Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 6, 988-994 (2020)
www.astesj.com
Special Issue on Multidisciplinary Sciences and Engineering

ASTES Journal
ISSN: 2415-6698

Mobile Money Wallet Attack Resistance using ID-based Signcryption Cryptosystem with Equality Test

Seth Alornyo[*,1], Mustapha Adamu Mohammed[1,2], Francis Botchey [1,3], Collinson Colin M. Agbesi [1]

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

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

[3] *University of Electronic Science and Technology of China, School of Information and Software Engineering, UESTC, Chengdu, China*

ARTICLE INFO

Article history:
Received: 18 September, 2020
Accepted: 17 November, 2020
Online: 08 December, 2020

Keywords:
ID-based encryption
Signcryption
Equality test

ABSTRACT

This paper is an extension of a research work presented at ICSIoT 2019. An attack continuum against the insider attack in mobile money security in Ghana using a witness based cryptographic method proposed by Alornyo et al. resisted the service provider from peddling with users data for economic gains. Our improved scheme achieves a simultaneous benefit of digital signature in public key encryption (PKE). The adoption of signcryption cryptosystem in our scheme achieved a desired security property of EUF-CMA using the random oracle model.

1 Introduction

Ghana and other African countries have seen a tremendous growth in mobile money service patronage in recent times. The use of the mobile money services platform requires the use of a less-resource constraint mobile devices that do not require access to internet or mobile app for mobile payment. Thus, any mobile device that does not have access to internet but can access the mobile money service provider cellualr network can perform financial transactions and other utility payments. This and many other reasons has lead to the high patronage of mobile money services in Ghana. However, the mobile money system is not immune to data forgery and re-play attacks. The system model of our scheme is depicted in 1

Our research work is an extension of a publication presented at ICSIoT 2019. The construction presented at ICSIoT 2019 [1] considered the service provider as the adversary who could launch the insider attack. The service provider had access to users token information and transaction details and was possible for the service provider to peddle with users data via the following:

- The mechant receives valid transaction details such as transaction ID, td_{ID} and finds out the content M_1 as well as the token information td_{ID} from the transaction details TSD.
- The adversary (insider) attains the ciphertext CT_1 of a guessed message M_1' and token tdk_{ID}.
- The adversary checks if the test $Test(CT_1, TSD, td_{ID}') = 1$

In the above scenario, the insider wins the game if it succeeds in deriving the token information from the transaction details. However, the scheme utilized the witness based cryptographic primitive with an added pairing operation to resist the insider attack continuum.

In spite of their construction, there were a possible attack during data transmission such as forgery and re-play attacks in mobile money payment systems. To solve the problem, we propose a scheme using a signcryption cryptographic primitive to achieve the simultanoeus benefit of digital signature and PKE in mobile money systems deployed in Ghana (West Africa). This approach resist data forgery and re-play attacks.

The first generic construction of identity-based signcryption was unveiled [2]. Their work fulfilled a dual function of digital signature and public key cryptosystem (PKE). Other traditional approaches that employed signature-then-encrypt had a high cost computations as compared to [2]. However, the scheme [2] adopted data encapsulation method instead of key encapsulation method [3]–[6] to achieve confidentiality and unforgeability instantiation in the standard model.

Signcryption scheme unveiled in [7] did not propose a secu-

[*]Corresponding Author: Seth Alornyo, Koforidua Technical University, Computer Science Department, +233 554936729 & sabigseth@ktu.edu.gh

rity proof even though their construction were based on discrete logarithm assumptions. In view of this, several research in signcryption and signature schemes have been unveiled [8]–[15] with other functional extensions [16]–[19]. In 2011, a survey of identity-based signcryption cryptosystem was examined by Li et al.[20] to examine the security models as well as a comparative study of their security properties and efficiency. Analysis of other flavours of signcryption constructions [4], [11]–[13], [21]–[24], threshold signcryption [25]–[30], proxy signcryptions [31]–[37] and ring signcryption [38]–[42] have been proposed and constructed. Subsequently, Xiong et al. [43] did a cryptanalysis on the scheme [21]. The security notion of CPA in their work was diffused by Xiong et al. [43]. Hence, [43] showed that their scheme did not achieve chosen plaintext attack (CPA) security as they claimed.

Due to the need to resist the cloud server from peddling users outsourced data, efficient signcryption cryptosystem was unveiled in [44]. According to him, some existing signcryption schemes in [45]–[55] had certain lapses such as lack of data integrity, authentication and non-repudiation. Hence the need to construct a scheme to deny the insider adversary in the cloud from data peddling and modification for economic gains became paramount. Furthermore, the emergence of distributed computing and interconnected systems propelled [56] to unveiled a signcryption scheme in heterogeneous systems. Although in [57], the author earlier discussed the above problem, they could not construct a scheme to solve the problem of signcryption in heterogeneous systems. However, the constructions in [57, 58] and [59] achieved insider and outsider attack resistant respectively.

