RESEARCH ARTICLE

Certificateless Encryption Supporting Equality Test with Cryptographic Reverse Firewalls in Smart City

Rashad Elhabob[1], Ahmed Elkhalil[3], Abdalla Hadabi[4,5], Mazin Taha[2], Negalign Wake Hundera[2] and Nabeil Eltayieb[1,*]

[1] College of Computer Science and Information Technology, Karary University, Omdurman, Sudan
[2] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[3] Qilu Institute of Technology, Jinan 250202, China
[4] Yibin Research Institute, Southwest Jiaotong University, Yibin 644000, China
[5] School of Computing and Artificial Intelligence, Southwest Jiaotong University, Chengdu 611756, China

Abstract

In the context of smart cities, sensors are pivotal for the collection and analysis of health data within smart healthcare systems. Despite their importance, securing this data for cloud storage poses significant challenges, particularly in terms of data searchability and encryption. Our paper introduces a novel solution, namely certificateless encryption supporting equality test with cryptographic reverse firewalls (CLE-ET-CRF). This protocol allows cloud servers to perform equality tests on encrypted data without compromising its confidentiality, effectively mitigating risks like offline message recovery attacks (OMRA) and algorithm substitution attacks (ASAs). By eliminating the need for traditional certificate management and addressing key escrow concerns, CLE-ET-CRF provides a secure, efficient, and privacy-preserving mechanism for managing healthcare data in smart city ecosystems. Our evaluation confirms that the protocol meets the high standards required for privacy and efficiency in smart healthcare applications.

Keywords: equality test, searchable encryption, smart healthcare, certificateless, cloud server, CRF.

1 Introduction

The rapid development of smart cities has significantly increased both the variety and volume of consumer electronic devices, which play a crucial role in shaping modern urban environments [1, 2]. This rapid expansion has introduced a vast array of sensors, ranging from individual wearable devices to interconnected networks of sensors and smart gadgets, fundamentally transforming convenience, automation, and efficiency across numerous industries and applications [3, 4].

These technological innovations in consumer electronics are at the core of advancing urban

Submitted: 17 December 2025
Accepted: 24 March 2026
Published: 30 March 2026

Vol. 2, **No.** 1, 2026.
10.62762/JRSC.2025.581803

***Corresponding author:**
✉ Nabeil Eltayieb
nabeil9@yahoo.com

Citation
Elhabob, R., Elkhalil, A., Hadabi, A., Taha, M., Hundera, N. W.,& Eltayieb, N. (2026). Certificateless Encryption Supporting Equality Test with Cryptographic Reverse Firewalls in Smart City. *Journal of Reliable and Secure Computing*, 2(1), 66–82.

living by enhancing multiple sectors, including economic development, education, healthcare, and overall quality of life. As illustrated in Figure 1, the integration of these smart devices contributes to creating intelligent and responsive city infrastructures that aim to streamline daily operations and improve the standard of living. Smart cities leverage these advancements to optimize energy consumption, traffic management, public services, and security, demonstrating their far-reaching impact beyond personal convenience.

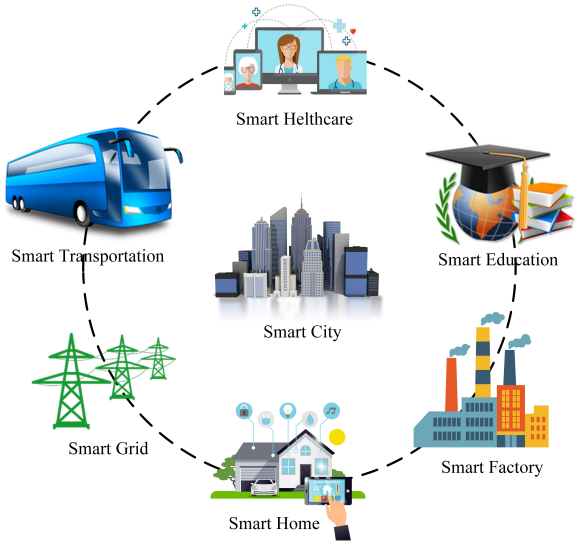

Figure 1. Smart city applications.

Among the various applications of smart technology, the healthcare sector has emerged as one of the most critical areas benefiting from sensor-based innovations. The implementation of wearable health monitors, remote patient monitoring systems, and IoT-enabled medical devices has transformed how healthcare services are delivered and accessed [5, 6]. These technological breakthroughs enable real-time health tracking, early disease detection, and more efficient medical interventions, contributing to a more proactive and preventive approach to healthcare. As smart city initiatives continue to evolve, the emphasis on leveraging sensor-based solutions in healthcare remains a primary focus, ensuring improved medical services, enhanced patient care, and a higher degree of personalization in treatment plans.

In the smart healthcare sector, driven by sensors, several challenges persist, including the provision of cost-effective services and the assurance of timely healthcare access in regions faced with geographical and infrastructural constraints [7, 8]. The role of wearable sensor devices in collecting and processing health data before its encryption and subsequent storage on cloud servers is critical [9, 10]. Nonetheless, the necessity to encrypt data due to the untrusted nature of cloud services complicates the searchability of this data, posing a significant hurdle [11, 12].

A Public-Key Encryption scheme with Keyword Search (PKE-KS) was proposed to satisfy particular security and functionality needs, enabling the efficient search of encrypted data without compromising privacy [13]. This scheme enables medical servers to use keywords to search for data [14, 15]. A significant drawback of PKE-KS, however, is that its search functionality is limited to scenarios where both the keyword and the data are encrypted using the same public key. To overcome this limitation, Yang et al. [16] developed a Public-Key Encryption scheme with Equivalence Test (PKE-ET) capability, which enables comparisons between ciphertexts encrypted with different public keys. This PKE-ET depends on traditional public key, which is known as Public Key Infrastructure (PKI) [17], requiring the verification of user public keys via certificates issued by a trusted Certificate Authority (CA). To address the need for certificates in PKI systems, Ma [18] introduced an identity-based encryption with equality test (IBE-ET) scheme, which utilizes user identities as public keys. This approach eliminates the dependency on certificates but introduces new challenges, particularly concerning key escrow issues. Building on this, Qu et al. [19] further developed the approach by combining equality test functionality with certificateless encryption in the CL-PKC-ET scheme, which effectively addresses both certificate management and key escrow issues. This innovation has spurred a succession of successful schemes that incorporate equality test functionality [20–24].

Although the CL-PKC-ET scheme overcomes the challenges of PKI and key escrow present in PKE-ET and IBE-ET schemes, respectively, it remains susceptible to specific cryptographic attacks. For instance, the offline message recovery attacks (OMRA). These attacks resemble the keyword guessing attacks (KGA) encountered in PKE-KS systems. As illustrated in Figure 2, a semi-honest cloud server tries to decrypt a message from the ciphertext C. This process involves encrypting the message with the public key Pk' and then comparing the resulting ciphertext using equality tests. The server uses two trapdoors, TD and TD', to perform the comparison and verify whether the ciphertext corresponds to the intended message. While message distributions are typically considered uniform and infinite, practical weaknesses emerge from

non-uniform distributions and constrained message spaces. To mitigate OMRA, Tang [25] introduced a dual-tester approach that prevents individual testers from independently determining the outcome, albeit at the cost of increased computational and transmission efforts and a remaining risk of collusion. Subsequently, Ling et al. [26] suggested a group-based method that remains susceptible to collusion if a group member and the tester conspire. More recently, IBEET [27] presented an OMRA-resistant framework that implements a novel authorization mechanism via data owner signatures, necessitating a new trapdoor for each test and thereby elevating computational demands.

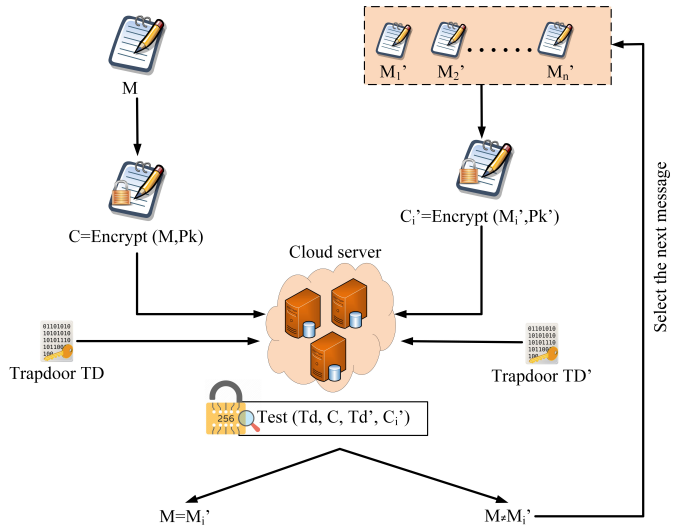

Figure 2. A typical scenario for OMRA.

Another notable obstacle for PKE-ET schemes is the exfiltration attack, demonstrated by the Snowden incident, reveals how insider attackers can extract confidential information from compromised algorithms. This episode underscored the capacity of entities like the National Security Agency (NSA) to harvest vast quantities of sensitive data by leveraging vulnerabilities in encryption systems or backdoors within cryptographic protocols [28]. In 2014, Bellare et al. [29] investigated the Algorithm Substitution Attack (ASA), an exfiltration technique where adversaries stealthily extract user messages by substituting the encryption algorithm. In 2015, Mironov et al. [30] introduced cryptographic reverse firewalls (CRF), ensuring the security of cryptographic protocols even on compromised systems and preventing secret data disclosure from tampered computers.

