions:

- When d is the private key generated by Key Generation algorithm and v is given as the public key, then

$$\forall M \in \mathcal{M} : \text{Decrypt}(CT, d) = M,$$

where

$$CT = \text{Encrypt}(v, M).$$

- When td_A and td_B are trapdoors generated by Trapdoor algorithm and, v_A and v_B are given as the public keys, then

$$\forall M \in \mathcal{M} : \text{Test}(CT_A, td_A, CT_B, td_B) = 1,$$

where,

$$CT_A = \text{Encrypt}(v_A, M)$$

and

$$CT_B = \text{Encrypt}(v_B, M).$$

- When td_A and td_B are trapdoors generated by Trapdoor algorithm and, v_A and v_B are given as the public keys, then
$\forall M \in \mathcal{M}$ and $M \neq M'$:

$$\Pr[\text{Test}(CT_A, td_A, CT_B, td_B) = 1]$$

is negligible, where

$$CT_A = \text{Encrypt}(v_A, M)$$

and

$$CT_B = \text{Encrypt}(v_B, M').$$

Here $M \neq M'$ holds.

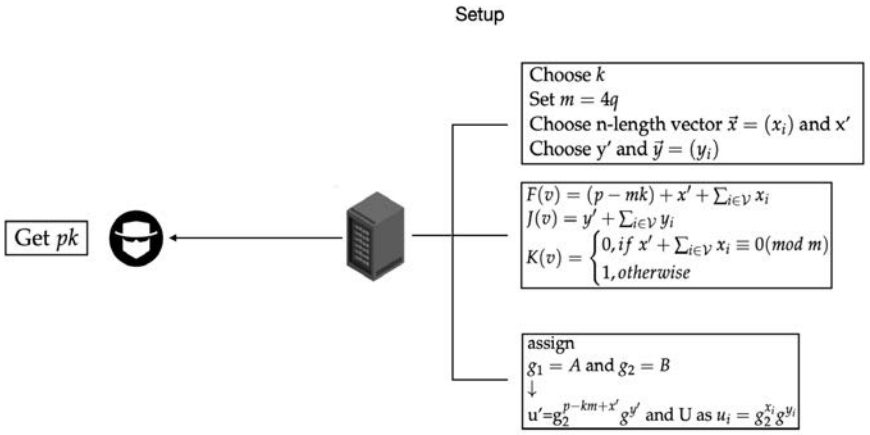

FIGURE 4. Setup of Game 1.

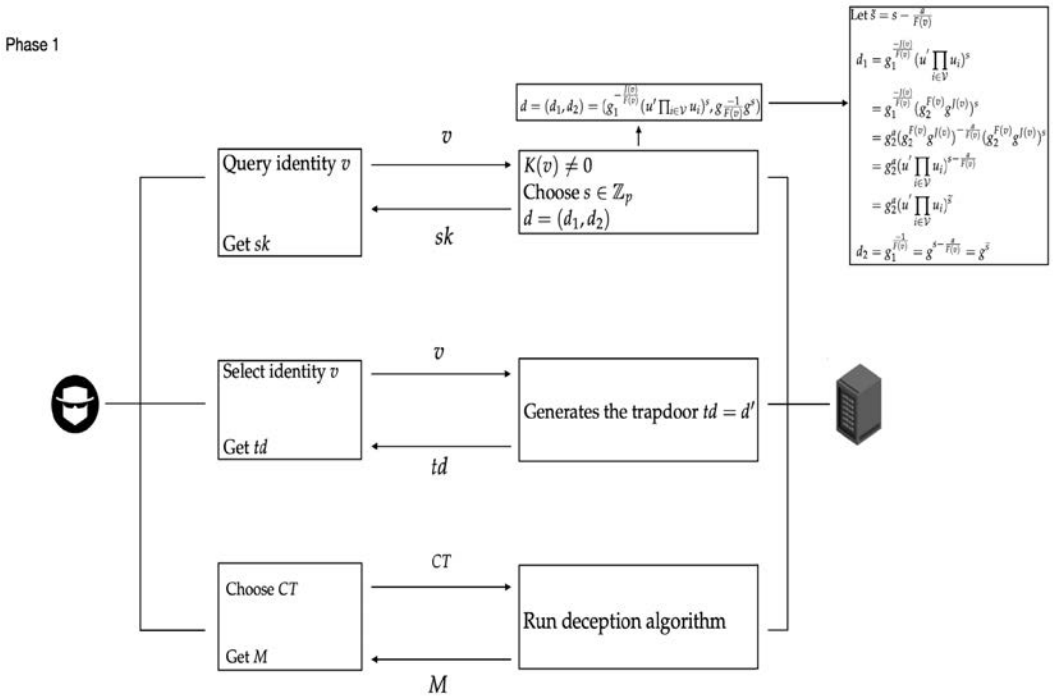

FIGURE 5. Phase 1 of Game 1.

