Research Article

ID-based key-insulated signcryption with equality test in cloud computing

Seth Alornyo[1] · Kingsford Kissi Mireku[2] · Mustapha Adamu Mohammed[1,4] · Daniel Adu-Gyamfi[3] · Michael Asante[4]

Received: 10 September 2020 / Accepted: 5 March 2021 / Published online: 24 March 2021

Abstract
Key-insulated encryption reduces the problem of secret key exposure in hostile setting while signcryption cryptosystem attains the benefits of digitally signing a ciphertext and public key cryptosystem. In this study, we merge the primitives of parallel key-insulation cryptosystem and signcryption with equality test to construct ID-based parallel key-insulated signcryption with a test for equality (ID-PKSET) in cloud computing. The construction prevent data forgery, data replay attacks and reduces the leakage of secret keys in harsh environments. Our scheme attains the security property of existential unforgeable chosen message attack (EUF-CMA) and indistinquishable identity chosen ciphertext attack (IND-ID-CCA2) using random oracle model.

Keywords Key leakage · Digital signature · Equality test · ID-based cryptosystem

1 Introduction

The cloud system has seen paradigm shift in data outsourcing and computations. Thus, the cloud ecosystem has served as a means to data outsourcing in this era of ubiquitous and distributed computing. However, trust as a security property has been evasive over the years due to the peddling of data outsourced to the cloud. The user's data needs to be encrypted before being uploaded to the cloud [1]. In spite of the encryption of user's data before uploading to the cloud, there is no guarantee to the security and privacy of the outsourced encrypted or unencrypted data to the cloud system. Several research in this direction has been conducted with provable security.

With regard to public key encryption (PKE) [2], a disasterous phenomenon curtailed by key-insulation [3] has played a major role for the effective deployment of PKE constructions in an insecure environment. Thus, private keys for encryption/decryption can be exposed in an insecure environment and the approach to alleviate this menace requires the adoption of key-insulation in public key cryptosystem. It is not practical to download the entire data stored in the cloud before a search on the data is conducted. Thus, the user should be able to search on the data while the data is stored in the cloud. The user makes a request to the cloud system and the cloud system respond to the request by searching through the stored data. In this way, the entire data is not downloaded from the cloud system before a search is conducted (see Fig. 1). The use of the helper in key-insulated cryptosystem enables the user update his decryption key with a time-stamp. Thus, helper serves as a physically secured device (see Fig. 2) used to update the secret keys during user key updates. The helper serves as an attachment during user key update and it is designed such that the presence of the helper is required to ensure a successful key update process. Figure 2 depicts a typical scenario of our scheme using multiple helper to update decryption keys.

✉ Seth Alornyo, sabigseth@outlook.com | [1]Computer Science Department, Koforidua Technical University, Koforidua, Ghana. [2]Ghana Institute of Management and Public Administration, School of Technology, Accra, Ghana. [3]Department of Cybersecurity and Computer Engineering Technology, CK Tedam University of Technology and Applied Sciences, Navrongo, Ghana. [4]Computer Science Department, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.