1.1 Motivation and contribution

To address the OMRA and ASA challenges, our work introduces the certificateless encryption supporting equality test with cryptographic reverse firewalls (CLE-ET-CRF) tailored for smart healthcare systems enhanced by sensors. The distinct advantages and innovations of the CLE-ET-CRF scheme, especially in the context of wearable sensors in smart healthcare, are detailed further in this paper.

1. Our proposed protocol integrates the equality test concept with cryptographic reverse firewalls, resulting in the CLE-ET-CRF. This scheme enables a cloud server to conduct equivalence tests on two distinct ciphertexts.

2. We have developed three distinct CRFs within our CLE-ET-CRF scheme, strategically deployed across three key components: the key generation center (KGC), the patient, and the doctor. This design ensures robust protection of the private key, encrypted messages, and trapdoors, safeguarding them against potential compromises.

3. Our CLE-ET-CRF scheme has been rigorously evaluated in the random oracle model, demonstrating its compliance with OW-CCA security and IND-CCA security.

4. Through experimental simulation and analysis, we have verified that our CLE-ET-CRF scheme optimally suits for smart healthcare systems.

1.2 Related Works

In the modern digital era, wearable sensors like smartphones and smartwatches are becoming integral components of our daily lives [38]. These devices, particularly in the healthcare domain, are central to the collection and cloud-based storage of patient data, making them indispensable for enhancing healthcare services [39]. However, one of the key challenges in this context is the difficulty of efficiently searching through the vast amounts of data generated by these sensors. This creates barriers to easy access and analysis of critical health information [40].

The concept of searchable encryption, which allows data to be retrieved without needing to decrypt it first, was first introduced by Song et al. [31]. While this foundational approach made strides in enabling secure data retrieval, it faced limitations, particularly when it came to uploading encrypted content and facilitating search functionalities. Building on these initial ideas, Boneh et al. [13] proposed a framework that integrated

Table 1. Properties of different works.

Schemes	KS	ET	CMP	KEP	OMRA	ASA	Security Type-1	Security Type-2	Assumption	Cryptosystem
[13]	✓	×	×	✓	×	×	OW-CCA	IND-CCA	BDH	PKI-based
[18]	✓	✓	✓	×	×	×	OW-ID-CCA	IND-ID-CCA	BDH	ID-based
[32]	✓	✓	×	✓	×	×	OW-CCA	IND-CCA	CDH	PKI-based
[21]	✓	✓	✓	×	×	×	OW-CCA	IND-CCA	DBDH	PKI-based
[33]	✓	✓	✓	×	×	×	OW-ID-CCA	IND-ID-CCA	BDH	ID-based
[34]	✓	✓	×	×	×	×	OW-CCA2	IND-CCA2	BDHIP	PKI&ID-based
[35]	✓	✓	×	×	×	×	OW-CCA2	IND-CCA2	q-SDHP	PKI&ID-based
[36]	✓	✓	✓	✓	×	×	OW-CCA	IND-CCA	BDH	CLC-based
CLE-ET-CRF	✓	✓	✓	✓	✓	✓	OW-CCA	IND-CCA	BDH	CLC-based

keyword searches within public key encryption systems. However, their approach still relied on the PKI system, which introduced complexities in managing certificates.

The focus then shifted to identity-based encryption (IBE) systems, which offered an alternative approach and allowed for the outsourcing of equality tests, marking a significant step forward in addressing some of the challenges associated with PKI systems [18, 33]. This transition was part of a broader effort to address the limitations posed by traditional PKI setups. In subsequent years, significant progress was made in the area of heterogeneous cryptosystems. Researchers like Xiong et al. [34], Fazrina et al. [35] and Hou et al. [41] advanced the integration of equality tests across various cryptographic environments, broadening their applicability to wireless networks. Despite these advancements, the problem of key escrow remained a persistent issue. To address this, Qu et al. [36] and Qu et al. [19] proposed certificateless public key encryption with equality test (CL-PKE-ET), which aimed to mitigate the key escrow problem inherent in traditional public key systems.

The importance of enhancing security measures became even more apparent following the Snowden revelations, which exposed the vulnerabilities in existing cryptographic methods. In response, Mironov et al. [30] introduced the concept of Cryptographic Reverse Firewalls (CRFs), designed to alter client communications in ways that protect against internal threats. This laid the foundation for Zhou et al. [42], who developed the first CRF protocol for searchable public key encryption (SPKE-CRF), marking a critical step in the ongoing effort to defend against Algorithm Substitution Attacks (ASAs).

Despite the progress made in integrating certificateless public key encryption with equality tests and CRFs for comparing encrypted keywords across different public keys, this combination, especially in the context of the post-Snowden landscape, has yet to be explored in existing literature. This gap highlights the need for further research into novel cryptographic solutions that can address these emerging security challenges.

Table 1 delineates a comparison between the CLE-ET-CRF scheme and other existing schemes, highlighting their approaches to various encryption challenges. Abbreviations such as KS for keyword searchable encryption, ET for equality test, CMP for certificate management, KEP for key escrow, OMRA for offline message recovery attacks, and ASA for algorithm substitution attacks, are used to denote the solutions provided by each scheme to these specific issues. Additionally, BDH, DBDH, BDHIP, and q-SDHP stand for the bilinear Diffie-Hellman assumption, Decisional bilinear Diffie-Hellman assumption, Bilinear Diffie–Hellman Inversion Problem, and q-Strong Diffie–Hellman problem, respectively. In this context, a ✓ indicates that the scheme effectively addresses the specified property, while × signifies that the property is not accommodated in the scheme's design.

2 DEFINITION

2.1 Properties of Bilinear Maps

Consider $\mathbb{G}_1$ and $\mathbb{G}_2$, two cyclic groups of prime order p, with g serving as a generator for $\mathbb{G}_1$. We define a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ that exhibits the following characteristics:

- **Bilinearity Property**: For any elements $g_1, g_2 \in \mathbb{G}_1$ and scalars $x, y \in \mathbb{Z}_p^*$, it holds that $e(g_1^x, g_2^y) = e(g_1, g_2)^{xy}$.
- **Non-degeneracy**: If g_1, g_2 are any elements of $\mathbb{G}_1$, then $e(g_1, g_2)$ is always distinct from the identity element of $\mathbb{G}_2$.
- **Efficient Computability**: For every pair of elements g_1 and g_2 in $\mathbb{G}_1$, there exists an effective computational method to determine $e(g_1, g_2)$.

2.2 Bilinear Diffie-Hellman (BDH) Problem

Under the BDH assumption, consider a, b, c as random elements in $\mathbb{Z}_p^*$. The conjecture posits that for any efficient algorithm $\mathcal{A}$, distinguishing the tuple $< g^a, g^b, g^c, e(g,g)^{abc} >$ from $< g^a, g^b, g^c, e(g,g) >$ represents a challenging problem, with $\mathcal{A}$ achieving only a negligible success rate.

2.3 Cryptographic Reverse Firewall (CRFs)

The CRF is envisioned as a dynamic algorithm, symbolized by S. It functions by processing two inputs: its existing state and a new message. Based on these inputs, it produces two outputs: a refreshed state and a modified message. To maintain clarity in this description, the detailed state representation of S is deliberately omitted. Now, consider delineating the CRF S alongside a participant $X = (receive, next, output)$ in the subsequent framework:

$$\begin{aligned} S \circ X := (&Receive_{S\circ X} := Receive_X(\gamma, S(m)),\\ &Next_{S\circ X}(\gamma) = S(Next_X(\gamma)),\\ &Output_{S\circ X}(\gamma) = Output_X(\gamma)). \end{aligned}$$

Consider a situation where a message m is sent together with an initial public parameter γ. The following are the key attributes that the compliant constrained randomized functions should exhibit:

1. Maintaining Functionality: Suppose S, X, Y, Z represent a CRF, a participant, a protocol, and a function, respectively. For any polynomially bounded $\lambda \geq 1$:
   - We can say S preserves Z for X in Y if $S^\lambda \circ X$.
   - We can say S preserved functionality if X, Y, and Z are obvious.

   Note that, $S \circ (S^{\lambda-1} \circ X)$.
2. Preserving Security: Assume that W denotes a security requirement. It is determined that:
   - S maintains W for X in Y if $Y_{X \Rightarrow S\circ X^*}$ fulfills W. If X, Y, and W are obvious, S deserves highly security.
   - S maintains W for X in Y against Z-maintaining adversaries if $Y_{X \Rightarrow S\circ X^*}$ fulfills W. If X, Y, Z, and W are obvious, S deserves weakly security.

   Note that X^* is denoted to the functionality-preserving adversarial implementation, and $Y_{X \Rightarrow S\circ X^*}$ is denoted to the replacing x with $S \circ X^*$.
3. Resisting Exfiltration: It is established that:
   - If no adversary can compromise the game $Game(X, Y, S, \lambda)$, then S may be said to exhibit robust non-disclosure for participant X within protocol Y.
   - If no adversary can break the game $Game(X, X', X^*, S, \lambda)$, then S can be characterized as providing constrained non-disclosure protection for X' against X^* in the context of Y.