D. DEFINITIONS

In this subsection, we present definitions of PKE security and correctness.

One-way against chosen-ciphertext attack (OW-ID-CCA) security: The attacker can decrypt queries at any time except for the target ciphertext CT^*, and the corresponding message M cannot be obtained from the public key and CT^*.

Indistinguishable against chosen ciphertext attacks (IND-ID-CCA) security: The attacker can decrypt queries at any time except for the target ciphertext CT^*, and selects M_0 and M_1, then the challenger randomly selects $b \in \{0, 1\}$ and generates the target ciphertext CT^* by M_b. The attacker cannot guess the value of b by using ciphertext CT^*.

IV. SYSTEM MODELS

The proposed scheme is comprised of four entities, the tester, the trusted third party and two user users. Detailed description is shown in Fig.3. The scheme is comprised of six algorithms: Setup, Extract, Trapdoor, Encrypt, Decrypt, Test, where $\mathcal{M}$ and $\mathcal{C}$ are its plaintext space and ciphertext space. The details of these are briefed as follows:

Setup(k): It takes a security parameter and the public system parameter p as inputs and returns the master key msk.

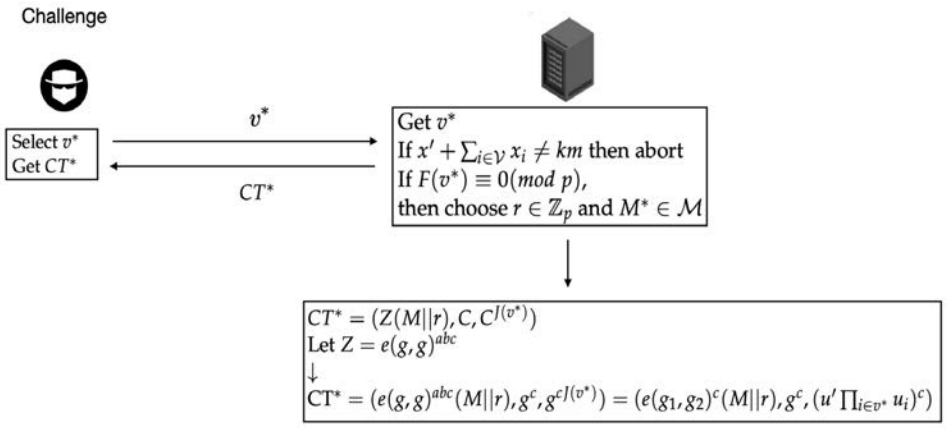

FIGURE 6. Challenge of Game 1.

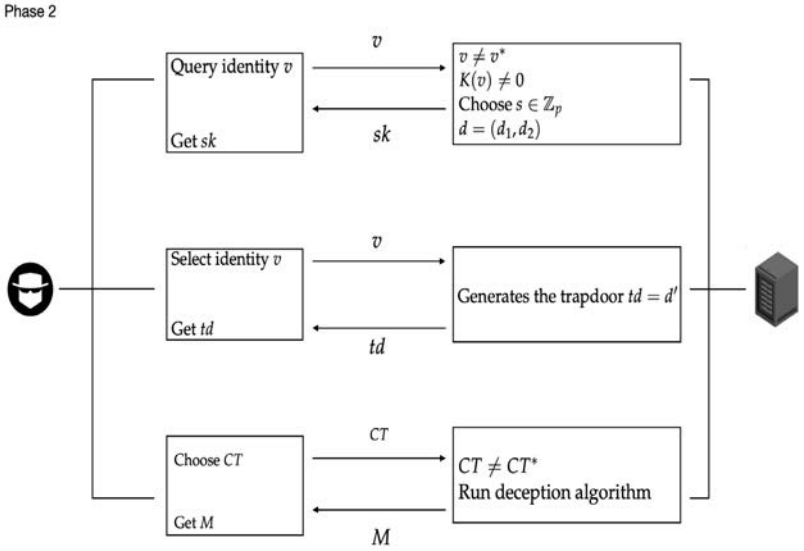

FIGURE 7. Phase 2 of Game 1.

Extract(msk, v): It takes msk and an arbitrary identity $v \in \{0, 1\}^*$ as inputs and returns a private key d for that identity.

Trapdoor(msk, v): It takes msk and an arbitrary identity $v \in \{0, 1\}^*$ as inputs and returns a trapdoor td for that identity.

Encrypt(v, M): It takes an identity $v \in \{0, 1\}^*$ and a plaintext $M \in \mathcal{M}$ as inputs and returns a ciphertext $CT \in \mathcal{C}$.

