SN Computer Science (2021) 2:52
https://doi.org/10.1007/s42979-020-00436-0

ORIGINAL RESEARCH

ID-Based Plaintext Checkable Signcryption with Equality Test in Healthcare Systems

Seth Alornyo[1] · **Mustapha Adamu Mohammed**[1] · **Bright Selorm Anibrika**[1] · **Michael Asante**[2]

Received: 29 October 2020 / Accepted: 22 December 2020
© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. part of Springer Nature 2021

Abstract
This work is an extension of a research work presented at ICSIoT 2019. A suggested cryptographic primitive by Carnard et al. 2012 permits the checkability of a plaintext to a ciphertext to determine whether the ciphertext is an encryption of the plaintext. The proposed construction ensures a public plaintext query to a ciphertext. However, their proposed scheme is susceptible to data forgery and re-play attacks during data transmission. Therefore, we propose an improved scheme to resist data forgery and re-play attacks, and to achieve a simultaneous benefit of digital signature and public key encryption. Our proposed scheme achieves a desirable security property of EUF-CMA via the random oracle model.

Keywords ID-based signcryption · Plaintext checkable signcryption · Equality test

Introduction

According to Ponemon institute's report, healthcare data breach has approximately reached 3.8 million dollars up from 23 percent in 2013. Mostly, this kind of data breach occurs in the United States and Germany. However, this trend of data breach is equally common in developing countries such as Ghana and Nigeria. The healthcare industry has seen a high level of data breach in recent times; therefore, there is the need to protect the privacy of healthcare data.

The scheme at ICSIoT 2019 [1] constructed ID-based checkable plaintext encryption in healthcare database systems. However, plaintext checkable encryption cryptographic primitive first presented by Carnard et al. [2] in CT-RSA-2012 enabled the checkability of plaintext to a ciphertext without revealing the content of the ciphertext. This cryptographic primitive enabled a plaintext check to a corresponding ciphertext without the message content being disclosed to the checker. According to Tables 1 and 2, the user can perform equality check between the plaintext and the ciphertext. The work in [1] enabled a medical keyword check such as 'HIV' whether encrypted or unencrypted. The checkability of encrypted and unencrypted keyword is a remarkable cryptographic tool in plaintext checkable encryption (PCE), since not all keywords need to be encrypted during a search process. However, the search for encrypted or unencrypted keyword during search process has a limitation during data transmission. Thus, their scheme was prone to data forgery and re-play attacks during data transmission and search process. In view of this, we propose an identity-based plaintext checkable signcryption with equality test (ID-PCS-ET) to curtail such vulnerabilities. Thus, our proposed scheme resists data forgery and re-play attacks during data transmission in PKE.

Related Work

A generic construction of identity-based signcryption was proposed in [3]. Their work fulfilled a dual function of digital signature and public key cryptosystem. Other traditional schemes adopted signature-then-encrypt. Digital signature ensures that a message is digitally signed by the sender and the receiver can inverse compute the message to verify the signer of the message, while public key cryptosystem requires a secret key digitally signed and certified by a trusted third party for encrypting/decrypting a message. Schemes that employed signature-then-encrypt had a higher computational cost comparable to the schemes in

✉ Seth Alornyo
sabigseth@ktu.edu.gh

[1] Computer Science Department, Koforidua Technical University (KTU), Koforidua, Ghana

[2] Computer Science Department, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana

Published online: 21 January 2021

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 1 Patients table—plaintext database

S/N	F_{Name}	B_{Day}	$\text{Height}_{(\text{cm})}$	$\text{Weight}_{(\text{Kg})}$
01	Kofi	02-10-1988	165	67
02	Kwame	13-02-19980	170	67
03	Kwasi	10-02-1788	163	61
04	Dan	04-12-1990	180	59

Table 2 Disease table—signcryptext database

S/N	F_{Name}	$\text{Malaria}_{\text{Positives}}$	$\text{Malaria}_{(\text{Negatives})}$	$\text{Viral}_{(\text{Weight})}$
01	dj834hna	0-2948mx	021149sdf	69xv70s
02	900688850	90()-44=	*(*UJS0)	6kjfs7
03	Kwasi	10-02-1788	1w216dsj3	6uwhd1
04	Daskcnwn	0qqas4-1wsl2-1990	1d,lsh8ywsnz0	5bczf[]9

[3] with low computational cost. However, the construction in [3,4] adopted data encapsulation method instead of key encapsulation method compared to [5–7], and their scheme achieves confidentiality and unforgeability instantiation in the standard model.

Signcryption scheme proposed by Zheng [8] was on the assumptions of discrete logarithm, but did not propose a security proof for their scheme. In view of this, several research in signcryption schemes such as the schemes in [9–11] and signature schemes in [12–14] have been constructed to simultaneously achieve digital signature and PKE, with other functional extensions in [15–18]. In 2011, a survey of identity-based signcryption cryptosystem was outlined in [19]. Analysis of the various constructions in [20–22] were discussed and other signcryption schemes without random oracles were also considered in [23–26]. Threshold signcryption schemes in [27–29] had a limit on the number of users who can join the scheme during secret key distribution. However, the scheme in [29] only achieved semantic security whereby the scheme in [30] pointed out the lack of formal models and security proof in their scheme and later unveiled a new improved scheme [30].