2.4 Definition of CLE-ET-CRF

The CLE-ET-CRF framework, an equality test on certificateless cryptography with cryptographic reverse firewalls, consists of the following essential algorithms:

1. **Setup:** Executed by the KGC, this procedure accepts the security parameter λ to generate the public parameters P_{pub} along with a master secret key.
2. **Re-Setup:** After obtaining P_{pub} from the KGC, the KGC's CRF re-randomizes the P_{pub} and issues ${P_{pub}}'$.
3. **Partial-Secret-Key-Extract:** Conducted by the KGC, this operation takes P_{pub}, a master secret key, and a user's public identity $ID \in \{0,1\}^*$ as inputs and delivers a partial secret key D.
4. **KGC-KeyMaul:** Following the receipt of a user's partial secret key D by the KGC's CRF, it re-randomizes D and returns D'.
5. **Set-Secret-Value:** This function, which is managed and executed by the user, takes the public parameters P'_{pub} and the identifier ID to compute and generate a unique secret value x, which is used in subsequent cryptographic operations.
6. **Full-Secret-Key-Extract:** Initiated by the user, this algorithm leverages the public parameters P'_{pub}, a derived value D', and the previously generated secret value x to compute the user's full secret key sk, enabling access to the corresponding encrypted data.
7. **Trapdoor:** This procedure utilizes the secret key sk as an input to compute and produce a corresponding trapdoor TD, which serves as a crucial component for secure data retrieval or verification.

8. **Trapdoor-KeyMaul:** Identified as a modified **Trapdoor** process, this algorithm re-randomizes a received trapdoor TD and outputs a modified trapdoor TD'.
9. **Public-Key-Extract:** Performed by the user, this involves inputting P'_{pub} and sk to obtain the user's public key pk.
10. **Encrypt:** This function takes P'_{pub}, a plaintext M, and pk to produce an encrypted message C.
11. **Encrypt-KeyMaul:** A modified version of the **Encrypt** process, this algorithm re-randomizes a received ciphertext C, resulting in a modified C'.
12. **Decrypt:** It takes P'_{pub} , C', and sk as inputs to decrypt and return the message M; it returns $\perp$ for unsuccessful decryption attempts.
13. **Test:** This algorithm tests for equality of encrypted messages between users U_i and U_j.

2.5 System Model

The system model of our proposed protocol, depicted in Figure 3, consists of six principal components:

1. Patient: Sensitive data collected by sensors are encrypted and uploaded to the cloud server. For data retrieval, the patient utilizes a trapdoor via his CRF.
2. Doctor: Assumes the role of monitoring patients and accessing encrypted data on the cloud server using a trapdoor through his CRF.
3. KGC: The KGC is responsible for generating unique private keys for participants, such as patients and doctors, based on their respective identities. This ensures that each participant has a distinct cryptographic key pair, which is used for secure communication and authentication within the system.
4. KGC CRF: Manages the modification of public parameters and private keys for privacy, ensuring these alterations do not interfere with the cloud server's operations.
5. CRFs of patient and doctor: Re-randomize data for privacy before it's sent to the cloud server, without affecting encryption, decryption, or testing functionalities.
6. Cloud server: Acts as a semi-trusted entity for data storage and test execution, maintaining privacy while providing results to the doctor.

2.6 Security Model

In this subsection, we ensure the security of the CLE-ET-CRF scheme through a detailed analysis targeting four specific types of adversarial threats, characterized below:

1. **Type-I Adversary:** Represented as $\mathcal{A}_1$, this adversary does not have access to the master secret key (msk), but it has the ability to replace public keys with its own. The security of CLE-ET-CRF against this adversary is evaluated under the OW-CCA, ensuring that the system remains resistant to unauthorized decryption attempts and mitigates the risk posed by the adversary's ability to manipulate public keys.
2. **Type-II Adversary:** Denoted as $\mathcal{A}_2$, it possesses the msk but lacks the ability to modify public keys of other users. The CLE-ET-CRF's security in this scenario is also evaluated using the OW-CCA framework to verify the system's resilience against adversarial decryption.
3. **Type-III Adversary:** Identified as $\mathcal{A}_3$, it does not possess the msk but can actively request and manipulate public keys. To assess security under these conditions, CLE-ET-CRF is examined using the IND-CCA, which measures the system's ability to prevent adversaries from distinguishing encrypted messages.
4. **Type-IV Adversary:** Labeled as $\mathcal{A}_4$, it possesses the msk but is restricted from altering any user's public keys. The security evaluation of CLE-ET-CRF against this adversary ensures that possessing the master secret key alone does not compromise confidentiality or system integrity.

Definition 1: This states that $\mathcal{A}_1$ and $\mathcal{A}_2$ are designated as **Type-I** and **Type-II** adversaries, respectively. Our analysis is centered around two specific games, **Game 1** and **Game 2**, in which both adversaries engage with a designated Challenger. It is important to note that the Challenger keeps a detailed log of all queries and responses while interacting with these adversaries.

Game 1: The engagement between the adversary $\mathcal{A}_1$ and the challenger unfolds through the following sequence of exchanges:

1. **Setup:** The Challenger initiates this phase by generating the public parameters, noted as P'_{pub}, and the msk.
2. **Phase 1:** This phase includes a series of requests that $\mathcal{A}_1$ can make:

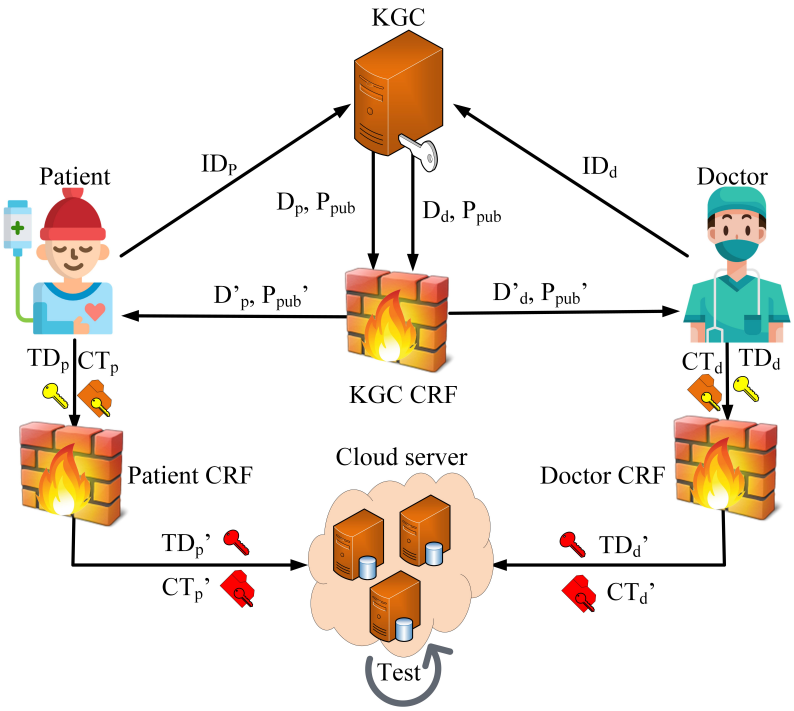

Figure 3. System model.

- *Partial-Secret-Key-Extract queries:* For each query received, the Challenger runs the **Partial-Secret-Key-Extract** to produce D, and executes the **KGC-KeyMaul** to get the re-randomized D', which is then delivered to $\mathcal{A}_1$.
- *Full-Secret-Key-Extract queries:* Upon receiving these queries, the Challenger performs the **Full-Secret-Key-Extract** algorithm to generate sk', and forwards it to $\mathcal{A}_1$.
- *Public-Key-Extract queries:* Each query prompts the Challenger to execute the **Public-Key-Extract** algorithm, resulting in pk, which is handed to $\mathcal{A}_1$.
- *Replace-public-key queries:* $\mathcal{A}_1$ is permitted to replace a public key pk with a new one at any point.
- *Decryption queries:* The Challenger carries out the **Decrypt** algorithm using sk' associated with ID. Subsequently, the decrypted message M from re-randomized ciphertext C' is given to $\mathcal{A}_1$.
- *Trapdoor queries:* The Challenger runs the **Trapdoor** algorithm to create TD, and executes the **Trapdoor-KeyMaul** to get the re-randomized TD'. Eventually, the Challenger passes TD' to $\mathcal{A}_1$.

3. **Challenge:** At this stage, the challenger randomly chooses a message M from the string $\{0,1\}^{n_1}$ and performs encryption, resulting in the ciphertext $C^* =$ **Encrypt**(ID^*, M). The adversary $\mathcal{A}_1$ then receives C^* as the challenge ciphertext.

Here's a revised version with more clarity and expansion:

4. **Phase 2:** In this phase, the challenger engages with $\mathcal{A}_1$ following the same procedures outlined in **Phase 1**, but with additional restrictions to maintain the integrity of the game and prevent any unfair advantage:
   - The challenge identity ID^* must not be involved in any *Full-Secret-Key-Extract queries*, ensuring that the adversary cannot directly extract the full private key associated with ID^*.
   - If the public key corresponding to ID^* is replaced, ID^* must be excluded from any *Public-Key-Extract queries*. This restriction prevents the adversary from obtaining sensitive information regarding the replaced public key.
   - In the event that a user's public key is replaced, the identity ID associated with the new key must be excluded from all

Public-Key-Extract queries. This ensures that the adversary cannot gain access to public keys that may have been altered during the game.