Decrypt(CT, d): It takes a ciphertext $CT \in \mathcal{C}$ and a private decryption key d as inputs and returns a plaintext $M \in \mathcal{M}$.

Test(CT_A, d'_A, CT_B, d'_B): It takes a ciphertext $CT_A \in \mathcal{C}$ of a receiver with v_A, a trapdoor td_A for the receiver with v_A, a ciphertext CT_B of a receiver with v_B and a trapdoor td_B for the receiver with v_B as inputs and returns 1 if CT_A and CT_B contain the same message; Otherwise returns 0.

V. SECURITY MODELS

We describe two different types of adversaries based on the adversarial permissions as follows:

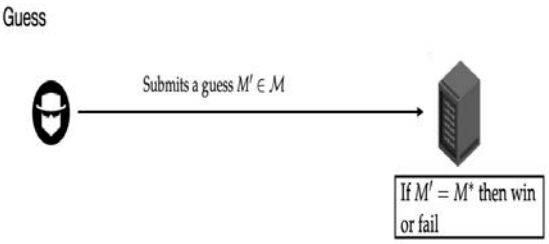

FIGURE 8. Guess of Game 1.

- Type-1 adversary: We allow this adversary a trapdoor. So this type of adversary cannot recover the plaintext with the challenge ciphertext CT^*.
- Type-2 adversary: To this adversary, we do not allow the trapdoor. So this type of adversary cannot decide that the CT^* is encrypted on which message.

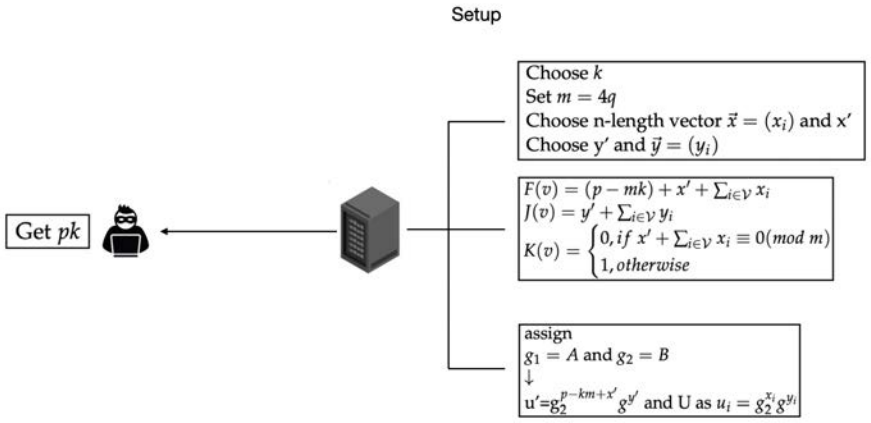

FIGURE 9. Setup of Game 2.

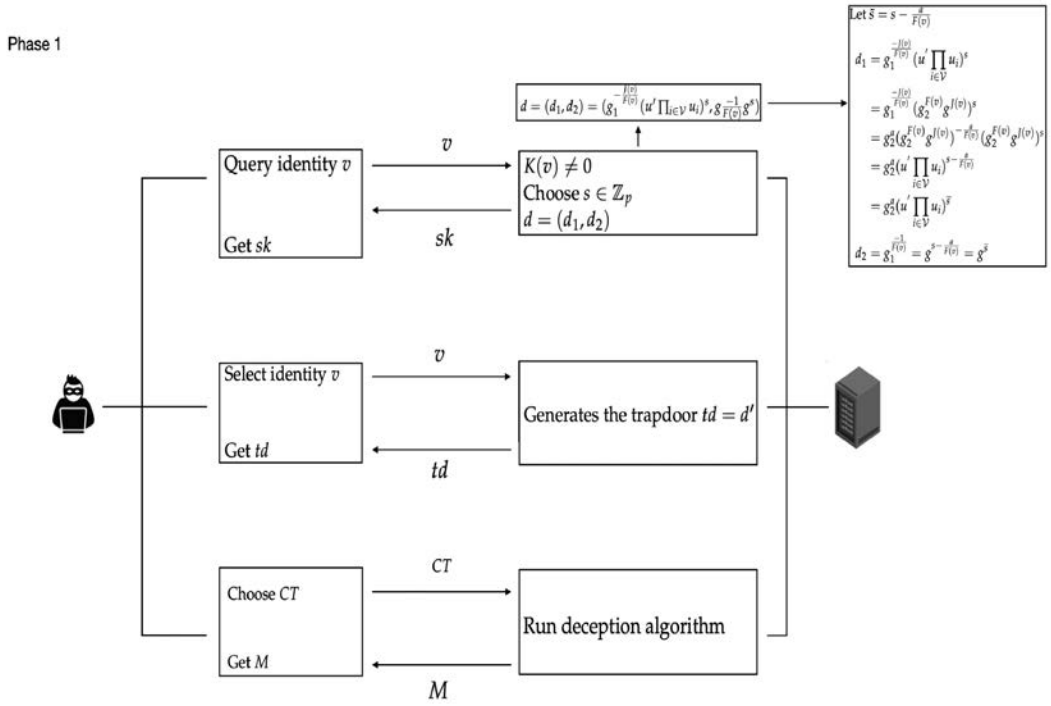

FIGURE 10. Phase 1 of Game 2.