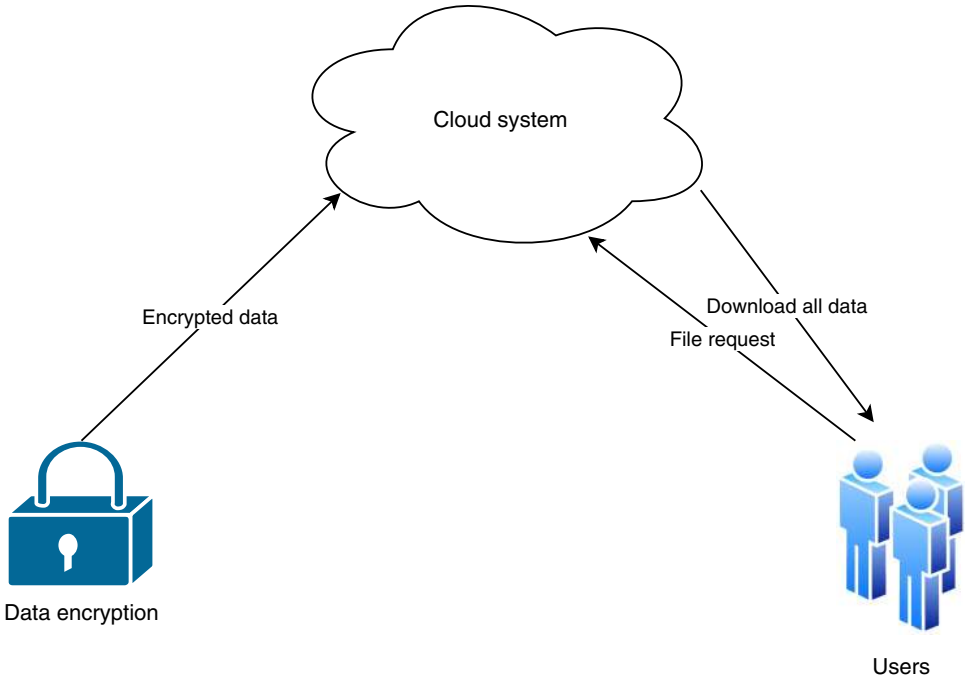

Fig. 1 Encrypted data download scenario

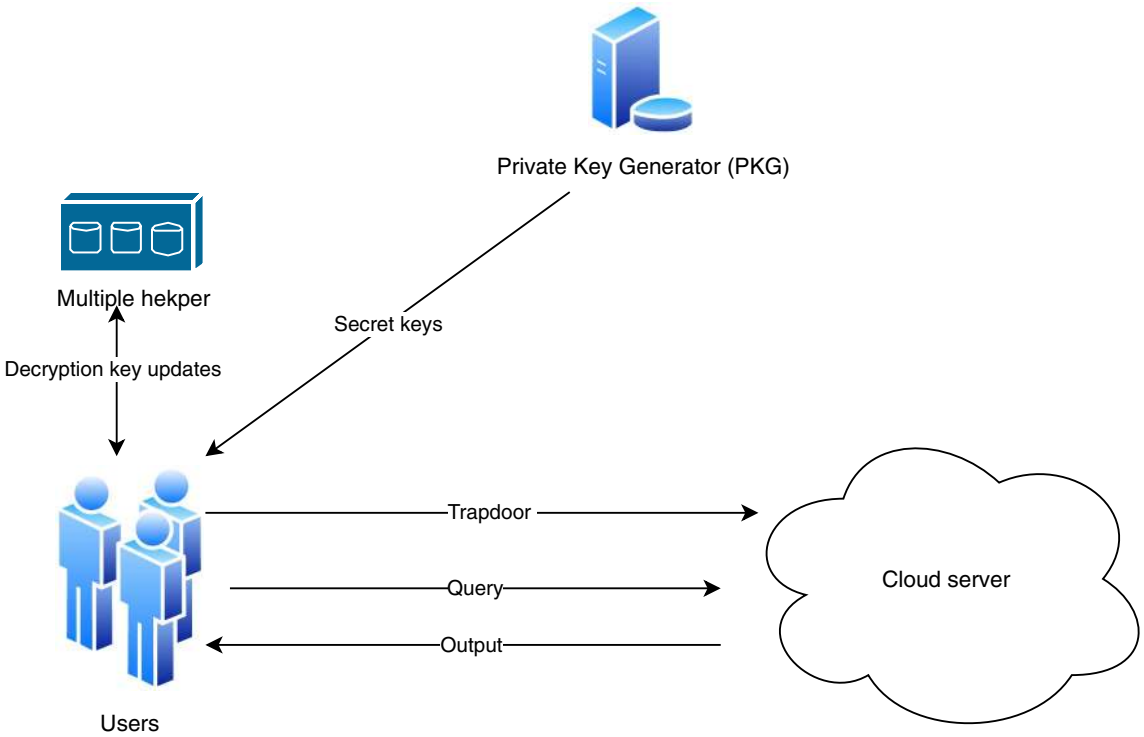

Fig. 2 System model of our scheme

Public key encryption with keyword search (PKE-KS) [2] ensures that user's can search on ciphertext stored in the cloud without the need to download the entire ciphertext before a search is conducted. In spite of this work by Boneh et al. [2], several key-insulated cryptosystem schemes on keyword search deployed using PKE [4–6], without random oracle model [7], and schemes deployed via identity-based encryption (IBE) [8, 9] have been constructed. The combination of identity (ID)-based key-insulated signcryption with equality test is yet to be unveiled.

It is important to safeguard the privacy concerns of user's data outsourced to the cloud system to attain a security property of digital signature with PKE. The adoption of key-insulated signcryption with equality test in this paradigm gives our scheme a novel approach to effectively secure user's data that has been outsourced to the cloud. Therefore, the construction of ID-based parallel key insulated signcryption with equality test (ID-PKSET) in cloud computing is presented. Our scheme achieves multiple security enhancement in PKE with signcrypted key-insulated cryptosystem. The use of multiple helper instead of single and or double helper as shown in Fig. 2 is considered in our construction.

1.1 Paper organization

The remaining part of our work is organized as follows; Sect. 2 outlines our contribution, sect. 3 details the related work, sect. 4 outlines the preceedings of our construction and formulates ID-PKSET definitions. Section 5 outlines the security model, section 6 details the construction of our scheme and section 7 gives a comparative anlysis and section 7 concludes our work and outlines future improvement.

2 Our contribution

A recent work by Zhu et al. [10] attacked Chen et al.'s [11] scheme. They dispelled their security of EUF-CMA. Accordingly, the scheme could not attain the security of EUF-CMA. In this regard, a scheme to fulfill the primitive of identity based key-insulated cryptosystem with equality test in support for EUF-CMA property is yet to be unveiled.

In this paper, our contribution is in three folds; (1) We construct an ID-based key-insulated signcryption scheme with equality test. (2) Our scheme achieves the security property of EUF-CMA with an added ID-based security assumption. (3) Our method delegates the cloud server to perform equality test and support for key-insulation while resisting re-play attacks and message forgery.

3 Related work

The untrusted nature of the cloud has called for the need to protect the integrity of outsourced data to cloud systems. There is a risk of private key exposure as a result of the deployment of cryptographic algorithms for harsh environments. Thus, the risk of private key exposure is equally disasterous for the effective utilization of cryptographic algorithms. Several schemes have deployed key-insulated constructions to reduce the exposure of decryption keys. Notably, Dodis et al. [4] were the first to introduce the concept of key-insulation in public key cryptosystem. Their proposed scheme had a total time period which was not known in advance. A combined effort of schemes in [4, 12, 13] has still not received the needed research attention. Several other schemes adopted the time based approach to construct key-insulated cryptosystems. Other directions of this primitive have been proposed; such as proxy re-encryption [14] which allowed a proxy to re-encrypt the ciphertext before transmission. A combination of key-insulated cryptosystem with certificateless encryption by He et al. [15] enabled the introduction of certificateless key-insulated cryptosystem. Moreover, a combination of identity-based scheme with support for key insulation by Hanaoka et al. [8] gave rise to identity based key insulated encryption using a single helper. The introduction of identity based key insulated cryptosystem without the use of random oracle model has also been proposed by Libert et al. [7]. These and many other related schemes has given rise to the need for further research into identity based key insulated cryptosystem.