Recently, secure identity-based cryptosystem has been unveiled in [60]. Their security improvement was based on certain proposed signcryption algorithms [11]–[14], [61] constructed using the random oracle, and as well as schemes designed using the standard model [21, 23, 24, 62] with certain deficiencies such as IND-CCA2 and existential unforgeable chosen message attack (EUF-CMA). However, an attack was launched in [63] to unveil a new functional secure identity-based signcryption cryptosystem in [60]. A scheme to curtail an attack continuum in mobile money wallet system in Ghana to prevent message forgeability and re-play attack is still an open problem.

1.1 Our Contribution

By considering that the integrity, authentication and non-repudiation of the data in mobile money wallet system in Ghana, we proposed the mobile money wallet attack resistant scheme using the ID-based signcryption cryptographic primitive with equality test (known as MWAR-ID-SET) to achieve a simultaneous benefit of digital signature with public key encryption, and with equality test. Concretely, the formal definition, security model and concrete construction of MWAR-ID-SET are proposed in this paper. Further, our proposed scheme was shown to achieve the security property of existential unforgeable chosen message attack (EUF- CMA) by using the formal security proof.

1.2 Paper Organization

The rest of this work is organized as follows; In Section 2, our scheme outlines preliminaries for the construction and formulate the definitions of MWAR-ID-SET. In Section 3, the definitions of our scheme are outlined, section 4 outlines the security model of MWAR-ID-SET. Section 5 details the construction of our scheme, and proof the security in Section 6. Section 7 compares our work with existing schemes. Section 8 concludes our work.

2 Preliminaries

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

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

Definition 2: Bilinear Diffie-Hellman (BDH) problem. Let G and G_T be two groups of prime order q. Let $e : G \times G \rightarrow G_T$ be an admissible bilinear map and let q be a generator of G. The BDH problem in (q, G, G_T, e) is as follows: Given (q, q^a, q^b, q^c), for random $c, d, f \in Z_p^*$, for any randomized algorithm. A computes the value $e(q, q)^{cdf} \in G_T$ with advantage:
$ADV_A^{BDH} Pr[A(q, q^c, q^d, q^f) = e(q, q)^{cdf}]$.
We say that the BDH assumption holds if for any polynomial-time algorithm A, its advantage ADV_A^{BDH} is negligible.

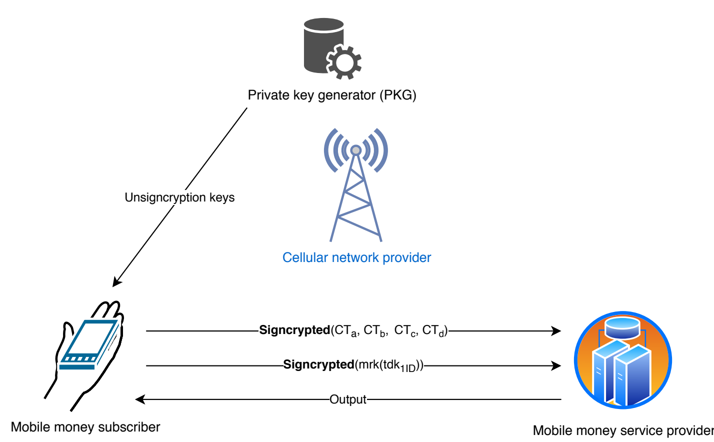

Figure 1: System model of our scheme

3 Definitions

In this section, the formal definition of our proposed scheme is outlined. MWAR-ID-SET achieves a formal security property of EUF-CMA. The construction specifies six(6) steps: $Setup$, $MW-Extract$, $TokenGen$, $MW-Signcrypt$, $MW-Unsigncrypt$, $MW-Test$. M_T and C_T are considered as the plaintext space and ciphertext space respectively.

1. $Setup$: The construction on input a security parameter k, output public parameter K with MSK as master secret key.

2. $MW - Extract$: The scheme on input MSK, $ID \in \{0, 1\}$ arbitrary and gives out a message recovery key mrk corresponding to an identity.

3. $TokenGen$: With the input message recovery key mrk, arbitrary $ID \in \{0, 1\}^*$ and it return token tdk_1 corresponding to an identity (ID_1).

4. $MW - Signcrypt$: The scheme on input $ID \in \{0, 1\}^*$, random witness $w \in W$, a chosen plaintext $m_1 \in M_1$, and output ciphertext $CT_1 = (x_1, c_1)$ where $x \in X$ from generated witness $WInsGen(w) = x$ with the relation R satisfied [1].

5. $MW - Unsigncrypt$: On input the ciphertext CT_1, message recovery key mrk with a random chosen witness $w \in W$, the plaintext $m_1 \in M_1$ is uncovered provided CT_1 is deemed as a valid ciphertext derived from a witness relation R.

6. $MW - Test$: The scheme on input the ciphertext $CT_A \in CT_1$ with its corresponding receiver ID_A derived from the token tdk_{1_A} with its corresponding ID_A, the ciphertext $CT_A \in CT_1$ with its corresponding receiver ID_B derived from the token tdk_1 with its corresponding ID_B. The scheme respond 1, provided CT_A and CT_B have same message. Otherwise it respond as $\perp$.

4 Security Model

We assume $\sqcap = \{Setup, MW - Extract, TokenGen, MW - Signcrypt, MW-Unsigncrypt, MW-Test\}$ as the scheme and polynomial time algorithm adversary A. $MWAR - ID - SET$ achieves two main security notion of $IND - CCA2$ and $EUF - CMA$. However, our scheme adds the security notion of ID-based indistinquishability to IND-CCA2 and is coined as IND-ID-CCA2, similarly presented in [55] via the standard model..