- Any *Decryption queries* that inquire about the pair (ID^*, C^*) are prohibited. This is to prevent the adversary from querying the challenge ciphertext C^* with the challenge identity ID^*, which could reveal information about the encrypted message.

5. **Phase 2:** During this phase, the challenger interacts with $\mathcal{A}_1$ using the same procedures as in **Phase 1**, but adhering to specific restrictions:
   - The challenge identity ID^* is not to be used in any *Full-Secret-Key-Extract queries*.
   - Should the public key associated with ID^* be replaced, ID^* must not be used in any *Public-Key-Extract queries*.
   - In instances where a public key of the user is replaced, the identical ID must be excluded from all *Public-Key-Extract queries*.
   - *Decryption queries* must exclude any inquiries related to the pair (ID^*, C^*).
6. **Guess:** $\mathcal{A}_1$ submits a guess M^*. The adversary is deemed successful if M^* matches the original plaintext M.

Game 2: The engagement between $\mathcal{A}_2$ and the challenger proceeds below:

1. **Setup:** The challenger executes the appropriate algorithm to generate the public parameters, denoted as P'_{pub}, along with the *msk*.
2. **Phase 1:** $\mathcal{A}_2$ initiates queries following the procedure outlined in **Game 1**, but is restricted from performing *Partial-Secret-Key-Extract queries* and *Replace-public-key queries* during this phase.
3. **Challenge:** In this phase, the challenger randomly selects a message M from $\{0,1\}^{n_1}$ and encrypts it, resulting in the ciphertext $C^* = \textbf{Encrypt}(ID^*, M)$. This ciphertext C^* is then provided to $\mathcal{A}_2$ as the challenge ciphertext.
4. **Phase 2:** In this phase, the challenger replies to $\mathcal{A}_2$ using the same procedures as in **Phase 1**, with constraints:
   - The challenge identity, denoted by ID^*, is excluded from *Full-Secret-Key-Extract queries*.
   - *Decryption queries* must avoid any inquiries concerning the (ID^*, C^*) pair .
5. **Guess:** $\mathcal{A}_2$ makes a guess, outputting M^*. Success is defined as M^* matching M.

The advantage of $\mathcal{A}_i$ in Game$_i$, where $i \in \{1,2\}$, is quantified as follows:

$$\textbf{Adv}^{OW-CCA,Game_i}_{CL-PKE-ET,\mathcal{A}_i}(\lambda) = \Pr[M^* = M].$$

Definition 2: Defines $\mathcal{A}_3$ and $\mathcal{A}_4$ as adversaries categorized as **Type-III** and **Type-IV**, respectively. Our analysis includes two different games, **Game 3** and **Game 4**, where $\mathcal{A}_3$ and $\mathcal{A}_4$ interact with a dedicated Challenger. It is crucial to note that the Challenger meticulously documents all queries and responses throughout these interactions.

Game 3: The engagement between $\mathcal{A}_3$ and the challenger follows this structured sequence:

1. **Setup:** The challenger executes the appropriate algorithm to generate the P'_{pub}, along with the *msk*.
2. **Phase 1:** $\mathcal{A}_3$ proceeds by making queries in line with the steps and procedures established in **Game 1**, adhering to the defined rules for interaction with the challenger and the system.
3. **Challenge:** The adversary $\mathcal{A}_3$ selects two plaintext messages, M_0 and M_1, from the set $\{0,1\}^{n_1}$, ensuring they are of the same length. The challenger then randomly picks a bit $b \in \{0,1\}$ and encrypts the chosen plaintext M_b using the **Encrypt** function along with the identifier ID^*. The resulting ciphertext, C_b, is given to $\mathcal{A}_3$ as the challenge ciphertext.
4. **Phase 2:** The challenger continues responding to $\mathcal{A}_3$ following the same approach as in **Phase 1**, subject to the following conditions:
   - Any *Set-Private-Key-queries* must exclude the challenge identity ID^*.
   - The public key linked to ID^* is altered or replaced, it is imperative that ID^* is not utilized in any *Full-Secret-Key-Extract queries*, ensuring that the integrity of the key extraction process remains intact and secure.
   - If a public key the user is replaced, the associated identity ID must be exempt from all *Full-Secret-Key-Extract queries*.

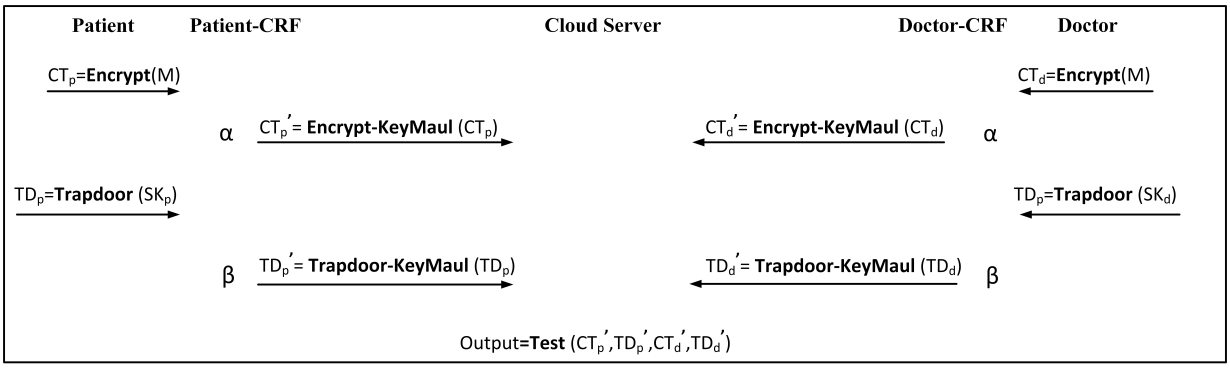

Figure 4. A basic CLE-ET-CRF protocol.

- *Decryption queries* are prohibited from addressing the combination of ID^* and C_b.
- *Trapdoor queries* must not involve querying ID^*.

5. **Guess:** $\mathcal{A}_3$ submits a guess b^*, aiming to match it with the original bit b. Success is confirmed if b^* equals b.

Game 4: The interaction between $\mathcal{A}_4$ and the challenger is detailed below:

1. **Setup:** The challenger executes the appropriate algorithm to generate the P'_{pub}, along with the *msk*.
2. **Phase 1:** $\mathcal{A}_4$ begins by initiating queries according to the protocol defined in **Game 1**, with the restriction that it is not allowed to perform *Extract-Partial-Private-Key queries* or *Replace-public-key queries* as outlined in **Game 4**.
3. **Challenge:** $\mathcal{A}_4$ submits two messages, M_0 and M_1, both of equal length and drawn from the set $\{0,1\}^{n_1}$. Then, the challenger picks a bit b from $\{0,1\}$ randomly and encrypts the chosen plaintext M_b using the **Encrypt** function with ID^*. The resulting ciphertext, C_b, is provided to $\mathcal{A}_4$.
4. **Phase 2:** The challenger continues interacting with $\mathcal{A}_4$ using the established procedures from **Phase 1**, but with the following specific conditions:
   - The challenge identity, ID^*, must be excluded from all *Full-Secret-Key-Extract queries* to prevent any unauthorized access to the secret key associated with the challenge.
   - *Decryption queries* should not include any requests involving the pair (ID^*, C_b), ensuring that no decryption attempts are made with the challenge identity and its corresponding ciphertext.
   - Inquiries involving ID^* in *Trapdoor queries* are prohibited.
5. **Guess:** $\mathcal{A}_4$ predicts a bit b', and success is achieved if and only if b^* matches the bit b originally selected by the challenger.

The advantage of $\mathcal{A}_i$ in Game_i, where $i \in \{3,4\}$, is quantified as follows:

$$\mathbf{Adv}^{IND-CCA,Game_i}_{CL-PKE-ET,\mathcal{A}_i}(\lambda) = \Pr[b^* = b].$$

3 CONSTRUCTION

The CLE-ET-CRF scheme is designed to merge functionalities from CRFs and CLE-ET, outlined as follows (see Figure 4):

1. **Setup:** The KGC operates under the following protocol upon receiving a security parameter λ:
   (a) It begins by generating two prime order groups $\mathbb{G}_1$ and $\mathbb{G}_2$, and defines a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. A random element g from $\mathbb{G}_1$ is selected as the generator.
   (b) Next, it establishes four hash functions: $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \to \mathbb{Z}^*_p$, $H_3 : \mathbb{G}_2 \to \{0,1\}^{n_1+n_2}$, and $H_4 : \{0,1\}^* \to \mathbb{Z}^*_p$, where n_1 and n_2 denote the sizes of $\mathbb{G}_1$ and $\mathbb{Z}^*_p$, respectively.
   (c) The KGC then randomly selects s_1 and s_2 from $\mathbb{Z}^*_p$, and computes $g_1 = g^{s_1}$ and $g_2 = g^{s_2}$.
   (d) Finally, the KGC disseminates the public parameters $P_{pub} = \langle p, \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, H_1, H_2, H_3, H_4 \rangle$ to its CRF.
2. **Re-Setup:** Upon receipt P_{pub} from KGC, the KGC's CRF selects a random element ψ from $\mathbb{Z}^*_p$. Then, it proceeds to compute $g'_1 = g_1^{\psi}$ and

$g_2' = g_2^{\psi}$. Subsequently, the updated $P_{pub}' = \langle p, \mathbb{G}_1, \mathbb{G}_2, e, g, g_1', g_2', H_1, H_2, H_3, H_4 \rangle$ and made available to the public.