First, we define OW-ID-CCA security to the Type-1 adversary in IBEwET-S scheme. The specific details are depicted in Fig.1,

Definition 1: The IBEwET-S scheme is OW-ID-CCA secure if for all OW-ID-CCA adversaries, $Adv^{OW-ID-CCA}_{IBEwET-S,\mathcal{A}}(k) = \Pr[M = M']$ is negligible.

Next, we define the IND-ID-CCA security to the Type-2 adversary in IBEwET-S. The specific details are depicted in Fig.2,

Definition 2: The IBEwET-S scheme is IND-ID-CCA secure if for all IND-ID-CCA adversaries, $Adv^{IND-ID-CCA}_{IBEwET-S,\mathcal{A}}(k) = |\Pr[b = b'] - \frac{1}{2}|$ is negligible.

VI. PROPOSED SCHEME

In this section, we provide a detailed construction for the IBEwET-S scheme as follows:

Setup(k) Given a security parameter $k \in \mathbb{Z}^+$, the algorithm works as follows:

Step 1: Let identities composed of bitstrings of arbitrary length n be the output length of a collision-resistant hash function, $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$.

Step 2: Generate the pairing parameters including two groups $\mathbb{G}_1$, $\mathbb{G}_2$ of prime order p, and an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. A secret $\alpha \in \mathbb{Z}_p$ is chosen at random. We choose a random generator $g \in \mathbb{G}_1$ and set the

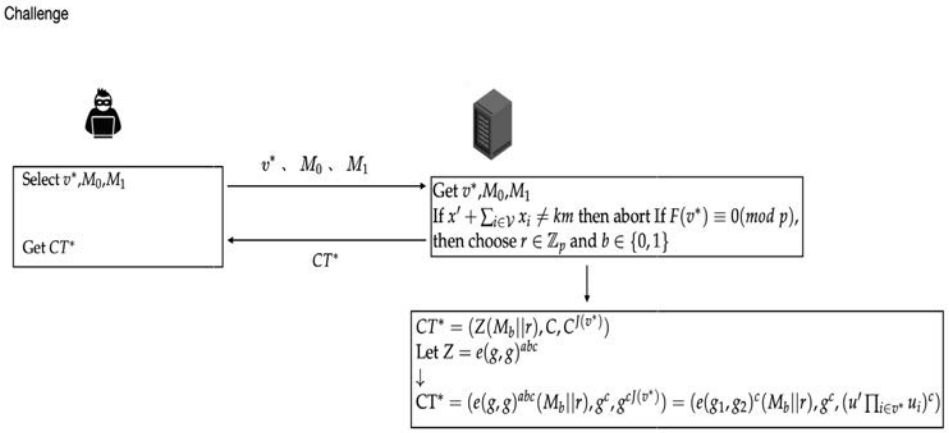

FIGURE 11. Challenge of Game 2.

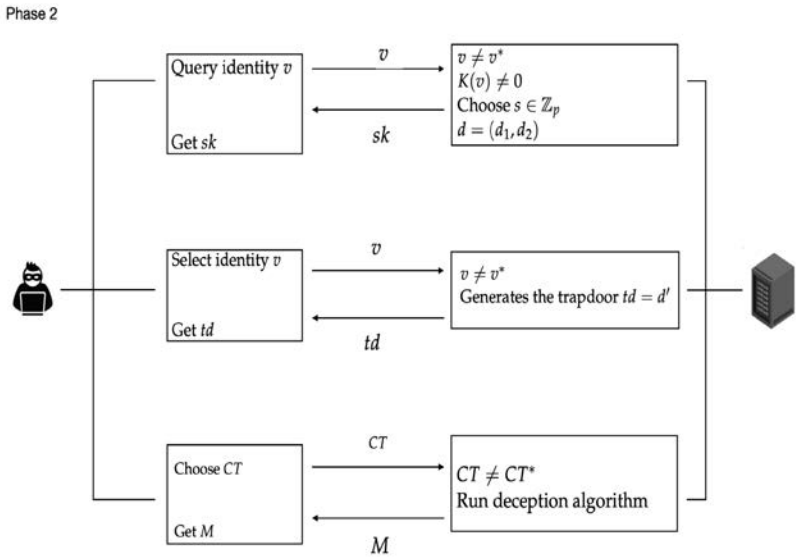

FIGURE 12. Phase 2 of Game 2.