3.1 Equality test

The concept of PKEKS unveiled by Boneh et al. [2] made it possible to encrypt a keyword with data. However, their scheme only supported an encryption scheme with same public key. The use of same public key in their scheme was a drawback to the successful implementation of the construction, hence Yang et al. [16] constructed public key encryption with equality test (PKE-ET) that supported encryption with same and different public key. With regard to the construction in [2], Yang et al.'s [16] work served as an improved version of Boneh et al.'s [2] work. Several schemes have been unveiled afterwards [17, 18]. Most of the schemes constructed were based on public key infrastructure (PKI). Therefore, there was the need to forego the inhibiting properties of using certificates generated by certificate authority (CA) in public key crptosystem. Hence, Ma et al. [19] proposed ID-based cryptographic primitive with equality test to curtail the problems associated with CA. Although, Ma et al. [19] had an excellent performance in terms of security improvement and the use of ID-based primitive to support keyword search, their scheme does not achieve the benefit of digital signature and key-insulation simultaneously. Therefore, the need to construct a scheme to fill this gab has become necessary.

3.2 Key-insulated signcryption cryptosystem

A signcryption cryptographic primitive proposed by Li et al. [12] attained the benefit of digitally signing a ciphertext and PKE. Their scheme served as improvement to previous schemes that were not based on signature-then-encrypt with high computational cost. Thus, the use of signature-then-encrypt inherits high computational cost. The deployment of signcryption ensures the attainment of less computational cost. In view of this, several schemes on signcryption have been constructed [20, 22] and a combination of digital signature and signcryption [21, 23] cryptosystems with its variants in proxy-signcryption [24–26], anonymous signcryption [11, 27] and ring signcryption [10, 28].

Key-insulated signcryption schemes have also been constructed [10, 11]. The scheme in [11] launched an attack on Chen et al.'s [26] construction to dispel the security feature of EUF-CMA. Up till now, no scheme have been constructed to fulfill the cryptographic primitive of key-insulated signcryption with equality test.

4 Outline of ID-PKSET

In ID-based parallel key-insulated signcryption with equality test (ID-PKSET), the scheme outlines the following; $Setup$, $SET-Extract$, $KeyGeneration$, $KeyUpdate-BaseKey$, $TempKeyUpdate$, $SET-Trapdoor$, $Signcrypt$, $Unsigncrypt$, $Test$, where M_σ and CT_σ are the plaintext space and ciphertext space, respectively:

1. **Setup**: Given the secured paramenter ι, time period TP, helper keys υ. The algorithm returns PP, helper keys $(U_{n_0}, ..., U_{n_{\upsilon-1}})$ as well as temporal master key MTK.
2. **SET** $-$ *Extract*: On input, MTK, arbitrary $ID \in \{0,1\}^*$, system parameter PP, it returns a secret key sdk_{ID_0} to user associated with identity ID. PKG executes same function and forwards to corresponding user with the identity ID through a secured channel.
3. **KeyGeneration**: The key generation method on input received secret key sdk_{ID}, public parameter PP, time period TP with identity ID. It finally outputs base key BSK_0.
4. **KeyUpdate-HelperKey**(BK_0, bk_j, t): On input base key BSK_0 at a span bsk_j and index t_s. The scheme outputs updated key UTK_{t_s}.
5. **TempKeyUpdate**: On input $sdk_{ID_{t_{s-1}}}$, index t_s of the next updated key UTK_t. It output the secret key $mdk_{ID_{t_s}}$ for a next span t_s corresponding to a user.
6. **SET-Trapdoor**: It selects as input MTK, arbitrary $ID \in \{0,1\}^*$ index time span t_s and returns a $SET-trapdoorstdr$ to the corresponding identity ID.
7. **Signcrypt**: It inputs PP, the index t_s, identity $ID \in \{0,1\}^*$ with plaintext $M_1 \in M_\sigma$, and return the ciphertext CT_{t_s} as $CT_{t_s} = (t_s, CT_1)$, where $CT_{t_s} \in CT_\sigma$.
8. **Unsigncrypt**: It takes current private secret key $sdk_{ID_{t_s}}$ and ciphertext CT_{t_s} as input and returns plaintext $M_1 \in M_\sigma$ or generates $\perp$ as invalid, if there is a mismatch of ciphertext is invalid.
9. **Test**: It takes ciphertext $CT_{t_{s_A}}$ and $CT_{t_{s_A}}$ outputted by two users: A and B. It outputs 1 of the message corresponding to $CT_{t_{s_A}}$ and $CT_{t_{s_B}}$ if they are equal. It outputs 0, otherwise.

5 Security model of ID-PKSET

Definition (IND-ID-CCA and EUF-CMA). ID-PKSET fulfil two security properties. Indistinguishable chosen ciphertext attack, acronym (IND-CCA2) and EUF-CMA [29–31]. However, ID-PKSET adds ID-Based indistinquishability as a feature to IND-CCA2 and coined as IND-ID-CCA2 in [29]. With IND-ID-CCA2 technique, the game between adversary A and challenger are outlined. We Let Δ =($Setup$, $SET-Extract$, $KeyGeneration$, $TempKeyUpdate$, $SET-Trapdoor$, $Signcrypt$, $Unsigncrypt$, $Test$) be the same scheme and a polynomial time algorithm A.