1. $Setup$: The challenger A executes the security parameter k and outdoors K with a randomly chosen witness $w \in W$ and generates $x \in X$ of the relation R. It gives out the relation R to the adversary A.

2. Phase 1: The mobile merchant adversary A then issues $(\wedge_1, \wedge_2, ..., \wedge_{n-1})$. It is assumed that such query is of:
   - $MW-Query(ID_i)$: The merchant executes $H(.)$ and generates mrk_i which corresponding to ID_i as the identity. The recovered mrk_i is forwarded to A.
   - $TokenGen(ID_i)$: The merchant executes the $MW - Unsigncryption$ to generates tdk_i via the witness relation R. The algorthm then forwards tdk_i to A.

3. $MW - Challenge$: When the phase comes to an end, two messages (m_1, m_2) with equal-length and ID^* is submitted by A to the challenger and wishes to be challenged. But (m_1, m_2) were both not issued during signcryption and ID^* was never extracted during phase 1 section. Given this, the challenger randomly chooses $t \in \{0, 1\}$ and returns $CT_1 = MW - Signcrypt(m_t, ID^*, w^*)$. Again, a challenge ciphertext token $mrk^* = (ID^*, x^*)$ is issued by the execution of $TokenGen$ phase $mrk^* \leftarrow mrk(tdk, m_t, x^*)$ and it output mrk^* to A.

4. $MW - Unsigncrypt$: The merchant executes an unsigncryption algorithm to unsigncrypt CT_1. The merchant obtains mrk_1 which corresponds to a public key of ID_i. The plaintext m_i is forwarded to A.

5. Phase 2: The merchant adversary issue the query $(\wedge_1, \wedge_2, ..., \wedge_n)$. The query is of the form:
   - $MW - Query$. A similar response as in phase 1 is given because $ID_i \neq ID^*$.
   - $TokenGen(ID_1)$. Given $x \neq x^*$, the merchant respond same as in phase 1.

6. Result. The adversary A does a guess v' of v. Since $v' = v$, then the adversary will win the game.

   The adversary advantage in breaking the scheme is noted as: $ADV_{MWAR-ID-SET}(k) = Pr[v' = v] - \frac{1}{2}$ as a negligible probability.

5 Construction

A detailed construction of our proposed scheme is outlined as follows:

1. On input a secured parameter k, the algorithm output public parameter K, with MSK as master secret key.
   - Two multiplicative group G and G_T are generated by the system with the same order of lemgth θ bits with a bilinear map $e : G \times G \to G_T$. The group generater $P \in G$ is selected.
   - The algorithm exploits keyed permutation $F : \{0, 1\}^s \times \{0, 1\}^n \to Z_p^*$ with a positive interger $D = k(i)$ and $L = b(i)$, it then activate a random value r_1 from $\{0, 1\}^L$. Message authentication code (MAC), $MAC = GSV$. Thus, generate, sign, verify (GSV). After executing $G(i)$, it obtains r_2. It then set master token key as $MTK_1 = (r_1, r_2)$.
   - A hash functions $H_a : \{0, 1\}^\tau \to Z_p^*$, $H_b : \{0, 1\}^* \to G$, $H_c : A \times G \times G_T \to \{0, 1\}^{\tau + r_1}$, where r_1 represent random numbers and τ as length of message. $(\tau_1, \tau_2) \in Z_p^2$ is randomly chosen and $R_v = P^{\tau_1}$, $R_m = P^{\tau_2}$. The paramrter $K = (A, \tau, G, G_T, P, R_v, R_m, MAC, H_a, H_b, H_c)$ is made public (published)

2. $MW-Extract$: With an $ID \in \{0, 1\}$ as string, the system computes $Q_{ID} = H_b(ID) \in G$ and private key $mrk_{ID} = (Q_{ID}^{\tau_1}, Q_{ID}^{\tau_2})$. It should therefore be noted that (τ_1, τ_2) are secret value randomly chosen by the algorithm.

3. $TokenGen$: The algorithm with an input string $ID \in \{0, 1\}^*$, the computation $Q_{ID} = H_b(ID) \in G$ is executed and the token $tdk_{1_{ID}} = (Q_{ID}^{\tau_2})$ is generated.

4. $MW-Signcrypt$: The algorithm with an input public parameter K, string ID, it executes $Q_{ID} = H_b(ID) \in G$ and a **signcryption** $m_1 \in G$ is triggered by choosing two random values $(q_1, q_2) \in Z_p^*$. The ciphertext is set as $CT_1 = (CT_a, CT_b, CT_c, CT_d)$ as :

$$CT_a = H_b(e(Q_{ID}, R_m)^{q_1}) \cdot m_1^{q_1}, \qquad CT_b = P^{q_1}$$

$$CT_c = P^{q_2} \quad CT_d = (m_1 \| w) \oplus H_b(CT_a \| CT_b \| Z \| e(Q_{ID}, R_v)^{q_2}).$$