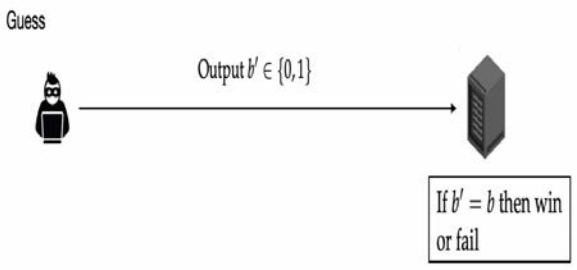

FIGURE 13. Guess of Game 2.

value $g_1 = g^\alpha$ and select g_2 randomly in $\mathbb{G}_1$. Additionally, the authority chooses a random value $u' \in \mathbb{G}_1$ and a random n-length vector $U = (u_i)$, whose elements are chosen at random from $\mathbb{G}_1$. The algorithm outputs the public key $pk = \langle g, g_1, g_2, u', U \rangle$. The master secret are g_1^α and g_2^α.

Key Generation(pk, msk) Let v be an n bitstring representing an identity, v_i denotes the ith bit of v, and $v \subseteq \{1, \ldots, n\}$ be the set of all i for which $v_i = 1$. (That is V is the set of f indices for which the bit string v is set to 1.) Secret key $sk = (d, d')$. First, choose two numbers $(s, s') \in \mathbb{Z}_p^2$. Then the secret key is constructed as follows:

$$d' = \left(g_1^\alpha (u' \prod_{i \in v} u_i)^s, g^s\right) \qquad d = \left(g_2^\alpha (u' \prod_{i \in v} u_i)^{s'}, g^{s'}\right)$$

Let $d' = (d_1', d_2')$, $d = (d_1, d_2)$.

Encrypt(pk, M) The message $M \in \mathbb{G}_1$ is encrypted for an identity v as follows. Three numbers $(r_1, r_2, r_3) \in \mathbb{Z}_p^3$ are selected as random. Set the ciphertext $CT = (C_1, C_2, C_3)$ to be

$$C_1 = g^{r_1} \qquad C_2 = \left(M^{r_1} e(g_1, g_2)^{r_2}, g^{r_2}, \left(u' \prod_{i \in v} u_i\right)^{r_2}\right)$$

$$C_3 = \left((M||r_1) e(g_1, g_2)^{r_3}, g^{r_3}, \left(u' \prod_{i \in v} u_i\right)^{r_3}\right)$$

Decrypt(CT, sk) Let $C_2 = (C_2^1, C_2^2, C_2^3)$ and $C_3 = (C_3^1, C_3^2, C_3^3)$. To decrypt C using the secret key $sk = (d', d)$,

$$\begin{aligned} & C_3^1 \frac{e(d_2, C_3^3)}{e(d_1, C_3^2)} \\ &= \left((M||r_1)e(g_1, g_2)^{r_3}\right) \frac{e\left(g^{s'}, \left(u' \prod_{i\in v} u_i\right)^{r_3}\right)}{e\left(g_2^{\alpha}\left(u' \prod_{i\in v} u_i\right)^{s'}, g^{r_3}\right)} \\ &= \left((M||r_1)e(g_1, g_2)^{r_3}\right) \frac{e\left(g^{s'}, \left(u' \prod_{i\in v} u_i\right)^{r_3}\right)}{e(g_1, g_2)^{r_3} e\left(g^{s'}, \left(u' \prod_{i\in v} u_i\right)^{r_3}\right)} \\ &= M||r_1 \end{aligned} \tag{1}$$

and it outputs M if the following equalities hold.

$$C_1 = g^{r_1} \qquad C_2^1 \frac{e(d_2', C_2^3)}{e(d_1', C_2^2)} = M^{r_1}$$

The authorization and test algorithm:

To decide whether $M_A = M_B$ assume A and B as two user in the system. $CT_A = (C_{1A}, C_{2A}, C_{3A}) = Encrypt(M_A, pk_A)$ is ciphertext from A and $C_{2A} = (C_{2A}^1, C_{2A}^2, C_{2A}^3)$, $CT_B = (C_{1B}, C_{2B}, C_{3B}) = Encrypt(M_B, pk_B)$ is ciphertext from B and $C_{2B} = (C_{2B}^1, C_{2B}^2, C_{2B}^3)$.