1. **Setup**: The challenger execute the parameter ι and total time period TP with helper keys $(U_{n_0}, ..., U_{n_{\upsilon-1}})$ and achieves PP. It forwards the parameter PP to the adversary and keeps MTK.
2. **Phase 1**: Adversary issues query $(N_1, N_2, ..., N_m)$. The query is as follows:
   - **Query** (ID_i): The challenger execute $H(.)$ to output sdk_{ID_i} corresponding to public key (ID_i). It forwards sdk_{ID_i} to A.
   - **SET-Trapdoor**: The challenger execute private **unsigncryption** on $TempKeyUpdate$. The algorithm run $SET-Trapdoor$ to derive a trapdoor std_i using MTK. Finally, it forwards $stdr_i$ to A.
   - **Unsigncrypt** queries: We execute the **unsigncrypt** algorithm to decrypt the ciphertext $CT_{t_{a_i}}$ by executing the extract algorithm to derive sdk_{ID_i} relating to (ID_i). Finally, plaintext M_i is forwarded to A.
3. **Challenge**: When phase 1 is over, A submits two equal-length message (m_0, m_1) and ID^* to be challenged by the challenger . However, both (m_0, m_1) were not the **signcrypt** query and ID^* happens not to be the extract

query used in phase 1. The challenger randomly picks $b \in \{0,1\}$ relating to $CT^*_\sigma \leftarrow \mathbf{signcrypt}(M_b, ID^*, t^*_s)$. The algorithm forwards a challenge $SET-trapdoor$ $stdr^* = (ID^*, t^*_s)$ by running the $SET-trapdoor$ $stdr^* \leftarrow stdr(dk, M_b, t^*_s)$ algorithm and returns $stdr^*$ to A.

4. **Phase 2**: The adversary issues query $(N_1, N_2, ..., N_m)$. Each query is of the form: • Query. The challenger reply similar to phase 1. This is because $ID_i \neq ID^*$. • $SET-Trapdoor$ query. Where $t_s \neq t^*_s$. The challenger respond as in phase 1. • *Unsigncryption* Query. Where $(ID_i, CT_{t_s} \neq (ID^*, CT^*_{t_s}))$
5. **Output**: The adversary A forwards a guess $b^{'}$ on b to win the game If $b^{'} = b$..

Adversary advantage is noted as:

$Adv_{ID-PKSET}(\iota) = Pr[b^{'} = b] - \frac{1}{2}$ is negligible.

ID-PKSET attains IND-ID-CCA2 property if there exist no polynomial adversary achieves non-negligible advantage with IND-ID-CCA2. ID-PKSET attains security of EUF-CMA as depicted below:

1. **Setup**: Challenger executes security parameter ι and total time period TP with helper keys $(U_{n_0}, ..., U_{n_{\upsilon-1}})$ and achieves PP. It forwards system parameter PP to adversary.
2. **Adversarial Attack**: Adversary does a polynomial bounded query same to definition A.
3. **Forgery**: The new tuple $(CT^*_\sigma, ID^*, t^*_s)$ is made available. However, new tuple was not part of the signcryption oracle. The adversary wins the game if **Unsigncrypt**$(CT^*_\sigma, ID^*, t^*_s)$ does not produce the symbol $\perp$.

It is seen that ID-PKSET achieves EUF-CMA. It is expected that there are no polynomial adversary with a non-negligible advantage.

6 Construction

Our construction includes the following:

1. **Setup**: Given an input parameter ι, total time period TP, number of helper key υ. The public parameter PP is returned. The system set initial master key as MTK and associated multiple multiple helper key $(U_{n_0}, ..., U_{n_{\upsilon-1}})$.

   • Multiplicative two groups of G and G_T generated with same order d with length λ bits and bilinear map $e : G \times G \rightarrow G_T$. Arbitrary generator $P \in G$ is selected by the system.

   • The algorithm deploys keyed permutation $F : \{0,1\}^k \times \{0,1\}^n \rightarrow Z^*_p$ for integer $K = k(\iota)$ and $L = n(\iota)$. A random value t_1 set from $\{0,1\}^L$. Message authentication code scheme MAC, $MAC = GSV$, Thus: Generate, Sign, and Verify. The algorithm obtain t_2 by executing $G(\iota)$. Token key is set as $MSTK = (t_1, t_2)$.

   •The system adopts hash functions $H_1 : \{0,1\}^{ml} \rightarrow Z^*_p, H_2 : \{0,1\}^* \rightarrow G, H_3 : A \times G \times G_T \rightarrow \{0,1\}^{ml+l}$, where l is the random numbers length and ml message length. The system randomly picks $(s_1, s_2) \in Z^2_p$ and set $P_1 = P^{s_1}$, $P_2 = P^{s_2}$. The public parameter $PP = (A, ml, G, G_T, e, P, P_1, P_2, Un_\upsilon, MAC, H_1, H_2, H_3)$ is published and a MTK=(s_1, s_2). A is known as Message Authentication Code (MAC) tag.
2. **SET-extract**: With a string $ID \in \{0,1\}^*$, the parameter PP and MTK. The system compute $J_{ID} = H_2(ID) \in G$, set temporal master key decryption $msdk_{ID_{t_s}} = (J^{s_1}_{ID_{t_s}}, J^{s_2}_{ID_{t_s}})$ where (s_1, s_2) are known as secret key at the initial time index t_s.
3. **KeyGeneration**: On input $msdk_{ID_{t_s}}$, a randomly choosen $Un_{\upsilon_i} \in \{0,1\}^{ml}$ and set: $Un_{\upsilon_0} = P^{Un_{\upsilon_i}}$, $P_3 = P^{s_1} \cdot (\prod_{\upsilon_i \in Un_{\upsilon-1}}^{0} P^{H_1(\upsilon_i)})^{r_1}$ $P_4 = (\prod_{\upsilon_i \in Un_\upsilon}^{0} g^{r_i})$, where $r_2 = F(Un_{\upsilon_i}, Un_{\upsilon-1})$.