The signature $Z \leftarrow S(r_2, CT_c)$ is used to signcrypt the ciphertext of the employed MAC. The signcrypted tag Z is used to verify signcrypted ciphertext CT_c

5. $MW-Unsigncrypt$: To **unsigncrypt**, the algorithm with an input the ciphertext CT_1, private **unsigncryption** key $mrk = (Q_{ID}^{\tau_1}, Q_{ID}^{\tau_2})$ with $CT_1 = (CT_a, CT_b, CT_c, CT_d)$ corresponding to an identity ID. The algorithm executes $(m_1 \| w') = CT_b \oplus H_b(CT_a \| CT_b \| CT_c \| e(CT_c, Q_{ID}^{\tau_1}))$. The algorithm do a check of $CT_a = (m_1')\|x'$ and $CT_b = P^{q_1'}$ to determine whether they are equal. If they are equal, the algorithm returns m_1, contrarily, it returns $\perp$.

6. $MW-Test$: With a given **signcrypted** ciphertext CT_{1_A} with trapdoor tdk_{1_A} and a different **signcrypted** ciphertext CT_{1_B} with a trapdoor tdk_{1_B}. The algorithm determines whether $m_{1_A} = m_{1_B}$ is equal or not. The algorithm does this by executing:

$$TD_A = \frac{CT_{a_A}}{H_b(e(CT_{a_A}, R_{m_A}))}, \quad TD_B = \frac{CT_{a_B}}{H_b(e(CT_{a_B}, R_{m_B}))}.$$

If the above equation holds, the algorithm then output 1 on success and 0 on failure.

Construction Correctness.
We assume that $CT_1 = (CT_a, CT_b, CT_c, CT_d)$.). Test algorithm executes:

$$CT_{1_A} = \frac{CT_{a_A}}{H_b(e(CT_{a_A}, R_{m_A}))}, \quad CT_{1_B} = \frac{CT_{a_B}}{H_b(e(CT_{a_B}, R_{m_B}))}$$

$$CT_{1_A} = \frac{H_b(e(Q_{ID}, P^{\tau_2})^{q_1}) \cdot m_{1_A}^{q_1}}{H_b(e(Q_{ID}, P^{\tau_2})^{q_1})}, CT_{1_B} = \frac{H_b(e(Q_{ID}, P^{\tau_2})^{q_1}) \cdot m_{1_B}^{q_1}}{H_b(e(Q_{ID}, P^{\tau_2})^{q_1})}$$

$$CT_{1_A} = m_{1_A}^{q_1}, \quad CT_{1_B} = m_{1_B}^{q_1}$$

Hence, $m_{1_A}^{q_1} = m_{1_B}^{q_1}$

From the above, the algorithm output 1 on success and 0 on failure.

Therefore:

$$e(CT_{b_A}, R_{m_B}) = e(CT_{b_A}, R_{m_B}).$$

$$e(CT_{b_A}, R_{m_B}) = (P^{q_1}, P^{\tau_2}) = e(P, P)^{q_1 \tau_2},$$

$$e(CT_{b_A}, R_{m_B}) = (P^{q_1}, P^{\tau_2}) = e(P, P)^{q_1 \tau_2}.$$

This implies that if, $m_{1_A} = m_{1_B}$, then

$$e(CT_{b_A} = R_{m_B}) = e(CT_{b_A} = R_{m_B}).$$

6 Security Analysis

In this section, we consider a formal security property of IND-CCA2 and EUF-CMA [60]. Our scheme adds the notion of ID-based indistinquishability to IND-CCA2 and referred to as IND-ID-CCA2.

6.1 IND-CCA2 Security

Our MWAR-ID-SET is $(SET_\varepsilon, t_s, q_{ks}, q_{ns}, q_{us})$-IND-CCA2 secure if $(\varepsilon_{mdbdh}, t_s) - mDBHDH$ 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:

$$\varepsilon_{SET} \le \varepsilon_{mdbdh} + \varepsilon_{H_1} + \varepsilon_{H_2} + \frac{q_{ks}+q_{us}+3}{p} + \frac{q_{ns}}{p^2}.$$

Where t_s refers to index period time, q_{ks} refers to number of extraction key queries, q_{ns} represent number of signcryption queries and q_{us} represents number of unsigncryption queries. Therefore, the security analysis with a collission resistant hash function proves our scheme secured.

6.2 EUF-CMA Unforgeability

Proof Theorem: This section outlines the security proof of unforgeability against adaptive CMA derived from the security constructions in Chow[41] ID-based **signcryption** cryptosystem. Thus, it is expected that the adversary can forge a ciphertextof a message m_1, if the assumption $CT_1 = (CT_a, CT_b, CT_c, CT_d)$ corresponding to a user identity ID holds. Thus, $CT_d = (m_1 \| w) \oplus H_3(CT_a \| CT_b \| CT_c \| e(Q_{ID}, R_v))^{q_2}$ is regarded as the signature of the message $m_1 \| w$, where $e(Q_{ID}, R_v)^{q_2}$ is regarded as the pairing of a corresponding user with secret **signcryption** key R_v. It is however noted that the difficulty of CDH problem makes the scheme unforgeable via the random oracle model.