- Authorization algorithm(Auth):
  For A, the trapdoor is $td_A = (d_{1A}', d_{2A}')$;
  For B, the trapdoor is $td_B = (d_{1B}', d_{2B}')$;
- Test algorithm(Test):
  The algorithm computes:

$$X_A = C_{2A}^1 \frac{e(d_{2A}', C_{2A}^3)}{e(d_{1A}', C_{2A}^2)}$$

$$X_B = C_{2B}^1 \frac{e(d_{2B}', C_{2B}^3)}{e(d_{1B}', C_{2B}^2)}$$

  While X_A, C_{1A} and X_B, C_{1B} are used to check the following:

$$e(C_{1B}, X_A) = e(C_{1A}, X_B).$$

If $M_A = M_B$ then it outputs 1, otherwise 0.

Theorem 1: The above IBEwET-S scheme satisfies the consistency property.

Proof: We now show that the three conditions are satisfied.

- For the first condition, it is straightforward to be verified.
- For the second condition, assuming the ciphertexts are well-formed for v_A and v_B:

$$e(C_{1,A}, X_B) = e(g^{r_{1,A}}, M_B^{r_{1,B}}) = e(g, M_B)^{r_{1,A} r_{1,B}}$$
$$e(C_{1,B}, X_A) = e(g^{r_{1,B}}, M_A^{r_{1,A}}) = e(g, M_A)^{r_{1,B} r_{1,A}}$$

  If $M_A = M_B$, then $e(C_{1,A}, X_B) = e(C_{1,B}, X_A)$. So the test algorithm outputs 1 as desired.
- For the third condition, for any $M_A \neq M_B$, it means that $e(g, M_B)^{r_{1,A} r_{1,B}} \neq e(g, M_A)^{r_{1,A} r_{1,B}}$. Then, Test $(CT_A, td_{vA}, CT_B, td_{vB}) = 0$, we claim that $\Pr[\text{Test}(CT_A, td_{vA}, CT_B, td_{vB}) = 1]$ is negligible.

VII. SECURITY ANALYSIS

Now, we prove the security of the proposed scheme.

Theorem 2: The proposed scheme is OW-ID-CCA secure, assuming the DBDH assumption holds to the Type-1 adversary.

Proof: Suppose there exists an adversary, A_1, against our scheme. We construct a simulator, $\mathcal{B}$, to play the DBDH game. The simulator takes DBDH challenge$(g, A = g^a, B = g^b, C = g^c, Z)$ and outputs a guess, M', as to whether the challenge is a DBDH tuple.

The simulator runs the game executing the following steps.

- The setup algorithm is shown in Fig.4. The simulator outputs pk to A_1.
- The Phase 1 queries are shown in Fig.5. A_1 can perform the following queries, such as the sk of v, decryption, trapdoor queries.
- The challenge is shown in Fig.6. After phase 1, A_1 picks v^* randomly to the simulator, and the simulator outputs CT^* to A_1.
- This step is similar to phase 1, in Phase 2, just some restrictions as shown in Fig.7. Here, $v \neq v^*$ and $CT \neq CT^*$.
- Finally, A_1 outputs a guess M' as in Fig.8.

Theorem 3: Our scheme is IND-ID-CCA secure, assuming the DBDH assumption holds to the Type-2 adversary.

Proof: Suppose there exists an adversary, A_2, against our scheme. We construct a simulator, $\mathcal{B}$, to play the DBDH game. The simulator takes DBDH challenge$(g, A = g^a, B = g^b, C = g^c, Z)$ and outputs a guess, b', as to whether the challenge is a DBDH tuple.

The simulator runs the game executing the following steps.

- The setup algorithm is shown in Fig.9. The simulator outputs pk to A_2.
- The phase 1 queries are shown in Fig.10. A_2 can perform the following queries, such as the sk of v, decryption, trapdoor queries.
- The challenge is shown in Fig.11. After phase 1, A_2 picks v^* and $M_0, M_1 \in \mathbb{G}_1$ randomly to the simulator, and the simulator outputs CT^* to A_2.
- This step is similar to phase 1, just some restrictions as shown in Fig.12. Here, $v \neq v^*$ in key and trapdoor queries, in decryption queries $CT \neq CT^*$.
- Finally, A_2 outputs a guess b' as in Fig.13.

Theorem 4: If the simulator takes $O(\epsilon^{-2} ln(\epsilon^{-1})\lambda^{-1} ln(\lambda^{-1}))$ samples when computing the estimate η', then $(\frac{1}{2} + \epsilon)\Pr[\overline{\text{abort}}|\gamma' = \gamma] - (\frac{1}{2} - \epsilon)\Pr[\overline{\text{abort}}|\gamma' = \gamma] \geq \frac{3}{2}\lambda\epsilon($ a lower bound $\lambda = \frac{1}{8(n+1)q})$.

Detailed proof of Theorem 4 is in reference [22].