   We therefore note that F is regarded as pseudorandom permutation.

   Therefore, we denote the base helper key as Un_{υ_0} =(P_3, P_4) corresponding to the helper $\{Un_{\upsilon_0}, Un_{\upsilon-1}\}$
4. **Key update-helper**: The algorithm on input helper key Un_{υ_i} and a period index t_s.The KeyUpdate-Helper computes the next t_{sth} key as:

   KUH_{t_s}=$(Un_{\upsilon_{t_s}}, Un^{'}_{\upsilon_{t_s}})$ with $BKU_{\upsilon-1}$=$(P_{3_{t_s}}, P_{4_{t_s}})$.

   $P_{4_{\upsilon-1}}$=$P_{4_{\upsilon-1}}(Un_{\upsilon_{t_s}})$, $P_{3_{\upsilon-1}}(Un^{'}_{\upsilon_{t_s}})$. Therefore,

   $BKU_{\upsilon-1}$=$(J_{ID_{t_{s_4}}}, J_{ID_{t_{s_3}}})$.

   The current index period decryption key is noted as:

   $sdk_{ID_{\upsilon t_s}}$=$(J^{s_1}_{ID_{t_s}}, J^{s_2}_{ID_{t_s}})$.
5. **SET-Trapdoor**: Given a string $ID \in \{0,1\}^*$, MTK with index time t_s the algorithm computes: $J_{ID} = H_2(ID) \in G$ and set the trapdoor $stdr_{ID} = J^{s_1}_{ID_t}$. It is however noted that $stdr_{ID}$ serves as the second element of $msdk$. $msdk_{ID_{t_s}}$, $stdr_{ID}$ and $MSTK$ are distributed in a secure secure channel to authorized users.
6. **Signcrypt**: To **signcrypt**, a signer with a corresponding ID can **signcrypt** a message M with a public ID by choosing two random selected numbers $(r_a, r_b) \in Z^*_p$ to computes:

   CT_{σ_1}=P^{r_a}, CT_{σ_2}=$D^{r_a} \cdot H_2(e(P_4, J_{ID_{t_s}})^{r_a})$

   CT_{σ_3}=P^{r_b}, CT_{σ_4}=$(M||r_a) \oplus H_3(CT_{\sigma_1}||CT_{\sigma_2}||X||e(P_3, J_{ID_{t_s}})^{r_b})$.

   Where D=$((\prod_{\upsilon_i \in Un_{\upsilon_{t_{s-1}}}}^{0} P^{H_1(\upsilon_i)}) \cdot M)$

   Therefore: CT_σ= $(CT_{\sigma_1}, CT_{\sigma_2}, CT_{\sigma_3}, CT_{\sigma_4})$.

However, $X \leftarrow S(t_2, CT_{\sigma_3})$ is for a **signcrypted** algorithm of MAC. Corresponding tag X is used to affirm the **signcrypted** CT_{σ_3}.

7. **Unsigncrypt**: The algorithm on input **signcrypted** ciphertext CT_σ, decryption helper updated key $sdk_{ID_{v_{t_s}}}$ and a token $MSTK = (t_1, t_2)$. The system compute:
$CT_{\sigma_4} \oplus H_3(CT_{\sigma_1}||CT_{\sigma_2}||X||e(CT_{\sigma_3}, sdk_{ID}^{s_1})) = M^{'}||r^{'}$,
$H_3(e(CT_{\sigma_3}, sdk_{ID_{t_s}}^{s_1}))=M^{'}||r^{'}$.
On input $X \leftarrow S(t_2, CT_{\sigma_3})$, where $X = MAC_{t_2}(CT_{\sigma_3})$, it verifies $X^{'}=MAC_{t_2}(CT_{\sigma_3})$. If $X^{'} = X$, then a check on whether:
$CT_{\sigma_1} = P^{r_a^{'}}$ and $CT_{\sigma_2} = D^{r_a} \cdot H_2(e(CT_{\sigma_1}, J_{ID}^{s_2}))$. Then the algorithm outputs M
8. **Equality-test**: Given a **signcrypted** ciphertext CT_{σ_A} with trapdoor $stdr_A$ and another **signcrypted** ciphertext CT_{σ_B} with a trapdoor $stdr_B$. Equality test of whether $M_A = M_B$ is checked. This is done by computing:
$ET_A=\frac{CT_{\sigma_{2_A}}}{H_2(e(CT_{\sigma_{1_A}}, stdr_{ID_A}))}$, $ET_B=\frac{CT_{\sigma_{2_B}}}{H_2(e(CT_{\sigma_{1_B}}, stdr_{ID_B}))}$.
Thus, $ET_A=D_A^{r_{a_A}} \cdot H_2(e(P_A^{r_a}, J_{ID_{t_{s_A}}}^{s_2}))$, $ET_B =D_B^{r_{a_B}} \cdot H_2(e(P_B^{r_a}, J_{ID_{t_{s_B}}}^{s_2}))$.
Therefore, $ET_A = D_A^{r_{a_A}}$ and $ET_B = D_B^{r_{a_B}}$
Algorithm outputs 1 or $\perp$ if the equation holds or otherwise.
$e(CT_{\sigma_A}, ET_B) = e(CT_{\sigma_B}, ET_A)$.