6.3 Security Analysis of Token Key

Further details on the token security analysis can be accessed in [1]. The token security analysis experiment to our scheme is defined as: $EXP_{MWAR-ID-SET_A}^{IND-ID-CCA2}(k)$.

With a security parameter k, a master token key $MTK_1 = (r_1, r_2)$ and A adversary against token security. According to [1], the adversary A win the game if $b' = b$, which shows that the output of the experiment is 1 on success and 0 on failure. Adversary A advantage in the experiment is defined as:

$$Adv_{MWAR-ID-SET}^{IND-ID-CCA2}(w) = |Pr[Exp_{MWAR-ID-SET}^{IND-ID-CCA2}] - \tfrac{1}{2}|$$

However, the probability for the adversary to win the game is negligible, hence proves our construction secured.

7 Comparison

A security strength comparison computations with existing **signcryption** schemes are outlined in Table 1. Constructions in ID-based **Signcryption** cryptosystem in [21, 23, 60, 64] are compared to with respect to security strength. The parameters for our comparison includes group multiplication, group exponentiation, inverse computations, pairing operation, test for equality, and support for EUF-CMA.

Table 1: The performance computational cost and Communication overheads

Scheme	G_{Mult}	G_{Exp_a}	$G_{T_{Mult}}$	$G_{T_{Exp_a}}$	$G_{T_{Inv}}$	Pr	IND-CCA2	EUF-CMA	ET
[21]	$2n_{u_a} + 2n_{m_a} + 1$	3	5	1	1	7(+2)	⊠	√	No
[23]	$2n_{u_a} + 2n_{m_a} + 1$	3	5	1	1	7(+2)	⊠	⊠	No
[60]	$2n_{u_a} + 2n_{m_a} + 1$	7	5	1	1	7(+2)	√	√	No
[64]	$2n_{u_a} + 2n_{m_a} + 3$	7	5	1	1	7	√	√	No
Ours	$2n_{u_a} + 2n_{m_a} + 1$	7	3	2	2	8	√	√	Yes

Legend: $''G_{Mult}$": multiplication in group G, $''G''_{Exp_a}$: exponentiation in group G, $''G''_{T_{Exp_a}}$: exponentiation in group G_T, $G_{T_{Inv}}$: inverse computation in group G_T, $''n_m, n''_u$: length of identity in bits string, $''Pr$": pairing operations in the form $x(+y)$ as in [23], $''ET''$: equality test, $''$⊠$''$: not supportive, $''\surd''$: supportive .

Table 2: Running Times with Symbols

Symbols	Description	Times
G_{Exp_a}	G exponentiation operation	6.3937
$G_{T_{Exp_a}}$	G_T exponentiation operation	1.9518
T_{p_a}	Operation with pairing	11.4173
T_{h_a}	Hash functions	000853
G_{Mult}	Multiplication operation in G	0.047
$G_{T_{Mult_a}}$	Multiplication operation in G_T	0.0119

The Pairing-Based Cryptography (PBC) Library [65] is used to quantify the time consumption of signcryption, unsigncryption and test operations. 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) Core (TM) i5-4460 CPU with 3.20GHZ and 4Gb RAM. The code was executed several times and average time of execution extracted (see Table 2). With respect to the scheme in [66], and other pairing-based constructions with a security level of 1024-bit RSA, a supersingular curve $z^2 = x^3 + x$ with an embedded degree of 2 is adopted. Also, $q = 2^{159} + 2^{17} + 1$ noted as a 160 bit Solinas prime 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 Table 1 and computational results in Table 2.

Therefore, it is clear that our scheme support equality test as compared with other schemes without equality test. The computation of trapdoor and trapdoor delegation to the tester is equally achieved in our scheme. In terms of computational cost, our scheme has a lower computation cost as compared to existing schemes. Also, the support for IND-ID-CCA2 is featured in our sccheme as compared to other existing scheme with IND-CCA support. However, the inverse compuatation to recover the message achieves a ligh computational cost as compared to others in Table 1. This is pardonable due to the additional trapdoor computations featured in our scheme.

8 Conclusion

The construction $MWAR - ID - SET$ achieves a security improvement in mobile money service security in Ghana via the adoption signcryption cryptosystem. Data forgery and re-play attack is curtailed in our construction and the simultaneous benefit of PKE and digital signature is achieved in our scheme using the random oracle model. A desirable security property of EUF-CMA is achieved in our construction. In spite of other applications and extentions of identity based cryptosystem [67]–[70], our scheme achieves a remarkable achievement in indentity based cryptosystem.

Conflict of Interest The authors declare no conflict of interest.

Acknowledgment We will like to use this opportunity to thank the anonymous reviewers for their kind support and consideration.

References

[1] S. Alornyo, K. K. Mireku, A. Tonny-Hagan, X. Hu, "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), 82–87, IEEE, 2019, doi:10.1109/ICSIoT47925.2019.00021.

[2] F. Li, H. Xiong, Y. Liao, "A generic construction of identity-based signcryption," in 2009 International Conference on Communications, Circuits and Systems, 291–295, IEEE, 2009, doi:10.1109/ICCCAS.2009.5250509.

