information

MDPI

Article

A Novel Identity-Based Signcryption Scheme in the Standard Model

Yueying Huang [1,*] and Junjie Yang [2]

[1] Basic Education College of Lingnan Normal University, 524300 Zhanjiang, China
[2] School of Information Engineering, Lingnan Normal University, 524048 Zhanjiang, China; yangjunjie1998@lingnan.edu.cn
* Correspondence: yueyhuang@126.com

Academic Editors: Man Ho Au, Jinguang Han, Joseph K. Liu and Ali El Kaafarani
Received: 2 March 2017; Accepted: 16 May 2017; Published: 19 May 2017

Abstract: Identity-based signcryption is a useful cryptographic primitive that provides both authentication and confidentiality for identity-based crypto systems. It is challenging to build a secure identity-based signcryption scheme that can be proven secure in a standard model. In this paper, we address the issue and propose a novel construction of identity-based signcryption which enjoys IND-CCA security and existential unforgeability without resorting to the random oracle model. Comparisons demonstrate that the new scheme achieves stronger security, better performance efficiency and shorter system parameters.

Keywords: identity-based; signcryption; provable security; standard model

1. Introduction

In [1], Shamir introduced the seminal concept of identity-based (ID-based) cryptography in 1984, which is supposed to provide a possible alternative to conventional public key infrastructure in terms of efficiency and convenience. The interesting feature of this kind of cryptosystem is that a user's public key can be any binary string that can identify the user, such as an email address. Using identities as public keys eliminates the requirement for public-key certificates. The first ID-based signature was proposed in the pioneer paper due to Shamir [1], but ID-based encryption schemes were not founded until Boneh and Franklin [2] invented a practical ID-based encryption from a bilinear pairing in 2001. The ID-based cryptography along with its applications has become a hot research topic in the last decade.

The properties of confidentiality and authentication are essential for computer networks. It seems that they can be easily achieved by consecutively executing a secure encryption scheme and a digital signature scheme. However, this trivial combination is expensive and vulnerable to some subtle attacks [3]. In [4], Zheng introduced the notion of signcryption in 1997, which is a cryptographic primitive that supplies both authentication and confidentiality in a reasonable logic step, at a lower price than that of the traditional signature-then-encryption approach. Many practical and novel signcryption schemes along with their applications have been proposed in the past years (such as [3,5–12]).

An interesting research topic is to combine signcryption and ID-based cryptography [13] to construct secure and efficient ID-based signcryption schemes. In [5], Malone-Lee gave the first ID-based signcryption from bilinear pairings with a corresponding security model, which dealt with privacy and unforgeability. However, Libert and Quisquater [14] showed that Malone-Lee's scheme does not provide semantic security since the signature of the signcrypted message is visible in the final ciphertext. They also built three new ID-based signcryption schemes, but forward security and public verifiability are mutually exclusive in these schemes. Chow et al. [15] constructed an ID-based signcryption that provides both public verifiability and forward security. Boyen [16] also

proposed a novel ID-based signcryption that provides public verifiability, forward security, ciphertext unlinkability and anonymity. Chen and Malone-Lee [17] enhanced the efficiency of Boyen's scheme in 2005. Subsequently, the concept of ID-based signcryption was further extended to cater to more applications. For example, in 2006, Duan and Cao [8] proposed a multi-receiver ID-based signcryption for more than one receiver scenario. In 2008, Li et al. [7] presented an ID-based broadcast signcryption for the application of broadcasting a message to multiple users in a secure and authenticated manner. In 2010, Liu et al. [18] proposed certificateless signcryption as an extension of ID-based signcryption. Unfortunately, Weng et al. [19] showed that Liu et al.'s scheme is neither semantically secure against chosen ciphertext attacks nor existentially unforgeable against chosen message attacks.