Consistency: $e(CT_{\sigma_A}, ET_B) = e(CT_{\sigma_B}, ET_A)$

$(CT_{\sigma_A}, ET_B) = e(J_{ID}^{r_{a_A}}, D_B^{r_{a_B}}) = (J_{ID}, D_B)^{r_{a_A} r_{b_B}}$

$(CT_{\sigma_B}, ET_A) = e(J_{ID}^{r_{a_B}}, D_A^{r_{a_A}}) = (J_{ID}, D_A)^{r_{a_B} r_{b_A}}$

If $D_A = D_B$, then the function outputs $M_A = M_B$. Thus, $e(CT_{\sigma_A}, ET_B)= e(CT_{\sigma_A}, ET_A)$. Then :
$Test(CT_{\sigma_A}, stdr_{ID_A}, CT_{\sigma_B}, stdr_B)$ output 1.
We assume that $Pr[Test(CT_{\sigma_A}, stdr_{ID_A}, CT_{\sigma_B}, stdr_B) = 1]$ is negligible.

6.1 Security property of IND-CCA2

Our ID-PKSET is $(\epsilon_{SET}, t_s, q_{ks}, q_{ns}, q_{us}) - IND - CCA2$ secure if $(\epsilon_{mdbdh}, t_s) - mDBHDH$ assumption holds. Thus, H_1 and H_2 serves as (ϵ_{H_1}) and (ϵ_{H_2}) are both collision resistant hash functions, such that:

$$\epsilon_{SET} \leq \epsilon_{mdbdh} + \epsilon_{H_1} + \epsilon_{H_2} + \frac{q_{ks}+q_{us}+3}{p} + \frac{q_{ns}}{p^2}$$

Where, t_s is noted as index period, q_{ks} as extract key queries, q_{ns} as **signcryption** queries and q_{us} as **unsigncryption** queries.

6.2 EUF-CMA unforgeability

Proof theorem: We outline the unforgeability against adaptive CMA derived from the security of Chow's ID-based cryptosystem under CDH assumption. Thus, if the attacker can forge a valid signcrypted message of a message, then he must equally be able to forge Chow's valid signature scheme. Thus, the adversary can equally forge ciphertext of a message M if we assume $CT_\sigma = (CT_{\sigma_1}, CT_{\sigma_2}, CT_{\sigma_3}, CT_{\sigma_4})$ of a user with an identity ID, then $CT_{\sigma_4} = (M||k) \oplus H_2(CT_{\sigma_1})||CT_{\sigma_2}||X||e(P_3, J_{ID_{t_s}})^{r_b}$ can be seen as the signature on message $M||k$ where $k = H_2(e(CT_{\sigma_1}, J_{ID}^{s_2})^{r_b}$. It is a known fact that the problem of CDH makes the primitive unforgeable.

Again, our scheme PKI-ID-SET is $(\epsilon_{SET}, t_s, q_{ks}, q_{ns}, q_{us}) - EUF - CMA$ secure assuming the work of Paterson and Sachuldt's signature is $(\epsilon_{SET}, t_s^{'}, q_{ks}, q_{ns})$ existentially unforgeable , whereby $t_s^{'} = t_s + q_{ks}C_{ek} + q_{ns}C_{sn} + q_{us}C_{un}$. Where q_{ks} represents key extract queries, q_{ns} as number of **signcryption** queries, q_{us} as number of **unsigncryption** queries, C_{ek} as key extract cost of ID-PKSET, C_{sn} also as cost of signcryption of ID-PKSET and finally C_{un} represents cost of **unsigncryption** of ID-PKSET. However, details of the security analysis proof similar to our work can further be accessed in the appendix section of the work by Li et al. [31]

Table 1 Security strength comparison of variant signcryption schemes

	IND-ID-SC-KI-CCA2	EUF-ID-SC-KI-CMA	KS	CL-Del	ET	TG
[11]	No	No	Yes	No	No	No
[31]	No	No	No	No	No	No
[33]	Yes	Yes	No	No	No	No
[32]	No	Yes	No	No	No	No
[10]	Yes	Yes	No	No	No	No
Ours	Yes	Yes	Yes	Yes	Yes	Yes

Remark: In this table, "$IND - ID - SC - KI - CCA2$" refers to Indistinguishable identity signcryption key-insulated chosen ciphertext attack, "$CL - Del$": cloud delegation, "$EUF - ID - SC - KI - CMA$": existential unforgeable identity signcryption key-insulated chosen message attack, "ET": Equality test, "TG": token generation, "Yes": supportive remark, "No": not supportive

Table 2 Computational running times

Symbol	Description	Computational Times
T_{Exp_1}	Exponentiation in G	6.3937
T_{Exp_2}	Exponentiation in G_T	1.9518
T_{p_1}	Pairing operations	11.4173
T_{h_1}	Hash function computations	0.000853
T_{p_m}	Multiplication in G	0.047
$T_{p_{m_1}}$	Multiplication in G_T	0.0119

7 Comparison

We outline the security strength of our proposed scheme with related signcryption schemes in terms of computational cost in Table 1. The current existing schemes on key-insulated signcryptions such as [10, 11] are compared with and other ID-based signcryption cryptosystem schemes [31–33] are also compared with in terms of their security strength. Thus, the security parameters for our comparison includes IND-ID-CCA2 with key exposure (IND-ID-SC-KI-CCA2), EUF-CMA with key exposure (EUF-CMA-KI-SC-CMA), support for key insulation, cloud delegation and token generation. Our method has a favourable security feature of IND-ID-KI-CCA2 and EUF-ID-SC-KI-CMA similar to [10, 33], but ID-PKSET has an added and extended security feature of key-insulation, delegated equality test and token key generation absent in [10, 11]. Therefore, it's clear that the additional computational overheads makes our scheme practical and feasible when deployed in cloud computing environment. This is agreeable due to the cost of group exponentiation and group multiplication same to our scheme, even though our scheme has additional computational overheads. Therefore, the computational results and communicational overhead outlined in our scheme scientifically makes the scheme feasible with an added security and improvement on [10, 33].