[3] K. Bentahar, P. Farshim, J. Malone-Lee, N. P. Smart, "Generic constructions of identity-based and certificateless KEMs," Journal of Cryptology, **21**(2), 178–199, 2008, doi:10.1007/s00145-007-9000-z.

[4] L. Chen, Z. Cheng, J. Malone-Lee, N. P. Smart, "An Efficient ID-KEM Based On The Sakai-Kasahara Key Construction." IACR Cryptol. ePrint Arch., **2005**, 224, 2005.

[5] E. Kiltz, D. Galindo, "Direct chosen-ciphertext secure identity-based key encapsulation without random oracles," in Australasian Conference on Information Security and Privacy, 336–347, Springer, 2006, doi:https://doi.org/10.1007/11780656_28.

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in Workshop on the theory and application of cryptographic techniques, 47–53, Springer, 1984, doi:https://doi.org/10.1007/3-540-39568-7_5.

[7] Y. Zheng, "Digital signcryption or how to achieve cost (signature or encryption) cost (signature)+ cost (encryption)," in Annual international cryptology conference, 165–179, Springer, 1997, doi:https://doi.org/10.1007/BFb0052234.

[8] A. Fiat, A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in Conference on the theory and application of cryptographic techniques, 186–194, Springer, 1986, doi:https://doi.org/10.1007/3-540-47721-7_12.

[9] L. C. Guillou, J.-J. Quisquater, "A "paradoxical" indentity-based signature scheme resulting from zero-knowledge," in Conference on the Theory and Application of Cryptography, 216–231, Springer, 1988, doi:https://doi.org/10.1007/0-387-34799-2_16.

[10] J. Malone-Lee, "Identity-Based Signcryption." IACR Cryptol. ePrint Arch., **2002**, 98, 2002.

[11] P. S. Barreto, B. Libert, N. McCullagh, J.-J. Quisquater, "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, 515–532, Springer, 2005, doi:https://doi.org/10.1007/11593447_28.

[12] X. Boyen, "Multipurpose identity-based signcryption," in Annual International Cryptology Conference, 383–399, Springer, 2003, doi:https://doi.org/10.1007/978-3-540-45146-4_23.

[13] S. S. Chow, S.-M. Yiu, L. C. Hui, K. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in International Conference on Information Security and Cryptology, 352–369, Springer, 2003, doi:https://doi.org/10.1007/978-3-540-24691-6_26.

[14] B. Libert, J.-J. Quisquater, "A new identity based signcryption scheme from pairings," in Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674), 155–158, IEEE, 2003, doi:10.1109/ITW.2003.1216718.

[15] T. H. Yuen, V. K. Wei, "Constant-Size Hierarchical Identity-Based Signature/Signcryption without Random Oracles." IACR Cryptol. ePrint Arch., **2005**, 412, 2005.

[16] Y. Zheng, H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information processing letters, **68**(5), 227–233, 1998, doi:https://doi.org/10.1016/S0020-0190(98)00167-7.

[17] F. Bao, R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in International Workshop on Public Key Cryptography, 55–59, Springer, 1998, doi:https://doi.org/10.1007/BFb0054014.

[18] J.-B. Shin, K. Lee, K. Shim, "New DSA-verifiable signcryption schemes," in International Conference on Information Security and Cryptology, 35–47, Springer, 2002, doi:https://doi.org/10.1007/3-540-36552-4_3.

[19] D. H. Yum, P. J. Lee, "New signcryption schemes based on KCDSA," in International Conference on Information Security and Cryptology, 305–317, Springer, 2001, doi:https://doi.org/10.1007/3-540-45861-1_23.

[20] F. Li, M. K. Khan, "A survey of identity-based signcryption," IETE Technical Review, **28**(3), 265–272, 2011, doi:https://doi.org/10.4103/0256-4602.81236.

[21] Y. Yu, B. Yang, Y. Sun, S.-l. Zhu, "Identity based signcryption scheme without random oracles," Computer Standards & Interfaces, **31**(1), 56–62, 2009, doi:https://doi.org/10.1016/j.csi.2007.10.014.

[22] K. G. Paterson, J. C. Schuldt, "Efficient identity-based signatures secure in the standard model," in Australasian Conference on Information Security and Privacy, 207–222, Springer, 2006, doi:https://doi.org/10.1007/11780656_18.

[23] Z. Jin, Q. Wen, H. Du, "An improved semantically-secure identity-based signcryption scheme in the standard model," Computers & Electrical Engineering, **36**(3), 545–552, 2010, doi:https://doi.org/10.1016/j.compeleceng.2009.12.009.

[24] F. Li, Y. Liao, Z. Qin, "Analysis of an identity-based signcryption scheme in the standard model," IEICE transactions on fundamentals of electronics, communications and computer sciences, **94**(1), 268–269, 2011, doi:https://doi.org/10.1587/transfun.E94.A.268.

[25] F. Li, J. Gao, Y. Hu, "ID-based threshold unsigncryption scheme from pairings," in International Conference on Information Security and Cryptology, 242–253, Springer, 2005, doi:https://doi.org/10.1007/11599548_21.

[26] S. Duan, Z. Cao, R. Lu, "Robust ID-based threshold signcryption scheme from pairings," in Proceedings of the 3rd international conference on Information security, 33–37, 2004, doi:https://doi.org/10.1145/1046290.1046298.