The early signcryption schemes only dealt with some informal security analysis. The situation changed since Baek et al. [20] proposed a formal security model for signcrytion and provided a security proof for Zheng's original scheme [4] using the random oracle model due to Bellare and Rogaway [21]. In this model, hash functions are treated as ideal random functions. Although the model is powerful to validate the designs of cryptographic schemes, it has received some criticism since the security in this model does not always lead to the security in the real world [22]. Accordingly, it is interesting to design secure ID-based signcryption schemes in the standard model. In 2009, Yu et al. [23] made the first attempt to construct an ID-based signcryption scheme without random oracles. Observing that Yu et al.'s scheme does not reach the semantic security, Jin et al. [24] proposed an improved scheme and claimed that the improvement is secure without using random oracles. Unfortunately, recent cryptanalysis due to Li et al. [25] shows that Jin et al.'s scheme [24] suffers from the indistinguishability against adaptive chosen ciphertexts attack and existential unforgeability against adaptive chosen messages attack. Zhang et al. [26] also built another new scheme, but Li et al. [27] found that Zhang et al.'s scheme does not have IND-CPA security and they proposed an improvement claiming it to achieve both IND-CCA2 and EUF-CMA security. However, a recent analysis due to Selvi et al. [28] concluded that Li et al.'s scheme reaches neither IND-CCA2 property nor EUF-CMA property. Another new construction was given by Li et al. in ProvSec 2011 [29], but, recently, Selvi et al. [28] showed that the proof of the scheme is not correct.

1.1. Our Contribution

A survey of the previous literature reveals that there does not exist a really secure ID-based signcryption scheme in the standard model. The attempts in ([23,24]) show that a simple combination of Waters' ID-based encryption [30] and Paterson–Schuldt's ID-based signature [31] may not produce a secure ID-based signcryption. Therefore, the main contribution of this paper is to fill this gap by proposing an ID-based signcryption scheme whose security proof does not need to resort to the random oracle model. Our construction makes use of Paterson–Schuldt's ID-based signature [31], Waters' ID-based encryption [30] and the techniques of constructing selective identity-based encryption due to Boneh and Boyen [32]. We also prove its CCA security and existential unforgeability under some well-studied complexity assumptions. Comparisons show that our scheme outperforms the previous ones in terms of security, computational efficiency and the size of system parameters.

1.2. Organization

The rest of this paper is organized in the following way. Some preliminaries used in our scheme are given in Section 2. The new ID-based signcryption along with the performance comparisons to the existing ones are given in Section 3. The security proof of the new scheme is provided in Section 4. Finally, conclusions are given in Section 5.

2. Preliminaries

Some basic knowledge, including bilinear pairings, complexity assumptions and a formal model for ID-based signcryption, is briefly revisited in this section.

2.1. Bilinear Pairings

$\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are multiplicative cyclic groups of prime order p and g is a generator of $\mathbb{G}$. The map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is an admissible bilinear pairing with the following properties [2]:

1. $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for all $a, b \in Z_p$,
2. $\hat{e}(g, g) \neq 1_{\mathbb{G}_T}$,
3. $\hat{e}$ can be efficiently computable.

2.2. Complexity Assumptions

Computational Diffie–Hellman (CDH) Problem [2]: Given $(g, g^a, g^b \in \mathbb{G})$ for some unknown $a, b \in Z_p$, output g^{ab}.

The success probability of a polynomial algorithm $\mathcal{A}$ in solving the CDH problem is denoted as

$$Succ^{CDH}_{\mathcal{A},\mathbb{G}} = \Pr[\mathcal{A}(g, g^a, g^b) = g^{ab} : a, b \in Z_p].$$

CDH Assumption: Given $(g, g^a, g^b \in \mathbb{G})$ for some unknown $a, b \in Z_p$, $Succ^{CDH}_{\mathcal{A},\mathbb{G}}$ is negligible.

Decisional Bilinear Diffie–Hellman (DBDH) Problem: Given $(g, A = g^a, B = g^b, C = g^c \in \mathbb{G})$ for some unknown $a, b, c \in Z_p$ and an element $Z \in \mathbb{G}_T$, determine whether $Z = \hat{e}(g, g)^{abc}$ or not.

The advantage of a distinguisher $\mathcal{B}$ against the DBDH problem is defined as

$$Adv(\mathcal{B}) = \big| \Pr[\mathcal{B}(g^a, g^b, g^c, e(g, g)^{abc}) = 1]$$

$$- \Pr[\mathcal{B}(g^a, g^b, g^c, e(g, g)^z) = 1] \big|.$$

DBDH Assumption: The (t, ϵ)-DBDH assumption [2] says that no t-time adversary has at least an ϵ advantage in solving the DBDH problem.

3. Our ID-Based Signcryption Scheme

In this section, we firstly describe our ID-based signcryption scheme. Then, we show the correctness and comparisons to the existing schemes in the same style.