Using [34], the pairing-based cryptographic repository were deployed to quantify time consumption of our scheme. The VC++ 6.0 program codes were executed using windows Operating System with capacity of i5-4460 CPU 3.20 Ghz and a RAM size of 4Gb. The average time of execution were extracted (see Table 2). Using [35] with other pairing based schemes of security level 1024-bit RSA, supersingular curve $z^2 = x^3 + x$ using embedded degree $2. q = 2^{159} + 2^{17} + 1$regarded as 160-bit Solinas prime with $p = 12qr - 1$as 512-bit prime. With ECC-based approach, a security of Koblitz elliptic curve $y = x^3 + ax^2 + b$ defined on $F_{2^{163}}$ function adopted to provide same security level in ECC. Milliseconds (ms) and bytes were used to measure the units. Each respective execution times were calculated using Matlab program in Table 3. Computational results are outlined in Table 3. Computational results are outlined in Table 4.

Table 3 The performance computational cost and Communication overheads

	G_{Mult}	G_{Exp_1}	$G_{T_{Mul_1}}$	$G_{T_{Exp_1}}$	$G_{T_{Inv_1}}$	Pr	IND-CCA2	EUF-CMA	ETs
[29]	$2n_{u_1} + 2n_{m_1} + 1$	3	5	1	1	7(+2)	-	Yes	No
[30]	$2n_{u_1} + 2n_{m_1} + 1$	3	5	1	1	7(+2)	-	-	No
[33]	$2n_{u_1} + 2n_{m_1} + 3$	7	5	1	2	7(+2)	-	Yes	No
[31]	$2n_{u_1} + n_{m_1} + 1$	7	5	1	1	7(+2)	Yes	Yes	No
[10]	$2n_{u_1} + n_{m_1} + 3$	7	5	1	1	7	Yes	Yes	No
Ours	$2n_{u_1} + n_{m_1} + 3$	7	3	2	2	8	Yes	Yes	Yes

Legends: $''G''_{Mult}$: multiplication operations in G, $''G''_{Exp_1}$: exponentiation operations in G, $''G''_{T_{Mult}}$: multiplications in G_T, $''G''_{T_{Exp_1}}$: exponentiations in G_T, $''G''_{T_{Inv_1}}$: inverse computations in group G_T, $''n''_m, n''_u$: identity length, $''Pr''$: pairing operations in the form $x(+y)$ where y relate to scheme in [30], $''ETs''$: equality test, Yes: supportive remark, –: not supportive

Table 4 Computational cost comparison result (ms)

Scheme	Enc_{Comp}	Dec_{Comp}	$Test_{Comp}$
[10]	$7T_{Exp_1} + 5T_{h_1} + 5T_{p_{m_1}} = 44.817$	$7T_{p_1} + 5T_{h_1} + 5T_{p_{m_1}} = 76.985$	N/A
Ours	$2T_{Exp_2} + 5T_{h_1} + 3T_{p_{m_1}} = 3.943$	$8T_{p_1} + 5T_{h_1} + 3T_{p_{m_1}} = 91.378$	$8T_{p_1} + 2T_{Exp_2} + 5T_{h_1} = 95.246$

Remark: Enc_{Comp}: encryption computations, Dec_{Comp}: decryption computations, $Test_{Comp}$: test computations

Computational cost of our method is outlined based on the running times in Table 2 to compare the computational cost and communication overheads in Table 4 with schemes in key-insulated signcryption cryptosystem. We compared the work of Yu et al. [10], the schemes [30, 31, 33] and the scheme [10] with ours.

It is clear that our scheme attains a remarkable security property in signcryption comparable to existing schemes. A security property of IND-ID-SC-CCA2, EUF-ID-SC-KI-CMA and key insulation are achieved in our scheme. However, ID-PKSET proposes additional security functionality to existing schemes such as secured delegation to cloud systems, equality test and a token key generation to enhance the security of our scheme. However, we achieve a computational equality test result of 95.246ms. Therefore, it is obvious that ID-PKSET achieves IND-ID-SC-CCA2, EUF-ID-KI-SC-CMA, key-insulated with multiple helper, cloud delegation, equality test and token generation simultaneously and thus an ideal scheme deployable in an insecure environment.

8 Conclusion and future work

Our paper proposed ID-based parallel key-insulated signcryption in cloud computing. Our construction achieves efficient and lesser computational cost. Even though other scheme on key-insulated cryptosystems with equality test exist [3, 36], ID-PKSET achieves remarkable property of signcryption cryptosystem using the random oracle model. Future direction of this work will invlove the construction of certificateless methodology to prevent the problem with key-escrow in PKE. The private key generator could be a bad actor and needs to be resisted.