Furthermore, Selvi [31] did a cryptanalysis and pointed out the drawbacks in [30]; thus, their security claims of unforgeability were not supported by a satisfactory proof and the security key of the sender could be exposed which will lead to a total break down of the scheme. In view of this, Selvi [31] proposed a corrected scheme under the security notion of signcryption. Again, a combination of threshold and proxy signcryption has been proposed by Li et al. [32] and Wang et al.[33].

Recently, secure identity-based cryptosystem has been proposed by Li et al. [34]. Their security improvement was based on a proposed signcryption algorithms in [10, 11, 20–22] constructed using the random oracle as well as schemes deployed via the standard model in [23, 26, 35], and semantic improved secure scheme in [25]. All these schemes had certain deficiencies such as indistinguishable chosen ciphertext attack (IND-CCA2) and existential unforgeable chosen message attack (EUF-CMA). However, an attack was launched in the scheme in [36] to unveil a new functional secure identity-based signcryption cryptosystem in [34]. Construction of signcryption cryptosystem in public key-insulated has also been studied in [37, 38]. Recently, Zhu et al. [37] launched an attack in [38] to disprove their security notion of EUF-CMA. According to the Zhu [37], Chen et al. [38] method did not satisfy security property of EUF-CMA. Hence, they improved their work to achieve a standard security notion of EUF-CMA. Nonetheless, there has not been any scheme to fill the gap in ID-based plaintext checkable signcryption with equality test in healthcare systems.

Plaintext Checkable Cryptosystem

Plaintext checkable encryption (PCE) was proposed by Carnard et al. [2] during CT-RSA-2012 conference. This concept unveiled the idea of searching on ciphertext using a plaintext keyword. Their scheme was based on the random oracle model and it achieved a desired probabilistic cryptographic property. According to Carnard et al. [2], anyone could perform equality test function on whether the encrypted data are an encryption of a desired plaintext with a corresponding public key. The anonymous test for equality exposes their scheme to attacks, and the use of public key certified by a certificate authority serves as a limitation to their scheme. However, our proposed scheme enables digital signing of the plaintext, delegating the test for equality to a third party via inverse trapdoor computation, and deployment of identity-based cryptosystem to eradicate the problem of key-escrow [39] associated with certificate authorities (CA). We observed that Carnard et al. [2] and Alornyo et al. [1] proposed constructions when improved will be useful in healthcare systems, such that plaintext keywords can be digitally signed to achieve a dual benefits of digital signature and public key encryption. Again, digitally signing the plaintext and delegating the search for equality to a third party denies anonymous tester to check for equality on whether the signed plaintext is the encryption of the signtext message.

Other constructions of PCE have been studied extensively; however, deployment of PCE via the standard model has been recently introduced by Ma et al. [40]. Their scheme deployed the smooth projective hash function and proved its security efficacy with s-priv1-cca and was independent of the unlink security approach. To the best of our knowledge, Id-based plaintext checkable signcryption with equality test in healthcare systems via the random oracle model with its efficient deployment is still a challenging problems.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Equality Test

Boneh et al. [41] proposed the first public key encryption using keyword search (PKEKS). Similar PKEKS schemes proposed in [42–44] enabled the user encrypt the keyword and the corresponding data under a specific users public key, meanwhile, users creates a target keyword trapdoor by using their private key and then uploads to cloud systems. Nonetheless, cloud system can only compare keywords with trapdoors corresponding to same public key. This has become bottlenecks for development of keyword search. To alleviate this problem, Yang et al. [45] proposed the concept of public key encryption with equality test(PKE-ET) based on bilinear pairing. Compared to PKE-KS, the equality test in PKE-ET can be performed between two ciphertexts encrypted with similar public key and with different public keys.

Following the works of Yang et al. [45], some well-designed schemes with equality test have been constructed [46–49]. Recently, Ma [40] proposed a scheme with equality test in cloud computing. Their above-mentioned scheme integrated identity-based cryptosystem into public key encryption with equality test as a novel approach; thus, it achieved the advantages of both cryptographic primitives. However, there has been a recent attack perpetuated by an adversary who is able to launch what is referred to as the insider attack [50]. In this era of cloud computing, equality test function is outsourced to a cloud system to examine whether two ciphertexts are encryptions with similar message [51]. Such a delegated responsibility to the cloud server gives it the leverage to launch the insider attack on users' ciphertext. This attack when successful enables the cloud server peddle with encrypted data for economic gains. If the cloud server has legitimate access to users ciphertext and is able to test their equality, then the cloud server (insider) should be resisted from peddling with users ciphertext. Recent schemes on insider attack has not been able to fully solve this problem. Therefore, a scheme to check the authenticity of the plaintext keyword during the check process is paramount in this era of encrypted analytics. Therefore, our proposed construction of a signcryption scheme checks the authenticity of the plaintext keyword during the check for equality.

Our Contribution

Because of the need to signcrypt and authenticate a signcryptext to achieve data integrity, authentication, and non-repudiation in the work presented at ICSIoT 2019 [1], we propose an improved identity-based plaintext checkable signcryption with equality test in healthcare to resist forgery and re-play attacks during data access and transmission. Our suggested construction achieved the simultaneous benefit of digital signature and public key encryption (PKE). The security analysis of our scheme affirms our construction to a desirable security property of existential unforgeability and chosen message attack (EUF-CMA).