3.1. The New Scheme

The proposed ID-based signcryption consists of the following algorithms.

Setup: On inputting a security parameter k, the PKG chooses two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order p, a generator g of $\mathbb{G}$ and a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. PKG also picks $u', \delta, v \in \mathbb{G}$, an n-length vector $\vec{u} = (u_i)$ whose elements are randomly from $\mathbb{G}$ and a collision resistant hash function $H : \{0,1\}^* \to Z_p^*$. Additionally, PKG picks a secret $\alpha \in Z_p$, $g_2 \in \mathbb{G}$ and computes $g_1 = g^\alpha$. The public parameters are $params = (\mathbb{G}, \mathbb{G}_T, \hat{e}, g, g_1, g_2, u', \delta, v, \vec{u})$ and the master secret key is $msk = g_2^\alpha$.

Extract: Identities in the new scheme are represented as bitstrings of length n, just as in Waters' scheme [30]. Suppose the sender, say, Alice's identity is ID_A, represented as a bit string $\mathtt{e} = (\mathtt{e}_1, \mathtt{e}_2, \cdots, \mathtt{e}_n)$, and the receiver Bob's identity is $ID_B = \mathtt{f} = (f_1, f_2, \cdots, f_n)$. PKG picks $r_e, r_f \in Z_q^*$ and computes their secret keys as follows:

$$d_{\mathtt{e}} = (d_{\mathtt{e}_1}, d_{\mathtt{e}_2}) = (g_2^\alpha (u' \prod_{i=1}^{n} u_i^{e_i})^{r_e}, g^{r_e}),$$

$$d_{\mathtt{f}} = (d_{\mathtt{f}_1}, d_{\mathtt{f}_2}) = (g_2^\alpha (u' \prod_{i=1}^{n} u_i^{f_i})^{r_f}, g^{r_f}).$$

Signcrypt: To signcrypt a message $M \in \mathbb{G}_T$ to Bob, Alice picks a random value r_m and executes the steps below.

1. Compute $c_2 = \hat{e}(g_1, g_2)^{r_m} M$,
2. Compute $c_3 = g^{r_m}$,
3. Compute $c_4 = (u' \prod_{i=1}^{n} u_i^{f_i})^{r_m}$,
4. Set $c_5 = d_{e_2}$,
5. Compute $h = H(ID_A, ID_B, c_2, c_3, c_4, c_5)$,
6. Compute $c_1 = d_{e_1}(\delta \cdot v^h)^{r_m}$ and output the ciphertext $c = (c_1, c_2, c_3, c_4, c_5)$.

Unsigncrypt: Receiving a signcrypted ciphertext $c = (c_1, c_2, c_3, c_4, c_5)$, Bob checks its validity and decrypts it as follows:

1. Compute $h = H(ID_A, ID_B, c_2, c_3, c_4, c_5)$.
2. Verify if the following equality holds. If it holds, go to the next step. Otherwise, reject the ciphertext:
$$\hat{e}(c_1, g) = \hat{e}(g_1, g_2)\hat{e}(u' \prod_{i=1}^{n} u_i^{e_i}, c_5)\hat{e}(\delta \cdot v^h, c_3).$$
3. Recover the plaintext $c_2 \hat{e}(d_{f_2}, c_4)\hat{e}(d_{f_1}, c_3)^{-1} \rightarrow M$.

3.2. Correctness

The correctness of the proposed scheme can be verified directly by the property of bilinear pairing, after $h = H(ID_A, ID_B, c_2, c_3, c_4, c_5)$ is determined:

$$\begin{aligned} \hat{e}(c_1, g) &= \hat{e}(d_{e_1}(\delta \cdot v^h)^{r_m}, g) \\ &= \hat{e}(g_2^{\alpha}(u' \textstyle\prod_{i=1}^{n} u_i^{e_i})^{r_e}(\delta \cdot v^h)^{r_m}, g) \\ &= \hat{e}(g_2^{\alpha}, g)\hat{e}((u' \textstyle\prod_{i=1}^{n} u_i^{e_i})^{r_e}, g)\hat{e}((\delta \cdot v^h)^{r_m}, g) \\ &= \hat{e}(g_2, g^{\alpha})\hat{e}(u' \textstyle\prod_{i=1}^{n} u_i^{e_i}, g^{r_e})\hat{e}(\delta \cdot v^h, g^{r_m}) \\ &= \hat{e}(g_1, g_2)\hat{e}(u' \textstyle\prod_{i=1}^{n} u_i^{e_i}, c_5)\hat{e}(\delta \cdot v^h, c_3), \end{aligned} \tag{1}$$