3. **Partial-Secret-Key-Extract:** For any given identity ID belonging to the set $\{0,1\}^*$, it calculates $h_{ID} = H_1(ID)$, then derives the partial secret key D as a pair $(D_1, D_2) = (h_{ID}^{s_1}, h_{ID}^{s_2})$.

4. **KGC-KeyMaul:** Upon the CRF of the KGC receiving a user's partial secret key D, the CRF updates the user's partial secret key to $D' = (D_1', D_2') = (h_{ID}^{\psi s_1}, h_{ID}^{\psi s_2})$. Subsequently, the KGC forwards D' to the respective user.

5. **Set-Secret-Value:** It operates with $P_{pub}{}'$ and D' as inputs. Then, a random selection of x from $\mathbb{Z}_p^*$ is made, subsequently designating x as the secret value.

6. **Full-Secret-Key-Extract:** Given $P_{pub}{}'$, D', and x, the algorithm calculates the full secret key $sk = (sk_1, sk_2) = (D_1'^{x}, D_2'^{x})$

7. **Trapdoor:** It takes as input sk then produces a trapdoor $TD = sk_1 = h_{ID}^{x\psi s_1}$ as output.

8. **Trapdoor-KeyMaul:** This algorithm is recognized as a re-randomized **Trapdoor** algorithm. Upon receipt of the trapdoor TD by the user's CRF, it selects β and α from $\mathbb{Z}_p^*$, ensuring $\beta\alpha = 1 \mod p$. Subsequently, the CRF computes a re-randomized trapdoor $TD' = TD^{\beta} = h_{ID}^{\beta x \psi s_1}$, which is then sent to the cloud server.

9. **Public-Key-Extract:** upon receiving inputs $P_{pub}{}'$ and x, computes $pk = (X, pk_1, pk_2) = (g^x, g_1'^{x}, g_2'^{x})$ as public key.

10. **Encrypt:** Given a message $M \in \{0,1\}^{n_1}$, an identity ID, and a public key $pk = (X, pk_1, pk_2)$, the following steps are carried out:

    (a) Compute $h_{ID} = H_1(ID) \in \mathbb{G}_1$.

    (b) Choose random $(r_1, r_2) \in \mathbb{Z}_p^*$.

    (c) Set $C_1 = g^{r_1}$ and $C_2 = g^{r_2}$.

    (d) Compute $C_3 = (m \cdot r_2) \cdot H_2(e(h_{ID}, pk_1)^{r_1})$, where $m = H_4(M)$.

    (e) Compute $C_4 = (M \parallel r_2) \oplus H_3(e(h_{ID}, pk_2)^{r_1})$.

    Note: $e(h_{ID}, pk_1)$ and $e(h_{ID}, pk_2)$ should be pre-computed.

11. **Encrypt-KeyMaul:** This algorithm is a re-randomized **Encrypt** algorithm. Upon the CRF of the user receives the ciphertext C, it calculates $C' = (C_1', C_2, C_3, C_4) = (C_1^{\alpha}, C_2, C_3, C_4)$. Finally, the user's CRF sends the C' to the cloud server.

12. **Decrypt:** Before receiving a ciphertext C', the user's CRF first calculates $C_1 = (C_1')^{\beta}$, then the algorithm calculates $M \parallel r_2 = C_4 \oplus H_3(e(sk_2, C_1))$. After that, validate that both $C_2 = g^{r_2}$ and $\frac{C_3}{(H_4(M)\cdot r_2)} = H_2(e(sk_1, C_1))$ hold true. If valid, return M; else, output $\perp$.

13. **Test:** For two users U_i and U_j in the system, denote their ciphertexts as C_i' and C_j', respectively. The **Test** performs as follows.

$$
\begin{aligned}
m_i \cdot r_{i,2} &= \frac{C_{i,3}}{H_2(e(TD_i', C_{i,1}'))} \\
&= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}^{x\beta_i\psi s_1}, C_{i,1}^{\alpha_i}))} \\
&= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}^{x\psi s_1}, g^{r_{i,1}}))} \\
&= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}, g^{x\psi s_1})^{r_{i,1}})} \\
&= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})} \\
&= m_i \cdot r_{i,2}.
\end{aligned}
$$

The analysis previously conducted confirms that $\frac{C_{j,3}}{H_2(e(TD_j', C_{j,1}'))} = m_j \cdot r_{j,2}$. An algorithm designed for this purpose will return a value of 1 when $(C_{i,2})^{m_j \cdot r_{j,2}} = (C_{j,2})^{m_i \cdot r_{i,2}}$. Otherwise, it outputs 0.

4 Security analysis

Theorem 1. *The CLE-ET-CRF protocol we propose is a one-way identity-based encryption scheme, ensuring that our scheme achieves both OW-CCA and IND-CCA security. Additionally, the CRFs for both the KGC and users remain functional, offer weak security preservation, and provide weak resistance against exfiltration, assuming that the basic CL-PKE scheme [37] is secure under the OW-CCA and IND-CCA conditions.*

Proof. In this section, we provide a detailed demonstration that our framework maintains the following key properties, ensuring its effectiveness and security in various scenarios:

1. *Preservation of Functionality:* Verifying the functionality of our approach is straightforward. For example, when users U_i and U_j encrypt their

messages and transmit them to the cloud, the server then performs the following operation:

$$\begin{aligned} m_i \cdot r_{i,2} &= \frac{C_{i,3}}{H_2(e(TD'_i, C'_{i,1}))} \\ &= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}^{x\beta_i\psi s_1}, C_{i,1}^{\alpha_i}))} \\ &= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}^{x\psi s_1}, g^{r_{i,1}}))} \\ &= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}, g^{x\psi s_1})^{r_{i,1}})} \\ &= \frac{m_i \cdot r_{i,2} \cdot H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})}{H_2(e(h_{ID,i}, pk_{i,1})^{r_{i,1}})} \\ &= m_i \cdot r_{i,2}. \end{aligned}$$

The analysis previously conducted confirms that $\frac{C_{j,3}}{H_2(e(TD'_j, C'_{j,1}))} = m_j \cdot r_{j,2}$. An algorithm designed for this purpose will return a value of 1 when $(C_{i,2})^{m_j \cdot r_{j,2}} = (C_{j,2})^{m_i \cdot r_{i,2}}$. Otherwise, it outputs 0.

Hence, it is apparent that implementing CRFs does not hinder the capacity of the cloud server to perform equality tests and ascertain the correct outcomes.

2. *Weak Security Preservation and Weak Exfiltration Resistance:* We confirm the OW-CCA and IND-CCA security of our protocol, even with tampered algorithms, by demonstrating the indistinguishability between the security games of our CLE-ET-CRF and the foundational CL-PKE scheme by Al-Riyami and Paterson [37]. We briefly detail the OW-CCA and IND-CCA secure games for our CLE-ET-CRF in relation to Al-Riyami and Paterson's scheme, highlighting key similarities and distinctions from the games described in subsection 2.6:

   - Initially, the challenger runs the **Setup** algorithm with a security parameter λ to create public parameters P_{pub}. This is followed by the **KGC-KeyMaul** step, where P_{pub} is altered to P'_{pub}.
   - *Partial-Secret-Key-Extract queries:* An adversary chooses an identity ID. The challenger begins by running the **Partial-Secret-Key-Extract** algorithm to derive a user's partial private key D. The **KGC-KeyMaul** is then employed to modify D into D', which is subsequently provided to the adversary.
   - *Trapdoor queries:* The Challenger executes the **Trapdoor** algorithm to generate TD, then applies the **Trapdoor-KeyMaul** to produce the re-randomized TD'. This modified trapdoor is then handed over to $\mathcal{A}_1$.

   We then outline a series of progressively modified security games to further analyze and establish the robustness of our cryptographic protocol:

   - *Game 0:* This game is consistent with the OW-CCA-CRF and IND-CCA-CRF security games as initially described. It uses the current configurations and operations from the security model to test the protocol's resistance to both types of cryptographic attacks.
   - *Game 1:* This game is similar to *Game 0*, with the primary difference being that P_{pub} is obtained directly using the *Setup* algorithm rather than the *Re-Setup* algorithm during the setup stage. This modification tests the impact of using initial setup parameters without additional re-randomization.
   - *Game 2:* This game follows *Game 1*, but modifies the method by which the user's partial secret key D is generated. In this game, D is created directly by the **Partial-Secret-Key-Extract** algorithm instead of being re-randomized by the **KGC-KeyMaul** algorithm during both *Phase 1* and *Phase 2*. This tests the security implications of removing an additional layer of key mauling.
   - *Game 3:* Similar to *Game 2*, but with the trapdoor TD being generated using the *Trapdoor* algorithm rather than the **Trapdoor-KeyMaul** algorithm during both *Phase 1* and *Phase 2*. This game assesses the effects of direct trapdoor generation on the protocol's overall security, especially concerning the integrity and confidentiality of the communication.

   These games aim to dissect the security layers of our protocol, identifying any potential weaknesses introduced by each stage of the cryptographic process and demonstrating the inherent security offered by the initial cryptographic design.