Definition

Preliminaries

Definition 1 Bilinear Map. Let G_1 and G_T be two multiplicative cyclic groups of prime order p. Suppose that q is a generator of G_1. A bilinear map $e : G_1 \times G_1 \rightarrow G_T$ satisfies the following properties:

1. Bilinearity: For any $g \in G_1$, and $b \in Z_p$, $e(g^x, g^y) = e(g, g)^{xy}$.
2. Non-degenerate: $e : (g, g) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(g, g)$ for any $g \in G_1$.

Definition 2 Bilinear Diffie–Hellman (BDH) problem. Let G_1 and G_T be two groups of prime order q. Let $e : G_1 \times G_1 \rightarrow G_T$ be an admissible bilinear map and let q be a generator of G_1. The BDH problem in (q, G_1, G_T, e) is as follows: Given (q, q^x, q^y, q^z), for random $x, y, z \in Z_p^*$, for any randomized algorithm. A computes the value $e(q, q)^{xyz} \in G_T$ with advantage:

$$\mathrm{ADV}_A^{\mathrm{BDH}} Pr[A(q, q^x, q^y, q^z) = e(q, q)^{xyz}].$$

We say that the BDH assumption holds if for any polynomial-time algorithm A, its advantage ADV_A^{BDH} is negligible.

System Model

Tables 1 and 2 depict two medical database records of a plaintext database and signcryptext database. The primitive of PCE enables a relational plaintext check from Table 1 to signcryptext Table 2. The system works as follows:

1. **System Registration**: Authorized users forward their unique identity to a key generation center (KGC). KGC forwards secret keys to the users authorized in the system.
2. **Setup**: User signcrypt medical records and forwards it through outsourcing to the cloud service provider. In addition, the authorized user delegates the cloud service provider using the delegation algorithm with his secret key, and forwards it to the cloud service provider.
3. **Signcryptext Query**: In a case where the authorized user demands for the data stored in the cloud either signcrypted or unsigncrypted. The user sends a query keyword to the cloud service provider. The sent key-

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

word can either be signcrypted data or unsigncrypted. Thus, the keyword search can enable plaintext check on signcrypted or unsigncrypted data. For instance, we could conduct a search for equality check between the F_{Name} from Table 1 to that of a malaria parasite status in Table 2. The cloud service provider forwards the result of the search to the authorized user. It should, however, be noted that the authorized user is the only designated user to unsigncrypt the result sent by the cloud service provider corresponding to a specific user identity (ID).

4. **Search**: This phase, the cloud service provider is then delegated to check for equality after it has been given the delegated trapdoor from the ID-based authorized user. Again, the authorized user is the only designated user to unsigncrypt the result.

ID-PCSET Framework

Our scheme specifies seven algorithms. Thus, Setup, PCSET-Extract, *WBInsGen*, PCSET-Delegation, PCSET-Signcrypt, PCSET-Unsigncrypt, PCSET-Test. M_{PCSET} and CT_{PCSET} are plaintext space and ciphertext space, respectively.

1. **Setup**: The system on input a security parameter τ, the public parameters K and MK_{PCSET} are generated.
2. **PCSET-Extract**: The system on input MK_{PCSET}, $ID \in \{0,1\}^*$ chosen arbitrarily. The secret key $\text{sdk}_{\text{PCSET}}$ is returned corresponding to an identity ID.
3. **PCSET-WBInsGen**: The algorithm on input security parameter τ, $ID \in \{0,1\}^*$ arbitrarily chosen, a randomly chosen witness [52] $w_1 \in W_{\text{PCSET}}$ selected corresponding to w_{ID}, where $\text{WInsGen}(w_1) = x_1$ and $x_1 \in X_{\text{PCSET}}$. (w_1, x_1) must satisfy the witness relation R.
4. **PCSET-Delegation**: The scheme on input $ID \in \{0,1\}^*$ chosen arbitrarily, generated instance $x_1 \in X$ and forwards it to the healthcare database server.
5. **PCSET-Signcrypt**: The scheme on input $ID \in \{0,1\}^*$ chosen arbitrarily, plaintext $m_1 \in M$ associated with a randomly chosen witness relation $w_1 \in W$. The ciphertext $CT_1 = (m_1, w_1)$.
6. **PCSET-Unsigncrypt**: On input the ciphertext $CT_1 \in CT_{\text{PCSET}}$, secret key sdk_{PCSET} of a corresponding witness $w_1 \in W$. The plaintext m_1 is given as output, or $\perp$ otherwise.
7. **PCSET-Test**: Assuming two ciphertexts $CT_{1_A} \in CT_{\text{PCSET}}$ corresponding to ID_A, plaintext m_{1_A}, and another ciphertext $CT_{1_B} \in CT_{\text{PCSET}}$ corresponding to ID_B, plaintext m_{1_B}. The scheme will return a success (thus, 1) if m_{1_A} and m_{1_B} are both equal corresponding to their respective plaintext. Otherwise, it returns failure (thus, $\perp$)

ID-PCSET Security Model (IND-CCA and EUF-CMA)

The ID-PCSET satisfies two basic notions of security; thus, indistinguishable chosen ciphertext attack (IND-CCA2) and existential unforgeability against chosen message attack (EUF-CMA) [23, 25, 34]. However, ID-PCS-ET adds a notion of ID-based indistinguishability to IND-CCA2 referred to as IND-ID-CCA2 as equally presented in [34] using the standard model. Using IND-ID-CCA2 approach, the following game between the adversary A and the challenger is outlined. Let $\sqcup$=(Setup, Extract, Delegation, PCSET-Signcrypt, PCSET-Unsigncrypt, PCSET-Test) be the same scheme and a polynomial-time algorithm A. We illustrate the security proof in Fig. 1