and

$$\begin{aligned} & c_2 \hat{e}(d_{f_2}, c_4)\hat{e}(d_{f_1}, c_3)^{-1} \\ = \; & \hat{e}(g_1, g_2)^{r_m} M \hat{e}(g^{r_f}, (u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_m}) \\ & \hat{e}(g_2^{\alpha}(u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_f}, g^{r_m})^{-1} \\ = \; & \hat{e}(g_1, g_2)^{r_m} M \hat{e}(g^{r_f}, (u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_m}) \\ & \hat{e}(g_2^{\alpha}, g^{r_m})^{-1} \\ & \hat{e}((u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_f}, g^{r_m})^{-1} \\ = \; & \hat{e}(g_1, g_2)^{r_m} M \hat{e}(g^{r_f}, (u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_m}) \\ & \hat{e}(g_2, g_1)^{-r_m} \\ & \hat{e}((u' \textstyle\prod_{i=1}^{n} u_i^{f_i})^{r_m}, g^{r_f})^{-1} \\ = \; & M. \end{aligned} \tag{2}$$

3.3. Comparisons

We compare the security and the performance efficiency of our scheme to those of the known ID-based signcryption without random oracles in [23,24,26,27]. M_G, E_G, M_{G_T}, E_{G_T}, I_{G_T}, and $\hat{e}$, denote the multiplication in G, the exponentiation in G, the multiplication in G_T, the exponentiation in G_T, the inversion in G_T and the pairing operation, respectively. The comparisons of the five schemes are summarized in Table 1.

The **Extract** algorithm is omitted in the comparison since these schemes utilize the same secret key extraction. The **Signcrypt** column and the **Unsigncrypt** column specify the computation cost of

generating a signcrypted ciphertext and unsigncrypting a ciphertext in each scheme. The **Size** column shows the length of a ciphertext, represented by elements in $\mathbb{G}$ and $\mathbb{G}_T$. The **Params** column gives the number of group elements in G to be included in system parameters. The **EUF** column and **CCA** column indicate whether the scheme is secure against adaptive chosen message attack and adaptive chosen ciphertext attack. The symbol $\times$ means it is vulnerable to the attack while $\surd$ indicates that it can resist the attack. Note that the scheme in [23,24,26,27] can not be regarded as secure since they suffer either the IND-CCA attack or the IND-CCA attack. The new scheme achieves both IND-CCA security and EUF-CMA security. From this point of view, our scheme outperforms the previous ones in terms of security.

Assume that the output length of the secure hash functions used in the schemes are same, that is, $n_u = n_m = n$. $2n + 5$ group elements are required as public parameters in [23,24,26,27] while only $n + 6$ elements are needed in our scheme. Namely, the length of public parameters of the new scheme is only about one half of that of the schemes in [23,24,26,27]. From this point of view, a shorter public parameter makes the new scheme more suitable for low storage requirement of applications. For the communication cost, the scheme in [26] shares the same size of the resulted signcryption ciphertext and [27], which is comparatively longer than that of our new scheme and the schemes in [23,24]. Although the schemes [23,24] and the new scheme get the same length of a signcrypted ciphertext, our scheme achieves better performance than the schemes in [23,24] because nearly $n/2$ multiplications in G_1 are less required in **Signcrypt** and **Unsigncrypt** algorithms, respectively. Note that the proposed protocol is quite efficient. According to the the benchmark for exponentiations and pairing [33], it costs about 11.07 ms to signcrypt a plantext and 33.31 ms to unsigncrypt a ciphertext in our protocol.

Table 1. Security and performance comparisons.

