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

Seth Alornyo¹, Mustapha Adamu Mohammed¹,², Francis Botchey¹,³, Collinson Colin M. Agbesi¹

¹Koforidua Technical University, Computer Science Department, KTU, Koforidua, Ghana
²Kwame Nkrumah University of Science and Technology, Computer Science Department, KNUST, Kumasi, Ghana
³University 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 merchant receives valid transaction details such as transaction ID, tdID and finds out the content M₁ as well as the token information tdkID from the transaction details TSD.
- The adversary (insider) attains the ciphertext CT₁ of a guessed message M₁ and token tdkID.
- The adversary checks if the test Test(CT₁, TSD, tdID) = 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 simultaneous 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 [7]. 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 [4–6] to achieve confidentiality and unforgeability instantiation in the standard model.

Signcryption scheme unveiled in [7] did not propose a securi-
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 flavors 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 [50] 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 [21–24] 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 a generator of \( G \). A bilinear map \( e: G \times G \to G_T \) satisfies the following properties:

1. Bilinearity: For any \( g, h \in G \), and \( b \in \mathbb{Z}_q \), \( e(g^a, h^b) = e(g, h)^{ab} \).
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 \( e: G \times G \to G_T \) be an admissible bilinear map and let \( q \) be a generator of \( G \). The BDH problem \( (q, G, G_T, e) \) is as follows: Given \( (q, q^a, q^b, q^c) \), for random \( c, d, f \in \mathbb{Z}_q^* \), for any randomized algorithm, \( A \) computes the value \( e(q, q)^{cd} \in G_T \) with advantage:

\[ ADV^{BDH}_A \Pr[A(q, q^a, q^b, q^c) = e(q, q)^{cd}] \]

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

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: \( \text{Setup}, MW \rightarrow \text{Extract}, \text{TokenGen}, MW \rightarrow \text{Signcrypt}, MW \rightarrow \text{Unsigncrypt}, MW \rightarrow \text{Test} \). \( M_T \) 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 $WnsGen(w) = x$ with the relation $R$ satisfied \(\Box\).

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 $tdk_A$ with its corresponding $ID_A$, the ciphertext $CT_A \in CT_1$ with its corresponding receiver $ID_B$ derived from the token $tdk_B$ 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 $\square = \{Setup, MW − Extract, TokenGen, MW − Signcrypt, MW − Unsigncrypt, MW − Test\}$ 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 indistinguishability to IND-CCCA2 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 $(\lambda_1, \lambda_2, ..., \lambda_{n-1})$. It is assumed that such query is of:

   - **MW − Query:** $H(\cdot)$ and generates $mrk$, which corresponding to $ID_1$, as the identity. The recovered $mrk$ is forwarded to $A$.

   - **TokenGen:** $ID_1$: The merchant executes $MW − Unsigncryo$ to generates $tdk_1$ via the witness relation $R$. The algorithm then forwards $tdk_1$ 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 $CT_1 = MW − Signcrypt(m_1, ID^*, w^*)$. Again, a challenge ciphertext token $mrk^* = (ID^*, x^*)$ is issued by the execution of $TokenGen$ phase $mrk^* \leftarrow mrk(tdk, m, x^*)$ 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 $ID_1$. The plaintext $m_1$ is forwarded to $A$.

5. Phase 2: The merchant adversary issue the query $(\lambda_1, \lambda_2, ..., \lambda_{n})$. The query is of the form:

   - **MW − Query:** $H(\cdot)$ and generates $mrk$, which corresponding to $ID_1$, as the identity. The recovered $mrk$ is forwarded to $A$.

   - **TokenGen:** $ID_1$: Given $x \neq x^*$, the merchant respond same as in phase 1.

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 length $\theta$ bits with a bilinear map $e : G \times G \rightarrow G_T$. The group generator $P \in G$ is selected.

   - The algorithm exploits key permutation $F : \{0, 1\}^m \rightarrow \{0, 1\}^*$ with a random integer $D = k(i)$ and 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 $H_a : \{0, 1\}^m \rightarrow Z_p, H_b : \{0, 1\}^* \rightarrow G, H_c : A \times G \times G_T \rightarrow \{0, 1\}^{\tau r_1}$, where $r_1$ represent random numbers and $\tau$ as length of message. $(\tau_1, \tau_2) \in Z_p^2$ is randomly chosen and $R_1 = P^{r_1}, R_2 = P^{r_2}$. The parameter $K = (\lambda, \tau, G, G_T, P, R_1, R_2, MAC, H_a, H_b, H_c)$ 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 $mrk_{ID} = (Q_{ID}^0, Q_{ID}^1)$. It should therefore be noted that $(\tau_1, \tau_2)$ 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 $tdk_{ID} = (Q_{ID}^0)$ is generated.
4. **MW - Signcrypt**: The algorithm with an input public parameter $K$, string $ID$ executes $Q_{ID} = H_p(ID) \in G$ and a signcryption $m_1 \in G$ is triggered by choosing two random values $(q_1, q_2) \in \mathbb{Z}_p^*$. The ciphertext is set as $CT_1 = (CT_a, CT_b, CT_c, CT_d)$ as:

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

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

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 ciphertext $CT_1$, private unsigncryption key $mrk = (Q_{ID}, Q_{ID}^2)$ with $CT_1 = (CT_a, CT_b, CT_c, CT_d)$ corresponding to an identity $ID$. The algorithm executes $(m_1||w) = CT_b @ H_b(CT_a[CT_c][CT_d])e(CT_c, Q_{ID}^2)$). The algorithm do a check of $CT_a = (m_1||w)$ and $CT_b = P^{q_1}$ to determine whether they are equal. If they are equal, the algorithm returns $m_1$, contrarily, it returns ⊥.