We methodically demonstrate the indistinguishability between each consecutive pair of games, providing

robust proof of the security of our cryptographic protocol. Here is how we analyze each transition:

1. **Transition from Game 0 to Game 1:**
   - Despite modifications to the **Setup** algorithm, the application of the KGC's CRF through **Re-Setup** ensures that P'_{pub} remains uniformly random. This is akin to the outcomes generated by the standard **Re-Setup** process.
   - As a result, there is no discernible difference between the public parameters in both games, rendering **Game 0** and **Game 1** indistinguishable.
2. **Transition from Game 1 to Game 2:**
   - In this transition, while the generation of the user's partial secret key D changes, the KGC's CRF still processes this key post-extraction. The re-randomization by **KGC-KeyMaul** ensures that D' is uniformly random, mirroring the malleability inherent in the cryptographic process.
   - This uniform randomness in the processed keys makes the direct extraction in **Game 1** and the mauling in **Game 2** indistinguishable from an adversary.
3. **Transition from Game 2 to Game 3:**
   - Any changes to the **Trapdoor** algorithm are offset by the subsequent application of the user's CRF **Trapdoor-KeyMaul** processing.
   - Thus, despite the internal algorithmic changes, the result remains consistent, affirming the indistinguishability between **Game 2** and **Game 3**.

These transitions establish that the modifications between games do not introduce observable differences to an adversary, maintaining the protocol's security across changes. Since Al-Riyami and Paterson's basic CL-PKE scheme is known to achieve OW-CCA and IND-CCA security, our CLE-ET-CRF protocol, following these principles and processes, inherently meets the same security standards.

The analysis confirms that from **Game 0** through **Game 3**, there is a solid defense mechanism in place against both intrusion and data exfiltration. This comprehensive demonstration finalizes our proof, establishing the proposed CLE-ET-CRF as a secure and robust encryption framework capable of maintaining high-security standards even under potential adversarial challenges.

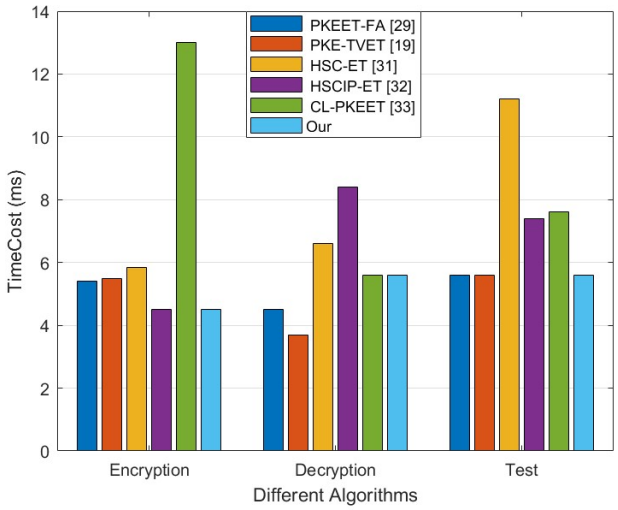

Figure 5. Comparison of computation cost.

5 Performance Evaluation

The following part is organized into two distinct subsections: the first discusses the computational cost efficiencies of the proposed scheme, highlighting its performance improvements. The second subsection focuses on the advantages related to energy consumption, emphasizing how the scheme contributes to reducing power usage.

5.1 Computational Cost

To achieve an 80-bit security level in pairing-based cryptography, the supersingular elliptic curve $E : y^2 + y = x^3 + x$ is employed over the finite field $\mathbb{F}_{2271}$. This curve is chosen due to its embedding degree of 4, which provides the necessary security strength for the intended cryptographic applications. The Eta pairing is identified as the fastest for achieving the 80-bit security level [43]. Research by [44] and [45] indicates that on the MICA2 platform, the pairing computation requires 1.90 seconds, and point multiplication takes 0.81 seconds at this security level. The MICA2 platform is built on the ATmega128 8-bit microcontroller, which utilizes the AVR architecture. It is equipped with 4KB of RAM for temporary data storage and 128KB of FLASH memory for program storage. According to Shim et al. [46], the platform takes around 0.9 seconds to complete exponentiation operations, highlighting the processing time involved for such cryptographic computations on this device.

In our analysis of computational costs, we focus

Table 2. Performance comparison of communication and computational costs.

Schemes	Communication cost		Computational cost		
	PK	CT	Enc	Dec	Test
PKEET-FA [32]	$3\|\mathbb{G}_1\|$	$5\|\mathbb{G}_1\|+\|\mathbb{Z}_p\|$	$6T_e$	$5T_e$	$2T_e$+$2T_p$
PKE-TVET [21]	$2\|\mathbb{G}_1\|$+$\|\mathbb{G}_2\|$	$3\|\mathbb{G}_1\|$+$2\|\mathbb{G}_2\|$	$4T_e$+T_p	$2T_e$+T_p	$2T_e$+$2T_p$
HSC-ET [34]	$3\|\mathbb{G}_1\|$+$\|\mathbb{G}_2\|$	$3\|\mathbb{G}_1\|$+$2\|\mathbb{Z}_p\|$	$2T_e$+$5T_m$	T_e+$3T_p$	$4T_e$+$4T_p$
HSCIP-ET [35]	$2\|\mathbb{G}_1\|$	$4\|\mathbb{G}_1\|$+$2\|\mathbb{Z}_p\|$	$5T_e$	$3T_e$+$3T_p$	$4T_e$+$2T_p$
CL-PKEET [36]	$2\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\|+\|\mathbb{G}_2\|$	$6T_e$+$4T_p$	$2T_e$+$2T_p$	$4T_p$
Our	$3\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\|+\|\mathbb{Z}_p\|$	$5T_e$	$2T_e$+$2T_p$	$2T_e$+$2T_p$

Legends: PK represents public key size; CT indicates ciphertext size; Enc, Dec, and Test are computational costs for encryption, decryption, and testing, respectively.

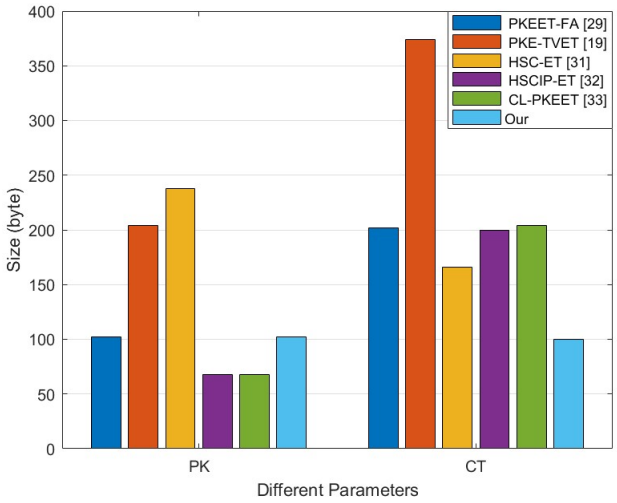

Figure 6. Comparison of communication cost.

solely on the pairing operation, point multiplication, and exponentiation in $\mathbb{G}_1$. Costs associated with arithmetic operations and hash functions are excluded due to their minimal significance compared to the aforementioned operations. A detailed comparison of the computational and communication costs of our scheme relative to established methods was also conducted, including PKEET-FA [32], PKE-TVET [21], HSC-ET [34], HSCIP-ET [35], and CL-PKEET [36], as depicted in Table 2. Execution times, measured in milliseconds, are graphically presented in Figure 5. Our scheme consistently outperforms the others in terms of encryption and testing costs. In the aspect of decryption, while our scheme shows lower costs compared to HSC-ET [34] and HSCIP-ET [35], it remains equal to CL-PKEET [36] and higher than those of PKEET-FA [32] and PKE-TVET [21]. Figure 6 demonstrates that our scheme also shows a reduced communication cost regarding ciphertext size. Concerning public key size, our scheme is smaller than PKE-TVET [21] and HSC-ET [34], equivalent to PKEET-FA [32], and slightly larger than HSCIP-ET [35] and CL-PKEET [36].

5.2 Energy Consumption

In this subsection, we provide an in-depth comparison of our proposed scheme against established schemes such as PKEET-FA [32], PKE-TVET [21], HSC-ET [34], HSCIP-ET [35], and CL-PKEET [36], focusing particularly on energy consumption metrics. The MICA2 platform serves as the basis for our simulation, characterized by a power specification of 3.0 V, a transmitting current of 27 mA, a receiving current of 10 mA, an active mode current of 8.0 mA, and a data rate of 12.4 kb/s [47]. We provide comprehensive details on energy utilization for both computational and communication activities.

5.2.1 *Energy for Computation*

The formula $R = K \times L \times T$ is employed to calculate energy consumption, where R measures the power consumption in millijoules (mJ), K is the voltage of the platform, L refers to the current draw in active mode in milliamps (mA), and T represents the duration in seconds (s) [48]. As noted in [46] and [49], the energy consumption during the computation process is exhaustively detailed for PKEET-FA [32], PKE-TVET [21], HSC-ET [34], HSCIP-ET [35], CL-PKEET [36], and our proposed scheme as follows: $3.0 \times 8.0 \times (13 \times 0.9 + 2 \times 1.9) = 372$ mJ, $3.0 \times 8.0 \times (8 \times 0.9 + 4 \times 1.9) = 355.2$ mJ, $3.0 \times 8.0 \times (7 \times 0.9 + 5 \times 0.81 + 7 \times 1.9) = 567.6$ mJ, $3.0 \times 8.0 \times (12 \times 0.9 + 5 \times 1.9) = 487.2$ mJ, $3.0 \times 8.0 \times (8 \times 0.9 + 10 \times 1.9) = 628.8$ mJ, and $3.0 \times 8.0 \times (9 \times 0.9 + 4 \times 1.9) = 376.8$ mJ, respectively.