Declarations

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. Zhou L, Varadharajan V, Hitchens M (2013) Achieving secure role-based access control on encrypted data in cloud storage. IEEE Transactions Information Forensics Secur 8(12):1947–1960
2. Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G (2004) Public key encryption with keyword search. International conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 506–522
3. Alornyo S, Zhao Y, Zhu G, Xiong H (2020) Identity based key-insulated encryption with outsourced equality test. IJ Netw Secur 22(2):257–264
4. Dodis Y, Katz J, Xu S, Yung M (2002) Key-insulated public key cryptosystems. International conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 65–82
5. Hanaoka G, Hanaoka Y, Imai H (2006) Parallel key-insulated public key encryption. International workshop on public key cryptography. Springer, Berlin, pp 105–122
6. Cheon J, Hopper N, Kim Y, Osipkov I (2006) Timed-release and key-insulated public key encryption. International conference on financial cryptography and data security. Springer, Berlin, pp 191–205
7. Libert B, Quisquater J, Yung, M (2007). Parallel key-insulated public key encryption without random oracles. In International workshop on public key cryptography . Springer, Berlin. pp 298-314
8. Hanaoka Y, Hanaoka G, Shikata J, Imai H (2005) Identity-based hierarchical strongly key-insulated encryption and its application. International conference on the theory and application of cryptology and information security. Springer, Berlin, pp 495–514
9. Weng J, Liu S, Chen K, Zheng D, Qiu W (2008) Identity-based threshold key-insulated encryption without random oracles. Cryptographers' Track at the RSA Conference. Springer, Berlin, pp 203–220
10. Zhu G, Xiong H, Qin Z (2014) Fully secure identity based key-insulated signcryption in the standard model. Wirel pers commun 79(2):1401–1416
11. Chen J, Chen K, Wang Y, Li X, Long Y, Wan Z (2012) Identity-based key-insulated signcryption. Informatica 23(1):27–45
12. Li F, Xiong H, Liao Y (2009). A generic construction of identity-based signcryption. In 2009 International Conference on Communications, Circuits and Systems. IEEE. pp 291-295
13. Boneh D, Franklin M (2001). Identity-based encryption from the Weil pairing. In Annual international cryptology conference. Springer, Berlin. pp 213-229
14. Wang Y, Yan D, Li F, Xiong H (2017) A key-insulated proxy re-encryption scheme for data sharing in a cloud environment. IJ Netw Secur 19(4):623–630
15. He L, Yuan C, Xiong H, Qin Z (2017) An efficient and provably secure certificateless key insulated encryption with applications to mobile internet. IJ Netw Secur 19(6):940–949
16. Yang G, Tan C H, Huang Q, Wong D.S (2010). Probabilistic public key encryption with equality test. In Cryptographers' Track at the RSA Conference. Springer, Berlin. pp 119-131
17. Xu P, Jin H, Wu Q, Wang W (2012) Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack. IEEE Transactions Comput 62(11):2266–2277

18. Yu Y, Ni J, Yang H, Mu Y, Susilo W (2014) Efficient public key encryption with revocable keyword search. Secur Commun Netw 7(2):466–472
19. Ma S (2016) Identity-based encryption with outsourced equality test in cloud computing. Information Sci 328:389–402
20. Libert B, Quisquater J (2003). A new identity based signcryption scheme from pairings. In Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674). IEEE. pp 155-158
21. Fiat A, Shamir A (1986). How to prove yourself: practical solutions to identification and signature problems. In Conference on the theory and application of cryptographic techniques. Springer, Berlin. pp 186-194
22. Malone-Lee J (2002) Identity-based signcryption. IACR Cryptol 2002:98
23. Barreto PS, Libert B, McCullagh N, Quisquater JJ (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In International conference on the theory and application of cryptology and information security. Springer, Berlin. pp 515-532
24. Li X, Chen K (2004). Identity based proxy-signcryption scheme from pairings. In IEEE International Conference on Services Computing, 2004.(SCC 2004). Proceedings. IEEE pp 494-497
25. Wang M, Li H, Liu Z (2005). Efficient identity based proxy-signcryption schemes with forward security and public verifiability. In International Conference on Networking and Mobile Computing . Springer, Berlin. pp 982-991
26. Wang Q, Cao Z (2005). Two proxy signcryption schemes from bilinear pairings. In International conference on cryptology and network security. Springer, Berlin. pp 161-171
27. Zhang M, Yang B, Zhu S, Zhang W (2008). Efficient secret authenticatable anonymous signcryption scheme with identity privacy. In International conference on intelligence and security informatics. Springer, Berlin. pp 126-137
28. Li FG, Masaaki S, Tsuyoshi T (2008) Analysis and improvement of authenticatable ring signcryption scheme. J Shanghai Jiaotong Univ (Sci) 13(6):679–683
29. Yu Y, Yang B, Sun Y, Zhu SL (2009) Identity based signcryption scheme without random oracles. Comput Standards Interfaces 31(1):56–62
30. Jin Z, Wen Q, Du H (2010) An improved semantically-secure identity-based signcryption scheme in the standard model. Comput Electrical Eng 36(3):545–552
31. Li F, Takagi T (2013) Secure identity-based signcryption in the standard model. Mathematical Comput Modell 57(11–12):2685–2694
32. Li F, Muhaya FB, Zhang M, Takagi, T (2011). Efficient identity-based signcryption in the standard model. In International conference on provable security. Springer, Berlin. pp 120-137
33. Qin B, Wang H, Wu Q, Liu J, Domingo-Ferrer J (2012). A new identity based signcryption scheme in the standard model. In 2012 Fourth international conference on intelligent networking and collaborative systems. IEEE pp 606-611
34. Lynn, B (2013). The stanford pairing based crypto library. Privacy preservation scheme for multicast communications in smart buildings of the smart grid 324, 2013. "Pbc library." [Online]. Available: https://crypto.stanford.edu/
35. Xiong H, Mei Q, Zhao Y (2019) Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. IEEE Syst J 14(1):310–320
36. Alornyo S, Mohammed MA, Kodzo BAS, Sarpong PA, Asante M (2020) Parallel key insulated ID-based public key cryptographic primitive with outsourced equality test. J Comput Commun 8(12):197–213