1. Setup: The challenger runs the security parameter τ and returns K. It gives the system parameter K to the adversary and keeps MK_{PCSET} to himself.
2. Phase 1: The adversary issues query $(P_1, P_2, ..., P_{n-1})$. Each query is of the form:
   - Query (ID_i): The challenger run $H(.)$ to generate MK_{PCSET} corresponding to the public key ID_i. It sends MK_{PCSET} to A.
   - PCSET-Delegation: The challenger runs private unsigncryption on PCSET-Delegation. The algorithm run PCSET-Delegation to generate a trapdoor Tpd_{PCSET} using MK_{PCSET} . Finally, it sends Tpd_{PCSET} to A.
   - **Unsigncrypt** queries: The challenger runs the unsigncrypt algorithm to unsigncrypt the ciphertext CT_1 by running the extract algorithm to obtain sdk_{PCSET} corresponding to the public key ID_i. Finally, it sends the plaintext m_1 to A.

3. **Challenge**: After phase 1 is over, A submits two equal-length messages (m_0, m_1) and ID^* to be challenged by the challenger. However, both (m_0, m_1) were not given out during the **signcrypt** query and ID^* happens NOT to be in the extract query as in phase 1. The challenger then randomly picks $b \in \{0,1\}^*$ and respond with $CT_1^* \leftarrow signcrypt(m_{1_b}, ID^*, w_1^*)$. The algorithm generates a challenge delegation $Tpd^*_{\text{PCSET}} = (ID^*, x^*)$ by running the delegation algorithm $Tpd^*_{\text{PCSET}} \leftarrow Tpd_{PCSET}(sdk_{\text{PCSET}}, m_{1_B}, x^*)$ and sends Tpd^*_{PCSET} to A.
4. Phase 2: The adversary issues query $(P_1, P_2, ..., P_{n-1})$. Each query is of the form:
   - Query. The challenger responds as in phase 1, since $ID_i \neq ID^*$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

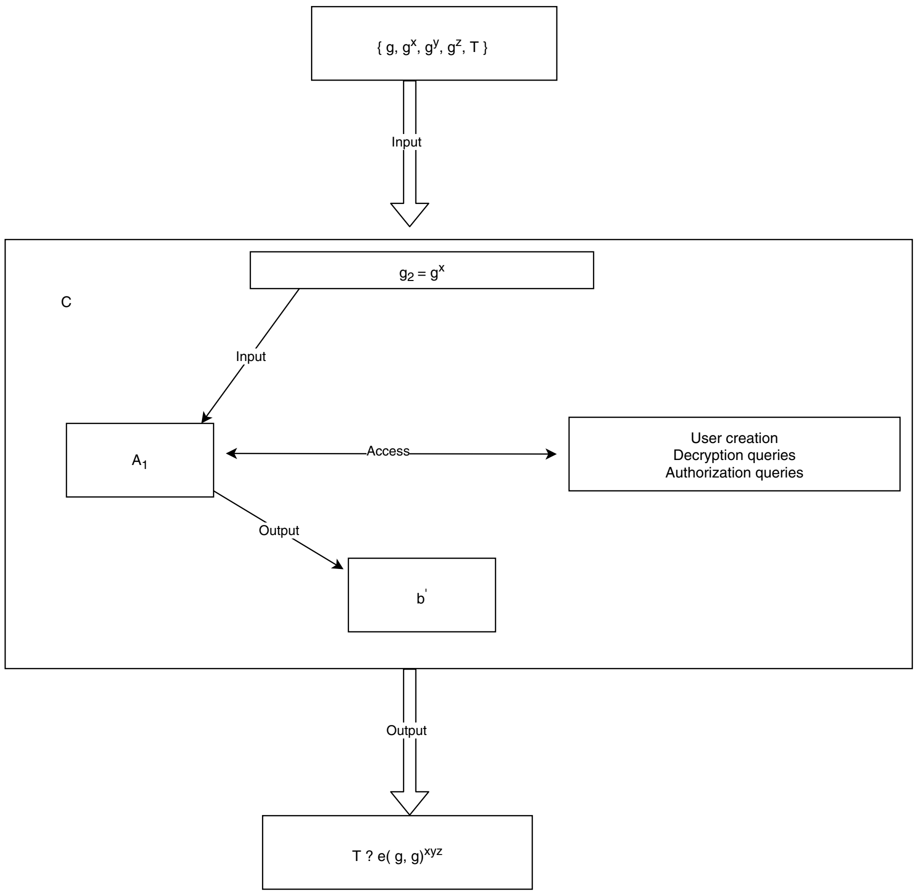

Fig. 1 Security proof model of our scheme

- Delegation Query. Where $x \neq x^*$. The challenger respond in the same way as in phase 1.
- Unsigncryptext Query. Where $ID, CT_1 \neq ID^*, CT_1^*$

5. Output: A submits a guess $b^{'}$ on b. If $b^{'} = b$, we say A wins the game.

$A's$ advantage in breaking the scheme is noted as:

$\mathrm{ADV}_{\text{ID-PCSET}} = Pr[b^{'} = b] - \frac{1}{2}$ is negligible.