VIII. PERFORMANCE ANALYSIS

In Table 1, the comparison of IBEwET-S scheme with some related schemes is detailed. The comparison is performed with respect to 8 aspects including encryption algorithm, decryption algorithm, test algorithm, supporting test algorithm, two types of security levels, random oracle and

TABLE 1. The comparison of computational complexity.

Scheme	C_{Enc}	C_{Dec}	C_{Test}	Test	OW-CCA	IND-CCA	ROM	Stand
[13]	5Exp	2Exp	2Exp+2P	√	√	√	√	-
[18]	7Exp+2P	Exp+P	2Exp+4P	√	√	√	√	-
[19]	2Exp+4P	2Exp+2P	-	-	√	√	-	√
[20]	6Exp	2Exp+2P	4P	√	√	-	√	-
[21]	nExp	(n+1)P	-	-	√	√	-	√
[22]	2Exp+2P	Exp+P	-	-	-	√	-	√
[23]	6Exp	5Exp	2Exp+2P	√	√	-	√	-
[24]	(n+2)Exp+2P	Exp+(n+1)P	nP	√	√	-	√	-
[25]	5Exp+P	4Exp+P	2Exp+4p	√	√	√	√	-
ours	4Exp+2P	2Exp+2P	4P	√	√	√	-	√

Note: C_{Enc}: computational complexity of encryption algorithm, C_{Dec}: decryption complexity of decryption algorithm, C_{Test}: the computational complexity of the test algorithm, Test: supporting equality test, Exp: exponential operation, P: pairing operation, Rom: random oracle model, Stand: the standard model

standard models. The number of operations are counted from exponential and bilinear pairing operations in encryption, decryption and test algorithms. The first column depicts the references of comparison schemes (including ours). The second to fourth columns show the computational costs in terms of encryption, decryption and testing algorithms. The fifth column indicates whether the scheme supports the test algorithm, and the sixth to seventh columns indicate the security level that the scheme achieves. The eighth and ninth columns show that the schemes are safe under the random oracle model or standard model.

IX. CONCLUSION

In this paper, we propose a new scheme of IBEwET-S based on the IBEET scheme which is proven secure in standard model. The comparison depict that the proposed sheme has a higher security profile. More precisely, the proposed scheme combines the test algorithms to enable flexible authorization equality testing in ciphertext. The scheme achieves security level of OW/IND-ID-CCA, which can be directional if the adversary is given a trapdoor, and indistinguishable if the adversary does not get a trapdoor. Currently, several schemes have proved to be secured and offer testing algorithms in the standard model, however, fewer schemes are applied to practice. We claim that the proposed scheme is more practical as proved by comparative anlysis, hence, it can be applied to more scenarios.

REFERENCES

[1] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, "Probabilistic public key encryption with equality test," in *Proc. Cryptographers Track RSA Conf. (CT-RSA)*, San Francisco, CA, USA. Berlin, Germany: Springer, Mar. 2010, Art. no. 119131.

[2] H. T. Lee, S. Ling, J. H. Seo, and H. Wang, "CCA2 attack and modification of Huang et al.'s public key encryption with authorized equality test," *Comput. J.*, vol. 59, no. 11, pp. 1689–1694, Nov. 2016.

[3] M. Nateghizad, Z. Erkin, and R. L. Lagendijk, "Efficient and secure equality tests," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2016, pp. 1–6.

[4] Y. Wang, H. Pang, N. H. Tran, and R. H. Deng, "CCA secure encryption supporting authorized equality test on ciphertexts in standard model and its applications," *Inf. Sci.*, vol. 414, pp. 289–305, Nov. 2017.

[5] L. Wu, Y. Zhang, K.-K.-R. Choo, and D. He, "Efficient and secure identity-based encryption scheme with equality test in cloud computing," *Future Gener. Comput. Syst.*, vol. 73, pp. 22–31, Aug. 2017.

[6] X.-J. Lin, L. Sun, and H. Qu, "Generic construction of public key encryption, identity-based encryption and signcryption with equality test," *Inf. Sci.*, vol. 453, pp. 111–126, Jul. 2018.

[7] T. K. Saha and T. Koshiba, "Outsourcing private equality tests to the cloud," *J. Inf. Secur. Appl.*, vol. 43, pp. 83–98, Dec. 2018.

[8] H. Qu, Z. Yan, X.-J. Lin, Q. Zhang, and L. Sun, "Certificateless public key encryption with equality test," *Inf. Sci.*, vol. 462, pp. 76–92, Sep. 2018.

[9] M. Zeng, J. Chen, K. Zhang, and H. Qian, "Public key encryption with equality test via hash proof system," *Theor. Comput. Sci.*, vol. 795, pp. 20–35, Nov. 2019.