[27] C. Peng, X. Li, "An identity-based threshold signcryption scheme with semantic security," in International Conference on Computational and Information Science, 173–179, Springer, 2005, doi:https://doi.org/10.1007/11596981_26.

[28] F. Li, Y. Yu, "An efficient and provably secure ID-based threshold signcryption scheme," in 2008 International Conference on Communications, Circuits and Systems, 488–492, IEEE, 2008, doi:10.1109/ICCCAS.2008.4657820.

[29] S. S. D. Selvi, S. S. Vivek, C. P. Rangan, N. Jain, "Cryptanalysis of Li et al.'s identity-based threshold signcryption scheme," in 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, **2**, 127–132, IEEE, 2008, doi:10.1109/EUC.2008.187.

[30] F. Li, X. Xin, Y. Hu, "ID-based threshold proxy signcryption scheme from bilinear pairings," International Journal of Security and Networks, **3**(3), 206–215, 2008, doi:https://doi.org/10.1504/IJSN.2008.020095.

[31] X. Li, K. Chen, "Identity based proxy-signcryption scheme from pairings," in IEEE International Conference onServices Computing, 2004.(SCC 2004). Proceedings. 2004, 494–497, IEEE, 2004, doi:10.1109/SCC.2004.1358050.

[32] M. Wang, H. Li, Z. Liu, "Efficient identity based proxy-signcryption schemes with forward security and public verifiability," in International Conference on Networking and Mobile Computing, 982–991, Springer, 2005, doi:https: //doi.org/10.1007/11534310 103.

[33] Q. Wang, Z. Cao, "Two proxy signcryption schemes from bilinear pairings," in International Conference on Cryptology and Network Security, 161–171, Springer, 2005, doi:https://doi.org/10.1007/11599371 14.

[34] S. Duan, Z. Cao, Y. Zhou, "Secure delegation-by-warrant ID-based proxy signcryption scheme," in International Conference on Computational and Information Science, 445–450, Springer, 2005, doi:https://doi.org/10.1007/11596981-65.

[35] M. Wang, Z. Liu, "Identity based threshold proxy signcryption scheme," in The Fifth International Conference on Computer and Information Technology (CIT'05), 695–699, IEEE, 2005, doi:10.1109/CIT.2005.129.

[36] J. Zhang, J. Mao, "A novel identity-based multi-signcryption scheme," Computer Communications, **32**(1), 14–18, 2009, doi:https://doi.org/10.1016/j.comcom.2008.07.004.

[37] S. S. D. Selvi, S. S. Vivek, C. P. Rangan, "Breaking and fixing of an identity based multi-signcryption scheme," in International Conference on Provable Security, 61–75, Springer, 2009, doi:https://doi.org/10.1007/978-3-642-04642-1 7.

[38] M. Zhang, B. Yang, S. Zhu, W. Zhang, "Efficient secret authenticatable anonymous signcryption scheme with identity privacy," in International Conference on Intelligence and Security Informatics, 126–137, Springer, 2008, doi:https://doi.org/10.1007/978-3-540-69304-8 14.

[39] F.-g. Li, S. Masaaki, T. Tsuyoshi, "Analysis and improvement of authenticatable ring signcryption scheme," Journal of Shanghai Jiaotong University (Science), **13**(6), 679–683, 2008, doi:https://doi.org/10.1007/s12204-008-0679-2.

[40] Z. Zhu, Y. Zhang, F. Wang, "An efficient and provable secure identity-based ring signcryption scheme," Computer standards & interfaces, **31**(6), 1092–1097, 2009, doi:https://doi.org/10.1016/j.csi.2008.09.023.

[41] Y. Yu, F. Li, C. Xu, Y. Sun, "An efficient identity-based anonymous signcryption scheme," Wuhan University Journal of Natural Sciences, **13**(6), 670–674, 2008, doi:https://doi.org/10.1007/s11859-008-0607-1.

[42] L. Zhun, F. Zhang, "Efficient ID–based ring signature and ring signcryption schemes," in 2008 International Conference on Computational Intelligence and Security, volume 2, 303–307, IEEE, 2008, doi:10.1109/CIS.2008.51.

[43] H. Xiong, Z. Qin, F. Li, "Cryptanalysis of an Identity Based Signcryption without Random Oracles," Fundamenta Informaticae, **107**(1), 105–109, 2011, doi:10.3233/FI-2011-395.

[44] F. Li, B. Liu, J. Hong, "An efficient signcryption for data access control in cloud computing," Computing, **99**(5), 465–479, 2017, doi:https://doi.org/10.1007/s00607-017-0548-7.

[45] V. Kirtane, C. P. Rangan, "RSA-TBOS signcryption with proxy re-encryption," in Proceedings of the 8th ACM workshop on Digital rights management, 59–66, 2008, doi:https://doi.org/10.1145/1456520.1456531.

[46] J. Malone-Lee, W. Mao, "Two birds one stone: signcryption using RSA," in Cryptographers' Track at the RSA Conference, 211–226, Springer, 2003, doi:https://doi.org/10.1007/3-540-36563-X_14.