EUF-CMA Security

The ID-PCSET achieves IND-ID-CCA2 property if and only if no polynomial adversary attains a non-negligible advantage via IND-ID-CCA2 game. ID-PCS-ET also achieves the security property of EUF-CMA as outlined below in the game between the challenger and adversary:

1. **Setup**: The challenger runs the security parameter τ and returns K. It gives the system parameter K to the adversary.
2. **Adversarial Attack**: The adversary undertakes a polynomial bounded queries similar to the above game.
3. **Forgery**: The adversary makes available a new tuple (CT_1^*, ID^*, x^*). It should be noted that the new tuple were not produced during the signcryptext oracle request. The adversary wins the game if unsigncryptext (CT_1^*, ID^*, x^*) does not output the symbol $\perp$.

According to the above game, it is assumed that ID-PCS-ET has EUF-CMA property if there exists no polynomial bounded adversary with a non-negligible advantage.

Construction

We outline the detailed construction of our scheme. This includes:

1. **Setup**: The system on input a secured parameter σ, it returns a public parameter K and MK_{PCSET} as the master secret key.
   - The system chooses two multiplicative groups G_1 and G_T with the same order of length θ bits with a

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 3 The performance communication overheads

Scheme	$G_{1_{mtt}}$	$G_{1_{Ep_1}}$	$G_{T_{mtt_1}}$	$G_{T_{Ep_1}}$	$G_{T_{Iv_1}}$	P	IND-2	EC_1	E
[55]	$2x_{u_1} + 2x_{m_1} + 1$	3	5	1	1	7(+2)	N/A	A	N/A
[56]	$2x_{u_1} + 2x_{m_1} + 1$	3	5	1	1	7(+2)	N/A	NA	N/A
[34]	$2x_{u_1} + 2x_{m_1} + 3$	7	5	1	2	7(+2)	N/A	N/A	N/A
[57]	$2x_{u_1} + x_{m_1} + 1$	7	5	1	1	7(+2)	A	A	N/A
[36]	$2x_{u_1} + x_{m_1} + 3$	7	5	1	1	7	N/A	N/A	N/A
Ours	$2x_{u_1} + x_{m_1} + 3$	7	3	2	2	8	A	A	A

legends: In this table,$''G''_{Mtt}$: multiplication in group G_1, $''G''_{Ep_1}$: G_1 group exponentiation, $''G''_{T_{Mtt}}$: multiplications in G_T, $''G''_{T_{Ep_1}}$: exponentiations in G_T, $''G''_{T_{Iv_1}}$: inverse computations in group G_T, $''x_m, x''_u$: length of identity in bit strings, $''P''$: pairing operations in the form $x(+y)$ with y as in [56], $''E''$: equality test and A: applicable, N/A: not applicable, $IND-2$: IND-CCA2, EC_1: EUF-CMA

bilinear map $e : G_1 \times G_1 \rightarrow G_T$. The generator g is selected for the group.

- A keyed permutation is deployed such that $F : \{0,1\}^s \times \{0,1\}^n \rightarrow Z_p^*$ with a positive integer $D = k(i)$ and $L = b(i)$, a random activated value r_1 is chosen from $\{0,1\}^L$. Message authentication code (MAC) remarked as Generate(G), Sign(S) and Verify(V). It executes G(i) to obtain r_2. A master token key $MSK = (r_1, r_2)$ is set.
- The algorithm deploys a hash function $H_a : \{0,1\}^t \rightarrow Z_p^*$, $H_b : \{0,1\}^* \rightarrow G_1$, $H_c : A \times G_1 \times G_T \rightarrow \{0,1\}^{t+r_1}$, where r_1 is noted as a random number and t as the length of the message. $(t_1, t_2) \in Z_p^2$ randomly chosen and sets $R_1 = g^{t_1}, R_2 = g^{t_2}$. The system parameter $K = (A, G_1, G_T, g, R_1, R_2, MAC, H_a, H_b, H_c)$ is published.

2. **PCSET-Extract:** The algorithm on input an $ID \in \{0,1\}^*$ as string, it computes $Q_{\text{PCSET}} = H_b(ID) \in G_1$, secret key $\text{SDK}_{\text{PCSET}} = (Q_{ID}^{t_1}, Q_{ID}^{t_2})$. (t_1, t_2) are the secret random values generated by the algorithm.
3. **PCSET-Delegation:** The algorithm on input a string $ID \in \{0,1\}^*$, it computes $Q_{ID} = H_b(ID) \in G_1$ and derives a token $\text{TDK}_{\text{PCSET}} = (Q_{ID}^{t_2})$.
4. **PCSET-Signcrypt:** The algorithm on input K, ID as string, it then executes $Q_{ID} = H_b(ID) \in G_1$. A plaintext $m \in M_{\text{PCSET}}$ is chosen and two random values $(P_1, P_2) \in Z_p^*$. It sets the ciphertext $CT_1 = (CT_e, CT_f, CT_g, CT_h)$ as:
   $CT_e = (H_b(Q_{ID}, \text{TDK}_{\text{PCSET}})^{P_1}) \cdot m^{P_1}, CT_f = g^{P_1}$
   $CT_g = g^{P_2}$, $CT_h = (m||w_1) \oplus H_b(CT_e||CT_f||U||e(Q_{ID}, R_2)^{P_2})$
   The MAC symmetric signature (S), $U = S(r_2, CT_f)$ is deployed to signcrypt CT_1. Thus, the signed Tag U is used to verify the ciphertext CT_f.
5. **PCSET-Unsigncrypt**: The unsigncrypt algorithm on input the ciphertext CT_1, secret key $\text{SDK}_{\text{PCSET}} = (Q_{ID}^{t_1}, Q_{ID}^{t_2})$. (t_1, t_2) are secret random numbers generated by the algorithm. The algorithm verify if $CT_e = (H_b(Q_{ID}, \text{TDK}_{\text{PCSET}}))$ and $CT_f = g^{P_1}$ are equal. If equal, it returns m and $\perp$ otherwise.
6. **PCSET-Test:** With a given plaintext m_A, identity ID_A, a ciphertext CT_{1_A}, and another plaintext m_B, identity ID_B, ciphertext CT_{1_B}. The algorithm then executes $Q_{ID} = H_b(ID) \in G_1$. It checks whether m_A is a plaintext checkable signcryption of a ciphertext CT_{1_B} and also if m_B is the plaintext checkable signcryption of a ciphertext CT_{1_B} via the computation of :