[10] L. Wu, Y. Zhang, K.-K.-R. Choo, and D. He, "Pairing-free identity-based encryption with authorized equality test in online social networks," *Int. J. Found. Comput. Sci.*, vol. 30, no. 4, pp. 647–664, Jun. 2019.

[11] H. Li, Q. Huang, S. Ma, J. Shen, and W. Susilo, "Authorized equality test on identity-based ciphertexts for secret data sharing via cloud storage," *IEEE Access*, vol. 7, pp. 25409–25421, 2019.

[12] K. Zhang, J. Chen, H. T. Lee, H. Qian, and H. Wang, "Efficient public key encryption with equality test in the standard model," *Theor. Comput. Sci.*, vol. 755, pp. 65–80, Jan. 2019.

[13] Y. Ling, S. Ma, Q. Huang, X. Li, and Y. Ling, "Group public key encryption with equality test against offline message recovery attack," *Inf. Sci.*, vol. 510, no. 4, pp. 16–32, Feb. 2020.

[14] A. Hassan, Y. Wang, R. Elhabob, N. Eltayieb, and F. Li, "An efficient certificateless public key encryption scheme with authorized equality test in healthcare environments," *J. Syst. Archit.*, vol. 109, Oct. 2020, Art. no. 101776.

[15] R. Elhabob, Y. Zhao, A. Hassan, and H. Xiong, "PKE-ET-HS: Public key encryption with equality test for heterogeneous systems in IoT," *Wireless Pers. Commun.*, vol. 113, no. 1, pp. 313–335, Jul. 2020.

[16] X.-J. Lin, Q. Wang, L. Sun, and H. Qu, "Identity-based encryption with equality test and datestamp-based authorization mechanism," *Theor. Comput. Sci.*, vol. 861, pp. 117–132, Mar. 2021.

[17] X. Shen, B. Wang, L. Wang, P. Duan, and B. Zhang, "Group public key encryption supporting equality test without bilinear pairings," *Inf. Sci.*, vol. 605, pp. 202–224, Aug. 2022.

[18] H. Zhu, Q. Xue, T. Li, and D. Xie, "Traceable scheme of public key encryption with equality test," *Entropy*, vol. 24, no. 3, p. 309, Feb. 2022.

[19] C. Gentry, "Practical identity-based encryption without random oracles," in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, St. Petersburg, Russia. Berlin, Germany: Springer, May/Jun. 2006, pp. 445–464.

[20] S. Ma, "Identity-based encryption with outsourced equality test in cloud computing," *Inf. Sci.*, vol. 328, pp. 389–402, Jan. 2016.

[21] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Proc. Crypto*, vol. 3152, 2004, pp. 443–459.

[22] B. R. Waters, "Efficient identity-based encryption without random oracles," in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Aarhus, Denmark. Berlin, Germany: Springer, May 2005, pp. 114–127.

[23] S. Ma, Q. Huang, M. Zhang, and B. Yang, "Efficient public key encryption with equality test supporting flexible authorization," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 458–470, Mar. 2015.

[24] Y. Ming and E. Wang, "Identity-based encryption with filtered equality test for smart city applications," *Sensors*, vol. 19, no. 14, p. 3046, Jul. 2019.

[25] S. Ma, M. Zhang, Q. Huang, and B. Yang, "Public key encryption with delegated equality test in a multi-user setting," *Comput. J.*, vol. 58, no. 4, pp. 986–1002, Apr. 2015.
[26] H. Hong and Z. Sun, "Constructing conditional PKEET with verification mechanism for data privacy protection in intelligent systems," *J. Supercomput.*, Apr. 2023, doi: 10.1007/s11227-023-05253-9.

HUIJUN ZHU received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2018. She is currently an Associate Professor with the Nanyang Institute of Technology. Her research interests include modern cryptography, network security, and cloud computing.

HASEEB AHMAD received the B.S. degree from Government College University Faisalabad, Pakistan, in 2010, the master's degree from the Virtual University of Pakistan, in 2012, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2017. He is currently an Assistant Professor with the Department of Computer Science, National Textile University, Faisalabad. His current research interests include data mining, information retrieval, and information security.

QINGJI XUE received the Ph.D. degree in computer science and technology from the Wuhan University of Technology, in 2000. He is currently a Full Professor with the Nanyang Institute of Technology. His research interests include artificial intelligence, big data analytic, and image processing.

TIANFENG LI received the Ph.D. degree in computer science from the Huazhong University of Sciences and Technology, in 2008. He is currently an Associate Professor with the Nanyang Institute of Technology. His research interests include digital media technology and graphic processing.

ZIYU LIU is the bachelor's student at the Nanyang Institute of Technology. His research interests include modern cryptography and network security.

AO LIU is the bachelor's student at the Nanyang Institute of Technology. His research interests include modern cryptography and network security.