5.2.2 *Energy of Communication*

The public key and ciphertext sizes produced by different schemes are analyzed, as these sizes are directly related to energy consumption. It is assumed that the element sizes in $\mathbb{Z}_p$, $\mathbb{G}_1$, and $\mathbb{G}_2$ are 32 bytes, 34 bytes, and 136 bytes respectively [46]. The sizes of the public key and ciphertext for our proposed scheme and other schemes are as follows.

1. PKEET-FA [32]: $3 \times |\mathbb{G}_1| + 3 \times |\mathbb{G}_1| + 3 \times |\mathbb{Z}_P| =$

Table 3. Energy consumption on MICA2.

Schemes	Energy of computation	Energy of communication	Total of energy consumption (mJ)
PKEET-FA [32]	372	15.89	387.89
PKE-TVET [21]	355.2	30.21	385.41
HSC-ET [34]	567.6	21.11	588.71
HSCIP-ET [35]	487.2	14.01	501.21
CL-PKEET [36]	628.8	14.21	643.01
Our	376.8	10.56	387.36

$8 \times 34 + 32 = 304$ bytes.

2. PKE-TVET [21]: $\times|\mathbb{G}_1| + 3 \times |\mathbb{G}_2| = 5 \times 34 + 3 \times 136 = 578$ bytes.
3. HSC-ET [34]: $6 \times |\mathbb{G}_1| + 1 \times |\mathbb{G}_2| + 2 \times |\mathbb{Z}_P| = 6 \times 34 + 136 + 2 \times 32 = 404$ bytes.
4. HSCIP-ET [35]: $6 \times |\mathbb{G}_1| + 2 \times |\mathbb{Z}_P| = 6 \times 34 + 2 \times 32 = 268$ bytes.
5. CL-PKEET [36]: $4 \times |\mathbb{G}_1| + 1 \times |\mathbb{G}_2| = 4 \times 34 + 136 = 272$ bytes.
6. Our: $5 \times |\mathbb{G}_1| + 1 \times |\mathbb{Z}_P| = 5 \times 34 + 32 = 202$ bytes.

The energy consumption of request/response messages is determined using the formula $R = K \times Y \times Z \times (8/W)$, where Y represents the current draw in transmitting mode, Z is the data size in bytes, and W is the data rate of the platform [48]. Detailed energy consumption figures for PKEET-FA [32], PKE-TVET [21], HSC-ET [34], HSCIP-ET [35], CL-PKEET [36], and our proposed scheme are meticulously documented as follows: $3.0 \times 27 \times 304 \times (8/12400) = 15.89$ mJ, $3.0 \times 27 \times 578 \times (8/12400) = 30.21$ mJ, $3.0 \times 27 \times 404 \times (8/12400) = 21.11$ mJ, $3.0 \times 27 \times 268 \times (8/12400) = 14.01$ mJ, $3.0 \times 27 \times 272 \times (8/12400) = 14.21$ mJ, and $3.0 \times 27 \times 202 \times (8/12400) = 10.56$ mJ, respectively.

Table 3 and Figure 7 illustrate the energy consumption. As shown in Figure 7, our proposed scheme consumes less energy compared to other related schemes.

As demonstrated in Tables 2 and 3, the computation cost, communication cost, and total energy consumption of our proposed scheme are comparable to those of other schemes, such as PKEET-FA [32], PKE-TVET [21], HSC-ET [34], HSCIP-ET [35], and CL-PKEET [36]. However, our scheme uniquely addresses vulnerabilities related to OMRA and ASA by incorporating a CRF, thereby enhancing both its robustness and security. Additionally, it effectively resolves challenges associated with certificate management and key escrow. Therefore, our proposed scheme offers greater security and includes additional features.

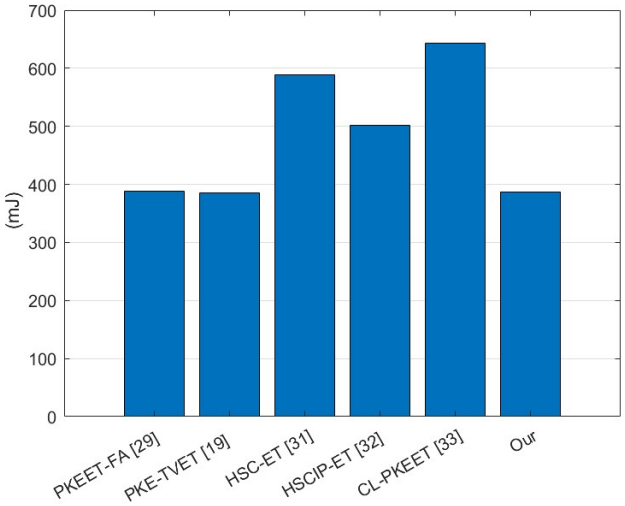

Figure 7. Total of energy consumption.

6 Conclusion

This paper presents the CLE-ET-CRF protocol, a significant enhancement to smart cities and cryptographic security sectors. The integration of CRFs notably strengthens the scheme's capability to counteract OMRA and ASA. This enhancement establishes a robust and secure framework for the efficient storage and retrieval of data on cloud servers, crucial for the integrity of such systems. Furthermore, the scheme effectively resolves prevalent issues in certificate management and key escrow, critical elements in maintaining user trust and data security. This advancement is particularly vital for the protection of sensitive healthcare data processed by consumer electronic devices. Looking ahead, we outline our plans to further extend the CRF methodology to address more complex security threats in attribute-based encryption (ABE) schemes, especially within frameworks that perform equality tests. This future work aims to refine and broaden the applicability of our scheme, enhancing its utility in securing advanced cryptographic applications.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Lopez Martinez, A., Gil Pérez, M., & Ruiz-Martínez, A. (2023). A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. *ACM Computing Surveys, 55*(12), 1-38. [CrossRef]

[2] Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2020). I-AREOR: An energy-balanced clustering protocol for implementing green IoT in smart cities. *Sustainable cities and society, 61*, 102254. [CrossRef]

[3] Zovko, K., Šerić, L., Perković, T., Belani, H., & Šolić, P. (2023). IoT and health monitoring wearable devices as enabling technologies for sustainable enhancement of life quality in smart environments. *Journal of Cleaner Production, 413*, 137506. [CrossRef]

[4] Vishnupriya, G., Anusha, S., & Kayikci, S. (2024). An efficient and secure wearable sensor based remote healthcare monitoring system using adaptive dilated transformer Bi-LSTM with gated recurrent unit. *Transactions on Emerging Telecommunications Technologies, 35*(2), e4932. [CrossRef]

[5] Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things, 22*, 100721. [CrossRef]

[6] Elhabob, R., Eltayieb, N., Xiong, H., Khan, F., Bashir, A. K., Kumari, S., ... & Kumar, S. (2024). Equality test public key encryption with cryptographic reverse firewalls for cloud-based E-commerce. *IEEE Transactions on Consumer Electronics, 70*(4), 6763-6775. [CrossRef]

[7] Khan, S., Khan, M., Khan, M. A., Khan, M. A., Wang, L., & Wu, K. (2025). A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. *IEEE Journal of Biomedical and Health Informatics*. [CrossRef]

[8] Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022, October). IoT-based healthcare-monitoring system towards improving quality of life: A review. *Healthcare, 10*(10), 1993. [CrossRef]

[9] Mei, Q., Yang, M., Chen, J., Wang, L., & Xiong, H. (2022). Expressive data sharing and self-controlled fine-grained data deletion in cloud-assisted IoT. *IEEE Transactions on Dependable and Secure Computing, 20*(3), 2625-2640. [CrossRef]

[10] Fong, B., Kim, H., & Sai, V. (2023). Consumer healthcare technologies in smart cities. *IEEE Consumer Electronics Magazine, 12*(4), 63-65. [CrossRef]

[11] Wang, L., Lin, Y., Yao, T., Xiong, H., & Liang, K. (2023). FABRIC: Fast and secure unbounded cross-system encrypted data sharing in cloud computing. *IEEE Transactions on Dependable and Secure Computing, 20*(6), 5130-5142. [CrossRef]

[12] Elhabob, R., Eltayieb, N., Xiong, H., & Kumari, S. (2024). Equality test on identity-based encryption with cryptographic reverse firewalls for telemedicine systems. *IEEE Internet of Things Journal, 12*(2), 2106-2121. [CrossRef]

[13] Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004, May). Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques* (pp. 506-522). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[14] Xiong, H., Wang, H., Meng, W., & Yeh, K. H. (2023). Attribute-based data sharing scheme with flexible search functionality for cloud-assisted autonomous transportation system. *IEEE Transactions on Industrial Informatics, 19*(11), 10977-10986. [CrossRef]

[15] Zhou, Y., Guo, J., & Li, F. (2020). Certificateless public key encryption with cryptographic reverse firewalls. *Journal of Systems Architecture, 109*, 101754. [CrossRef]