$$m_A^{P_1} = \frac{CT_{e_A}}{H_b(e(Q_{ID_A}, \text{TDK}_{\text{PCSET}})^{P_1})},$$
$$m_B^{P_1} = \frac{CT_{e_B}}{H_b(e(Q_{ID_B}, \text{TDK}_{\text{PCSET}})^{P_1})}$$
$$m_A^{P_1} = \frac{H_b(e(Q_{ID_A}, \text{TDK}_{\text{PCSET}})^{P_1}) \cdot m_A^{P_1}}{H_b(e(Q_{ID_A}, \text{TDK}_{\text{PCSET}})^{P_1})},$$
$$m_A^{P_1} = \frac{H_b(e(Q_{ID_B}, \text{TDK}_{\text{PCSET}})^{P_1}) \cdot m_B^{P_1}}{H_b(e(Q_{ID_B}, \text{TDK}_{\text{PCSET}})^{P_1})}$$
$$m_A^{P_1} = \frac{H_b(e(Q_{ID_A}, Q_{ID_A}^{t_2})^{P_1}) \cdot m_A^{P_1}}{H_b(e(Q_{ID_A}, Q_{ID_A}^{t_2})^{P_1})},$$
$$m_B^{P_1} = \frac{H_b(e(Q_{ID_B}, Q_{ID_B}^{t_2})^{P_1}) \cdot m_B^{P_1}}{H_b(e(Q_{ID_B}, Q_{ID_B}^{t_2})^{P_1})}. \text{ Therefore,}$$
$$m_A^{P_1} = m_B^{P_1}.$$

Computational Efficiency

The Pairing-Based Cryptography (PBC) Library [53] is used to quantify the time consumption of signcryption, unsigncryption and test delegation operations (Table 3) . We use the code of a program in VC++ 6.0 and executed on a computer (Windows 10 Pro, operating system), Capacity of Intel(R)

Table 4 Running times (ms)

Symbols	Description	Times
G_{Ep_1}	G_1 exponentiation operation	6.3937
$G_{T_{Ep}}$	G_T exponentiation operation	1.9718
P_1	Pairing operation	11.4173
H_{fn}	Hash functions	0.000853
G_{Mtt}	Multiplication operation in G_1	0.047
G_{Mt_1}	Multiplication operation in G_T	0.0119

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 5 Computational cost (ms)

Scheme	PCSET-Signcrypt	PCSET-Unsigncrypt	PCSET-Delegation
[57]	$7G_{Ep_1} + 5H_{fn} + 5G_{Mt} = 44.817$	$7P_1 + 5H_{fn} + 5G_{Mt} = 76.985$	N/A
Ours	$2G_{Exp_1} + 5H_{fn} + 5G_{Mt} = 3.943$	$8P_1 + 5H_{fn} + G_{Mt} = 91.378$	$1G_{Exp_1} + 1H_{fn} + 1G_{Mt_1} = 6.4065$

Core (TM) i5-4460 CPU with 3.20GHz and 4Gb RAM. The code was executed several times and average time of execution extracted in Table 4. With respect to the scheme in [54], and other pairing-based constructions with a security level of $1024 - bit$ RSA, a supersingular curve $z^2 = \times^3 + \times$ with an embedded degree of 2 is adopted. Also, $q = 2159 + 217 + 1$ noted as a 160 bit Solinas prime with $p = 12qr - 1$ noted as a 512 bit prime. With regards to ECC-based schemes, an equivalent security level of Koblitz elliptic curve of $y = x^3 + ax^2 + b$ defined on a $F_{2^{163}}$ is used to provide the same security level in the ECC group. The computational units are in millisecond (ms) and bytes, respectively. The execution times of each respective algorithm were calculated and Matlab program was used to generate the computational results in Table 5. According to Table 5, we achieved a signcryption cost of 3.942(ms), unsigncryption computational cost of 91.378 milliseconds and test delegation achieved a remarkable cost of 6.4065 milliseconds comparable to the scheme in [57]. This computational cost results make our scheme ideal for efficient implementation in mobile platforms and cloud computing environment.

Conclusion

Our paper introduced ID-based plaintext checkable signcryption with equality test in healthcare systems. The proposed construction is efficient and has a lesser computational cost than the usual encrypt-then-sign schemes that had a higher computational cost. In spite of the fact that other extensions of identity-based encryption with equality test (IBE-ET) exist [58–61], ID-PCS-ET achieves a desirable security property of IND-ID-CCA2 with EUF-CMA via the random oracle model.