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:

$$TD_A = \frac{CT_{1_a}}{H_b(e(CT_{1_a}, R_m))}, \quad TD_B = \frac{CT_{1_b}}{H_b(e(CT_{1_b}, R_m))}.$$ 

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:

$$CT_{1_a} = \frac{CT_{1_a}}{H_b(e(CT_{1_a}, R_m))}, \quad CT_{1_b} = \frac{CT_{1_b}}{H_b(e(CT_{1_b}, R_m))}$$

$$CT_{1_a} = \frac{H_b(e(Q_{ID}, P^r)^{q_1}) \cdot m_1^{q_1}}{H_b(e(Q_{ID}, P^r)^{q_2})}, \quad CT_{1_b} = \frac{H_b(e(Q_{ID}, P^r)^{q_1}) \cdot m_1^{q_1}}{H_b(e(Q_{ID}, P^r)^{q_2})}.$$ 

Hence, $m_{1_a} = m_{1_b}$

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

**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 ciphertext of 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, $CT_d = (m_1||w) @ H_2(CT_a[CT_c][CT_d])e(Q_{ID}, R_m)^{q_2}$ is regarded as the signature of the message $m_1||w$, where $e(Q_{ID}, R_m)^{q_2}$ is regarded as the pairing of a corresponding user with secret signcryption key $R_m$. It is however noted that the difficulty of CDH problem makes the scheme unforgeable via the random oracle model.

6.1 **IND-CCA2 Security**

Our MWAR-ID-SET is $(SET_c, t_e, q_{ns}, q_{ns})$-IND-CCA2 secure if $(\epsilon_{mWAR-ID-SET}) = mDBDH$ assumption holds. Thus, $H_1$ and $H_2$ serves as $(\epsilon_{H_1})$ and $(\epsilon_{H_2})$ are both collision resistant hash functions, such that:

$$\epsilon_{SET} \leq \epsilon_{mWAR} + \epsilon_{H_1} + \epsilon_{H_2} + \frac{q_{ns}q_{ns} + q_{ns}^2}{p} + \frac{q_{ns}^2}{p^2}.$$ 

Where $t_e$ refers to index period time, $q_{ns}$ refers to number of extraction key queries, $q_{ns}$ represent number of signcryption queries and $q_{ns}$ represents number of unsigncryption queries. Therefore, the security analysis with a collision 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 ciphertext of 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, $CT_d = (m_1||w) @ H_2(CT_a[CT_c][CT_d])e(Q_{ID}, R_m)^{q_2}$ is regarded as the signature of the message $m_1||w$, where $e(Q_{ID}, R_m)^{q_2}$ is regarded as the pairing of a corresponding user with secret signcryption key $R_m$. 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: $\text{EXF}_{MWAR-ID-SET}$, $(k)$.

With a security parameter $k$, a master token key $MT_{K_1} = (r_1, r_2)$ 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:

$$\text{Adv}_{MWAR-ID-CCA2} = |Pr[\text{Exp}_{MWAR-ID-CCA2} - \frac{1}{2}]|$$

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>
<thead>
<tr>
<th>Scheme</th>
<th>$G_{mul}$</th>
<th>$G_{ex}$</th>
<th>$G_{exp}$</th>
<th>$G_{hash}$</th>
<th>$Pr$</th>
<th>IND-CCA2</th>
<th>EUF-CMA</th>
<th>ET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ours</td>
<td>2$n_a$x$n_u$ + 1+ 3</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$T_{EUF}$</td>
<td>$T_{ET}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2$n_a$x$n_u$ + 1+ 3</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$T_{EUF}$</td>
<td>$T_{ET}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2$n_a$x$n_u$ + 1+ 3</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$T_{EUF}$</td>
<td>$T_{ET}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2$n_a$x$n_u$ + 1+ 3</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$T_{EUF}$</td>
<td>$T_{ET}$</td>
<td></td>
</tr>
</tbody>
</table>

Legend: "$G_{mul}$": multiplication in group $G$, "$G'_{exp}$": exponentiation in group $G$, "$G'_{hash}$": exponentiation in group $G_T$, $G_{hash}$": inverse computation in group $G_T$, "$m_r$, $m_i$": length of identity in bits string, "$Pr$": pairing operations in the form $x(y)$ as in [23]. "$ET$": equality test, "$\sigma$": not supportive, "$\sqrt{}$": supportive.

Table 2: Running Times with Symbols

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_{ex}$</td>
<td>$G$ exponentiation operation</td>
<td>6.3937</td>
</tr>
<tr>
<td>$G_{exp}$</td>
<td>$G_T$ exponentiation operation</td>
<td>1.9518</td>
</tr>
<tr>
<td>$T_{hash}$</td>
<td>Operation with pairing</td>
<td>11.4173</td>
</tr>
<tr>
<td>$T_{hash}$</td>
<td>Hash functions</td>
<td>0.00853</td>
</tr>
<tr>
<td>$G_{mul}$</td>
<td>Multiplication operation in $G$</td>
<td>0.047</td>
</tr>
<tr>
<td>$G_{exp}$</td>
<td>Multiplication operation in $G_T$</td>
<td>0.0119</td>
</tr>
</tbody>
</table>

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 Kobitz elliptic curve of $y = x^3 + ax^2 + b$ defined on a $F_{2^{60}}$ 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 2 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 scheme as compared to other existing scheme with IND-CCA2 support. However, the inverse computation to recover the message achieves a high 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 extensions of identity based cryptosystem [62, 70], our scheme achieves a remarkable achievement in identity 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