[47] C. Wang, X. Cao, "An improved signcryption with proxy re-encryption and its application," in 2011 Seventh International Conference on Computational Intelligence and Security, 886–890, IEEE, 2011, doi:10.1109/CIS.2011.200.

[48] W. Huige, W. Caifen, C. Hao, "ID-based proxy re-signcryption scheme," in 2011 IEEE International Conference on Computer Science and Automation Engineering, volume 2, 317–321, IEEE, 2011, doi:10.1109/CSAE.2011.5952478.

[49] X. Tian, X. Wang, A. Zhou, "DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS," in 2009 IEEE International Conference on Cloud Computing, 25–32, IEEE, 2009, doi:10.1109/CLOUD.2009.65.

[50] Q. Liu, C. C. Tan, J. Wu, G. Wang, "Reliable re-encryption in unreliable clouds," in 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, 1–5, IEEE, 2011, doi:10.1109/GLOCOM.2011.6133609.

[51] S. Yu, C. Wang, K. Ren, W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in 2010 Proceedings IEEE INFOCOM, 1–9, Ieee, 2010, doi:10.1109/INFCOM.2010.5462174.

[52] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE transactions on parallel and distributed systems, **24**(1), 131–143, 2012, doi:10.1109/TPDS.2012.97.

[53] M. Nabeel, N. Shang, E. Bertino, "Privacy preserving policy-based content sharing in public clouds," IEEE Transactions on Knowledge and Data Engineering, **25**(11), 2602–2614, 2012, doi:10.1109/TKDE.2012.180.

[54] K. Yang, X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE transactions on parallel and distributed systems, **25**(7), 1735–1744, 2013, doi:10.1109/TPDS.2013.253.

[55] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE transactions on knowledge and data engineering, **25**(10), 2271–2282, 2011, doi:10.1109/TKDE.2011.78.

[56] F. Li, H. Zhang, T. Takagi, "Efficient signcryption for heterogeneous systems," IEEE Systems Journal, **7**(3), 420–429, 2013, doi:10.1109/JSYST.2012.2221897.

[57] Y. Sun, H. Li, "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction," Science China Information Sciences, **53**(3), 557–566, 2010, doi:https://doi.org/10.1007/s11432-010-0061-5.

[58] Q. Huang, D. S. Wong, G. Yang, "Heterogeneous signcryption with key privacy," The Computer Journal, **54**(4), 525–536, 2011, doi:10.1093/comjnl/bxq095.

[59] J. H. An, Y. Dodis, T. Rabin, "On the security of joint signature and encryption," in International Conference on the Theory and Applications of Cryptographic Techniques, 83–107, Springer, 2002, doi:https://doi.org/10.1007/3-540-46035-7_6.

[60] F. Li, T. Takagi, "Secure identity-based signcryption in the standard model," Mathematical and Computer Modelling, **57**(11-12), 2685–2694, 2013, doi:https://doi.org/10.1016/j.mcm.2011.06.043.

[61] L. Chen, J. Malone-Lee, "Improved identity-based signcryption," in International Workshop on Public Key Cryptography, 362–379, Springer, 2005, doi:https://doi.org/10.1007/978-3-540-30580-4_25.

[62] B. Waters, "Efficient identity-based encryption without random oracles," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 114–127, Springer, 2005, doi:https://doi.org/10.1007/11426639_7.

[63] Y. Ming, Y. Wang, "Cryptanalysis of an Identity Based Signcryption Scheme in the Standard Model." IJ Network Security, **18**(1), 165–171, 2016, doi:10.6633/IJNS.

[64] G. Zhu, H. Xiong, Z. Qin, "Fully secure identity based key-insulated signcryption in the standard model," Wireless personal communications, **79**(2), 1401–1416, 2014, doi:https://doi.org/10.1007/s11277-014-1936-3.

[65] B. Lynn, et al., "The stanford pairing based crypto library," Privacy preservation scheme for multicast communications in smart buildings of the smart grid, **324**, 2013.

[66] H. Xiong, Q. Mei, Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," IEEE Systems Journal, **14**(1), 310–320, 2019, doi:10.1109/JSYST.2018.2890126.

[67] S. Alornyo, M. Asante, X. Hu, K. K. Mireku, "Encrypted Traffic Analytic using Identity Based Encryption with Equality Test for Cloud Computing," in 2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST), 1–4, IEEE, 2018, doi:10.1109/ICASTECH.2018.8507063.

[68] S. Alornyo, E. Aidoo, K. K. Mireku, B. Kwofie, X. Hu, M. Asante, "ID-Based Outsourced Plaintext Checkable Encryption in Healthcare Database," in 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), 48–53, IEEE, 2019, doi:10.1109/ICSIoT47925.2019.00016.

[69] S. Alornyo, Y. Zhao, G. Zhu, H. Xiong, "Identity Based Key-Insulated Encryption with Outsourced Equality Test." IJ Network Security, **22**(2), 257–264, 2020, doi:10.6633/IJNS.860.

[70] S. Alornyo, A. E. Mensah, A. O. Abbam, "Identity-based Public Key Cryptographic Primitive with Delegated Equality Test Against Insider Attack in Cloud Computing," International Journal of Network Security, **22**(5), 743–751, 2020, doi:10.6633/IJNS.202009_22(5).04.