Acknowledgements We would like to use this opportunity to thank the anonymous reviewers for their contributions and support.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical Approval This paper does not contain any studies with human participants or animals performed by any of the authors.

References

1. Alornyo S, Evans A, Kingsford KM, Benjamin K, Xiong H, Michael A. ID-based outsourced plaintext checkable encryption in healthcare database. In: 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), IEEE; 2019. pp. 48–53.
2. Canard S, Georg F, Aline G, Fabien L. Plaintext-checkable encryption. Cryptographers' track at the RSA conference. Berlin: Springer; 2012. p. 332–48.
3. Li F, Hu X, Yongjian L. A generic construction of identity-based signcryption. In: 2009 International Conference on Communications, Circuits and Systems, IEEE; 2009, pp. 291–5.
4. Shamir A. Identity-based cryptosystems and signature schemes. Workshop on the theory and application of cryptographic techniques. Berlin: Springer; 1984. p. 47–53.
5. Bentahar K, Farshim P, Malone-Lee J, Smart NP. Generic constructions of identity-based and certificateless KEMs. J Cryptol. 2008;21(2):178–99.
6. Chen L, Cheng Z, Malone-Lee J, Smart NP. An efficient ID-KEM based on the Sakai-Kasahara key construction. IACR Cryptol. 2005. https://eprint.iacr.org/2005/224
7. Kiltz E, David G. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles. Australasian conference on information security and privacy. Berlin: Springer; 2006. p. 336–47.
8. Zheng Y. Digital signcryption or how to achieve cost (signature and encryption) cost (signature)+ cost (encryption). Annual international cryptology conference. Berlin: Springer; 1997. p. 165–79.
9. Malone-Lee J. Identity-based signcryption. IACR Cryptol. 2002. https://eprint.iacr.org/2002/098
10. Barreto PSLM, Benoît L, Noel M, Jean-Jacques Q. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. International conference on the theory and application of cryptology and information security. Berlin: Springer; 2005. p. 515–32.
11. Libert B, Jean-Jacques Q. A new identity based signcryption scheme from pairings. In: Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674, IEEE; 2003, pp. 155–8
12. Am Fiat, Adi S. How to prove yourself: practical solutions to identification and signature problems. Conference on the theory and application of cryptographic techniques. Berlin: Springer; 1986. p. 186–94.
13. Guillou LC, Jean-Jacques Q. A paradoxical indentity-based signature scheme resulting from zero-knowledge. Conference on the Theory and Application of Cryptography. New York: Springer; 1988. p. 216–31.
14. Yuen TH, Victor KW. Constant-size hierarchical identity-based signature/signcryption without random oracles. IACR Cryptol. 2005.
15. Zheng Y, Imai H. How to construct efficient signcryption schemes on elliptic curves. Inform Process Lett. 1998;68(5):227–33.
16. Bao F, Robert HD. A signcryption scheme with signature directly verifiable by public key. International workshop on public key cryptography. Berlin: Springer; 1998. p. 55–9.
17. Shin J-B, Kwangsu L, Kyungah S. New DSA-verifiable signcryption schemes. International conference on information security and cryptology. Berlin: Springer; 2002. p. 35–47.
18. Yum DH, Pil JL. New signcryption schemes based on KCDSA. International conference on information security and cryptology. Berlin: Springer; 2001. p. 305–17.
19. Li F, Muhammad KK. A survey of identity-based signcryption. IETE Tech Rev. 2011;28(3):265–72.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