[16] Yang, G., Tan, C. H., Huang, Q., & Wong, D. S. (2010, March). Probabilistic public key encryption with equality test. In *Cryptographers' track at the RSA conference* (pp. 119-131). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[17] Lioy, A., Marian, M., Moltchanova, N., & Pala, M. (2006). PKI past, present and future. *International Journal of Information Security, 5*(1), 18-29. [CrossRef]

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

[19] Qu, H., Yan, Z., Lin, X. J., Zhang, Q., & Sun, L. (2018). Certificateless public key encryption with equality test. *Information Sciences, 462*, 76-92. [CrossRef]

[20] Taha, M., Zhong, T., Elhabob, R., Xiong, H., Kumari, S., Chen, C. M., & Alenazi, M. J. (2025). Identity-based

searchable encryption with cryptographic reverse firewalls for IoT-based healthcare systems. *Computers and Electrical Engineering, 124*, 110404. [CrossRef]

[21] Zhao, Z., Susilo, W., Wang, B., & Zeng, K. (2023). Public-key encryption with tester verifiable equality test for cloud computing. *IEEE Transactions on Cloud Computing, 11*(4), 3396-3406. [CrossRef]

[22] Xiong, H., Hou, Y., Huang, X., Zhao, Y., & Chen, C. M. (2021). Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs. *IEEE Systems Journal, 16*(2), 2391-2400. [CrossRef]

[23] Zhao, M., Ding, Y., Tang, S., Liang, H., Yang, C., & Wang, H. (2023). Dual-server certificateless public key encryption with authorized equality test for outsourced IoT data. *Journal of Information Security and Applications, 73*, 103441. [CrossRef]

[24] Elhabob, R., Taha, M., Xiong, H., Khan, M. K., Kumari, S., & Chaudhary, P. (2024). Pairing-free certificateless public key encryption with equality test for Internet of Vehicles. *Computers and Electrical Engineering, 116*, 109140. [CrossRef]

[25] Tang, Q. (2012). Public key encryption schemes supporting equality test with authorisation of different granularity. *International journal of applied cryptography, 2*(4), 304-321. [CrossRef]

[26] Ling, Y., Ma, S., Huang, Q., Li, X., & Ling, Y. (2020). Group public key encryption with equality test against offline message recovery attack. *Information Sciences, 510*, 16-32. [CrossRef]

[27] Lu, J., Li, H., Huang, J., Ma, S., Au, M. H. A., & Huang, Q. (2024). An Identity-Based Encryption with Equality Test scheme for healthcare social apps. *Computer Standards & Interfaces, 87*, 103759. [CrossRef]

[28] Tang, Q., & Yung, M. (2017, October). Cliptography: Post-snowden cryptography. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 2615-2616). [CrossRef]

[29] Bellare, M., Paterson, K. G., & Rogaway, P. (2014, August). Security of symmetric encryption against mass surveillance. In *Annual cryptology conference* (pp. 1-19). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[30] Mironov, I., & Stephens-Davidowitz, N. (2015, April). Cryptographic reverse firewalls. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 657-686). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[31] Song, D. X., Wagner, D., & Perrig, A. (2000, May). Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000* (pp. 44-55). IEEE. [CrossRef]

[32] Ma, S., Huang, Q., Zhang, M., & Yang, B. (2014). Efficient public key encryption with equality test supporting flexible authorization. *IEEE Transactions on Information Forensics and Security, 10*(3), 458-470. [CrossRef]

[33] Ma, S., Ye, Z., Huang, Q., & Jiang, C. (2024). Controllable Forward Secure Identity-based Encryption with Equality Test in Privacy-preserving Text Similarity Analysis. *Information Sciences, 662*, 120099. [CrossRef]

[34] Xiong, H., Zhao, Y., Hou, Y., Huang, X., Jin, C., Wang, L., & Kumari, S. (2020). Heterogeneous signcryption with equality test for IIoT environment. *IEEE Internet of Things Journal, 8*(21), 16142-16152. [CrossRef]

[35] Jin, C., Qin, W., Chen, Z., Sun, K., Chen, G., Shan, J., & Chen, L. (2024). Heterogeneous signcryption scheme with equality test from CLC to PKI for IoV. *Computer Communications, 220*, 149-159. [CrossRef]

[36] Qu, Z., Kumari, S., Obaidat, M. S., Alzahrani, B. A., & Xiong, H. (2023). Traceable attribute-based encryption with equality test for cloud enabled e-health system. *IEEE journal of biomedical and health informatics, 28*(9), 5033-5042. [CrossRef]

[37] Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security* (pp. 452-473). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[38] Chen, R., Mu, Y., Yang, G., Susilo, W., Guo, F., & Zhang, M. (2016, November). Cryptographic reverse firewall via malleable smooth projective hash functions. In *International conference on the theory and application of cryptology and information security* (pp. 844-876). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[39] Gupta, S., Chithaluru, P., El Barachi, M., & Kumar, M. (2024). Secure data access using blockchain technology through IoT cloud and fabric environment. *Security and Privacy, 7*(2), e356. [CrossRef]

[40] Hu, B., Chen, Y., Yu, H., Meng, L., & Duan, Z. (2021). Blockchain-enabled data-sharing scheme for consumer IoT applications. *IEEE Consumer Electronics Magazine, 11*(2), 77-87. [CrossRef]

[41] Hou, Y., Huang, X., Chen, Y., Kumar, S., & Xiong, H. (2021). Heterogeneous signcryption scheme supporting equality test from PKI to CLC toward IoT. *Transactions on Emerging Telecommunications Technologies, 32*(8), e4190. [CrossRef]

[42] Zhou, Y., Hu, Z., & Li, F. (2021). Searchable public-key encryption with cryptographic reverse firewalls for cloud storage. *IEEE transactions on cloud computing, 11*(1), 383-396. [CrossRef]

[43] Barreto, P. S., Galbraith, S. D., hÉigeartaigh, C. Ó., & Scott, M. (2007). Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography, 42*(3), 239-271. [CrossRef]

[44] Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer communications, 34*(3), 485-493. [CrossRef]

[45] Gura, N., Patel, A., Wander, A., Eberle, H., &

Shantz, S. C. (2004, August). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *International workshop on cryptographic hardware and embedded systems* (pp. 119-132). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[46] Shim, K. A., Lee, Y. R., & Park, C. M. (2013). EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad Hoc Networks, 11*(1), 182-189. [CrossRef]

[47] Crossbow Technology Inc. (2005). *MICA2 OEM Edition datasheet*. Retrieved from http://www.cmt-gmbh.de/Produkte/WirelessSensorNetworks/Datenblaetter/MICA2_OEM_Edition_Datasheet.pdf

[48] Shim, K. A. (2014). S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks. *Ad Hoc Networks, 19*, 1-8. [CrossRef]

[49] Cao, X., Kou, W., Dang, L., & Zhao, B. (2008). IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. *Computer communications, 31*(4), 659-667. [CrossRef]

Rashad Elhabob received the B.S. degree from Karary University, Sudan, in 2010, the M.Sc. degree from the University of Khartoum, Sudan, in 2014, and the Ph.D. degree in Software Engineering from the University of Electronic Science and Technology of China in 2019. He completed his postdoctoral research at the University of Electronic Science and Technology of China. He is currently an Associate Professor with the Faculty of Computer Science and Information Technology, Karary University, Sudan. His research interests include cryptography and network security.

Ahmed Elkhalil received the B.S. degree in computer engineering and technology in 2014 and the M.S. degree in computer engineering and networks in 2017 from the University of Gezira, Gezira, Sudan. He obtained the Ph.D. degree in computing and artificial intelligence from the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2024. He is currently an Associate Professor with the School of Computer and Information Engineering, Qilu Institute of Technology, China. His research interests include cryptography, network security, secure protocol design, key management, post-quantum cryptography, blockchain, cloud computing, virtualization, and network architecture.

Abdalla Hadabi received the B.S. degree in 2013 from the Faculty of Computer Science and Information Technology at Al-Neelain University in Khartoum, Sudan. In 2014, he obtained a master's degree from the Faculty of Mathematical Science at the University of Khartoum, located in Khartoum, Sudan. He received the Ph.D. degree from the School of Computer Science and Engineering at the University of Electronic Science and Technology of China (UESTC) in 2024. He is currently a postdoctoral fellow at the School of Computing and Artificial Intelligence, Southwest Jiaotong University. His current research interests include cryptography, network security, the Internet of Things, and cloud computing.

Mazin Taha received the B.S. degree in Computer Engineering from Karary University, Sudan, in 2010, the master's degree from the School of Computer Engineering, Al-Zaiem AL-Azhari University, Sudan, in 2018, and the PhD degree from the School of Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2025. His current research interests include cryptography and network security.

Negalign Wake Hundera received the B.S. degree from the Faculty of Engineering and Technology, Jimma University, Jimma, Ethiopia, in 2009, the master's degree from the School of Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2016, and the Ph.D. degree from the School of Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2021. He is currently a Postdoctoral Researcher with the School of Software Engineering, University of Electronic Science and Technology of China. His current research interests include cryptography and network security

Nabeil Eltayieb received a B.S. degree, in 2008 from the Faculty of Computer Science and Information Technology, University of Karary, Khartoum, Sudan. In 2016 received his Master's degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. He received his Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China in 2019. He is currently a Postdoctoral Researcher with the School of Software Engineering, University of Electronic Science and Technology of China, Chengdu, China. His main research interests include public key cryptography, network security, and information security, in particular, secure data sharing in cloud computing.