20. Chow SSM, Siu-Ming Y, Lucas CKH, Chow KP. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. International conference on information security and cryptology. Berlin: Springer; 2003. p. 352–69.
21. Boyen X. Multipurpose identity-based signcryption. Annual international cryptology conference. Berlin, Heidelberg: Springer; 2003. p. 383–399.
22. Chen L, John M-L. Improved identity-based signcryption. International workshop on public key cryptography. Berlin: Springer; 2005. p. 362–79.
23. Yu Y, Yang B, Sun Y, Zhu S-L. Identity based signcryption scheme without random oracles. Comput Stand Interfaces. 2009a;31(1):56–62.
24. Paterson KG, Jacob CNS. Efficient identity-based signatures secure in the standard model. Australasian conference on information security and privacy. Berlin: Springer; 2006. p. 207–22.
25. Jin Z, Wen Q, Hongzhen D. An improved semantically-secure identity-based signcryption scheme in the standard model. Comput Electr Eng. 2010a;36(3):545–52.
26. Li F, Liao Y, Qin Z. Analysis of an identity-based signcryption scheme in the standard model. IEICE Trans Fundam Electron Commun Comput Sci. 2011;94(1):268–9.
27. Li F, Juntao G, Yupu H. ID-based threshold unsigncryption scheme from pairings. International conference on information security and cryptology. Berlin: Springer; 2005. p. 242–53.
28. Duan S, Zhenfu C, Rongxing L. Robust ID-based threshold signcryption scheme from pairings. In: Proceedings of the 3rd international conference on Information security; 2004, pp. 33–7.
29. Peng C, Xiang L. An identity-based threshold signcryption scheme with semantic security. International conference on computational and information science. Berlin: Springer; 2005. p. 173–9.
30. Li F, Yong Y. An efficient and provably secure ID-based threshold signcryption scheme. In: 2008 International Conference on Communications, Circuits and Systems, IEEE; 2008, pp. 488–92.
31. Selvi SSD, Sree SV, Pandu CR, Neha J. Cryptanalysis of Li et al.'s identity-based threshold signcryption scheme. In: 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, IEEE; 2008, pp. 127–32.
32. Li F, Xin X, Yupu H. ID-based threshold proxy signcryption scheme from bilinear pairings. Int J Sec Netw. 2008;3(3):206–15.
33. Wang M, Zhijing L. Identity based threshold proxy signcryption scheme. In: The Fifth International Conference on Computer and Information Technology (CIT'05), IEEE; 2005, pp. 695–9.
34. Li F, Takagi T. Secure identity-based signcryption in the standard model. Math Comput Modell. 2013;57(11–12):2685–94.
35. Waters B. Efficient identity-based encryption without random oracles. Annual international conference on the theory and applications of cryptographic techniques. Berlin: Springer; 2005. p. 114–27.
36. Zhang B. Cryptanalysis of an identity based signcryption scheme without random oracles. J Comput Inform Syst. 2010;6(6):1923–31.
37. Zhu G, Xiong H, Qin Z. Fully secure identity based key-insulated signcryption in the standard model. Wirel Pers Commun. 2014a;79(2):1401–16.
38. Chen J, Chen K, Wang Y, Xiangxue L, Yu L, Wan Z. Identity-based key-insulated signcryption. Informatica. 2012;23(1):27–45.
39. Hassan A, Eltayieb N, Elhabob R, Li F. An efficient certificateless user authentication and key exchange protocol for client-server environment. J Ambient Intell Humaniz Comput. 2018;9(6):1713–27.
40. Ma S, Yi M, Susilo W. A Generic Scheme of plaintext-checkable database encryption. Inform Sci. 2018;429:88–101.
41. Boneh D, Matt F. Identity-based encryption from the Weil pairing. Annual international cryptology conference. Berlin: Springer; 2001. p. 213–29.
42. Boneh D, Giovanni DC, Rafail O, Giuseppe P. Public key encryption with keyword search. International conference on the theory and applications of cryptographic techniques. Berlin: Springer; 2004. p. 506–22.
43. Fang L, Susilo W, Ge C, Wang J. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. Inform Sci. 2013;238:221–41.
44. Shi J, Junzuo L, Yingjiu L, Robert HD, Jian W. Authorized keyword search on encrypted data. European symposium on research in computer security. Cham: Springer; 2014. p. 419–35.
45. Yang G, Chik HT, Qiong H, Duncan SW. Probabilistic public key encryption with equality test. Cryptographers' track at the RSA conference. Berlin: Springer; 2010. p. 119–31.
46. Lee HT, Huaxiong W, Kai Z. Security analysis and modification of ID-based encryption with equality test from ACISP 2017. Australasian conference on information security and privacy. Cham: Springer; 2018. p. 780–86.
47. Lipmaa H. Verifiable homomorphic oblivious transfer and private equality test. International conference on the theory and application of cryptology and information security. Berlin: Springer; 2003. p. 416–33.
48. Tang Q. Public key encryption schemes supporting equality test with authorisation of different granularity. Int J Appl Cryptogr. 2012;2(4):304–21.
49. Wu L, Zhang Y, Choo K-KR, He D. Efficient identity-based encryption scheme with equality test in smart city. IEEE Trans Sustain Comput. 2017;3(1):44–55.
50. Wu T, Sha M, Yi M, Shengke Z. ID-based encryption with equality test against insider attack. Australasian conference on information security and privacy. Cham: Springer; 2017. p. 168–83.
51. Chen R, Yi M, Guomin Y, Fuchun G, Xiaofen W. A new general framework for secure public key encryption with keyword search. Australasian conference on information security and privacy. Cham: Springer; 2015. p. 59–76.
52. Garg, S, Craig G, Amit S, Brent W (2013) Witness encryption and its applications. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing; 2013, pp. 467–76.
53. Lynn B. The stanford pairing based crypto library. Privacy preservation scheme for multicast communications in smart buildings of the smart grid. 2013.
54. Xiong H, Mei Q, Zhao Y. Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. IEEE Syst J. 2019;14(1):310–20.
55. Yu Y, Yang B, Sun Y, Zhu S-L. Identity based signcryption scheme without random oracles. Comput Stand Interfaces. 2009b;31(1):56–62.
56. Jin Z, Wen Q, Hongzhen D. An improved semantically-secure identity-based signcryption scheme in the standard model. Comput Electr Eng. 2010b;36(3):545–52.
57. Zhu G, Xiong H, Qin Z. Fully secure identity based key-insulated signcryption in the standard model. Wirel Pers Commun. 2014b;79(2):1401–416.
58. Ma S. Identity-based encryption with outsourced equality test in cloud computing. Inform Sci. 2016;328:389–402.
59. Alornyo S, Mensah AE, Abbam AO. Identity-based public key cryptographic primitive with delegated equality test

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

against insider attack in cloud computing. Int J Netw Sec. 2020;22(5):743–51.

60. Alornyo S, Kingsford KM, Abraham T-H, Xiong H. Mobile Money wallet security against insider attack using ID-based cryptographic primitive with equality test. In: 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), IEEE; 2019, pp. 82–7

61. Alornyo S, Zhao Y, Zhu G, Xiong H. Identity based key-insulated encryption with outsourced equality test. IJ Netw Sec. 2020;22(2):257–64.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com