Schemes	Signcrypt	Unsigncrypt	Size	Params	EUF	CCA
Yu2009 [23]	$1\hat{e} + 2E_G + 2E_{G_T} +$ $(3 + (n_u + n_m)/2)M_G$	$6\hat{e} + 2M_{G_T} + 1I_{G_T} +$ $(1 + (n_u + n_m)/2)M_G$	$4\|G\| + 1\|G_T\|$	$(2n+5)G$	$\surd$	$\times$
Jin2010 [24]	$1\hat{e} + 2E_G + 2E_{G_T} + 1\phi +$ $(3 + (n_u + n_m)/2)M_G$	$6\hat{e} + 2M_{G_T} + 1I_{G_T} + 1\phi^{-1} +$ $(1 + (n_u + n_m)/2)M_G$	$4\|G\| + 1\|G_T\|$	$(2n+5)G$	$\times$	$\times$
Zhang2010 [26]	$1\hat{e} + 3E_G + 1E_{G_T} +$ $(4 + (n_u + n_m)/2)M_G$	$6\hat{e} + 3M_{G_T} + 1I_{G_T} +$ $(6 + (n_u + n_m)/2)M_G$	$4\|G\| + 1\|G_T\| + 1\|Z_p\|$	$(2n+5)G$	$\times$	$\times$
Li2012 [27]	$1\hat{e} + 6E_G + 1E_{G_T} + 1\phi +$ $(n_u + (n_m)/2 + 4)M_G$	$6\hat{e} + 2M_{G_T} + 1I_{G_T} +$ $(3 + (n_u + n_m)/2)M_G$	$4\|G\| + 1\|G_T\| + 1\|Z_p\|$	$(2n+5)G$	$\times$	$\times$
Ours	$1\hat{e} + 4E_G + 1E_{G_T} +$ $1M_{G_T} + (3 + n/2)M_G$	$6\hat{e} + 2M_{G_T} + 1I_{G_T} +$ $1E_G + (2 + n/2)M_G$	$4\|G\| + 1\|G_T\|$	$(n+6)G$	$\surd$	$\surd$

4. Security of the New Scheme

In this section, we prove that the new scheme achieves the properties of IND-CCA and EUF-CMA in the standard model.

Theorem 1. *Assume that there exists an adversary $\mathcal{A}$ that can distinguish two valid signcrypted ciphertexts with an advantage ϵ when running in time t and asking at most q_e private key extraction queries, q_s signcryption queries and q_u unsigncryption queries. Then, there exists a distinguisher $\mathcal{C}$ that can solve an instance of the DBDH problem in time $t + O((q_e + q_s + q_u)n_u t_{mul} + (q_e + q_s)t_{exp} + q_u t_{pair})$ with an advantage*

$$Adv(\mathcal{C}) > \frac{1}{8(q_e + q_s + q_u)(n+1)},$$

where t_{mul}, t_{exp} and t_{pair} denote the time for a multiplication, an exponentiation in $\mathbb{G}$ and a pairing computation, respectively.

Proof. The distinguisher $\mathcal{C}$ is given a random DBDH problem instance $(g, g^{\alpha}, g^{\beta}, g^{\gamma}, Z \in G_T)$, and he tries to tell whether $Z = e(g,g)^{\alpha\beta\gamma}$ or not. $\mathcal{C}$ will act as $\mathcal{A}$'s challenger and run $\mathcal{A}$ as a subroutine in the IND-CCA game. The following proof is inspired by the techniques due to [30–32]. □

Setup: $\mathcal{C}$ sets $l = 4q_e$, picks the values below randomly and keeps them secret:

1. an integer $0 < k < n$,
2. an integer $x' \in Z_l$, and an n-length vector $\vec{x} = (x_i)$ where $x_i \in Z_l$,
3. an integer $y' \in Z_p$, and an n-length vector $\vec{y} = (y_i)$ where $y_i \in Z_p$,
4. three integers $t, a, c \in Z_p$.

Additionally, $\mathcal{C}$ chooses a collision resistent hash function $H : \{0,1\}^* \rightarrow Z_p$. For ease of description, we define the following functions as in [30] for an identity $\mathsf{e} = (e_1, \cdots, e_n)$:

1. $F(\mathsf{e}) = (p - lk) + x' + \sum_{i=1}^{n} e_i x_i$,
2. $J(\mathsf{e}) = y' + \sum_{i=1}^{n} e_i y_i$,
3. $K(\mathsf{e}) = \begin{cases} 0, & \text{if } x' + \sum_{i=1}^{n} x_i = 0 \pmod{l}, \\ 1, & \text{otherwise.} \end{cases}$

Then, $\mathcal{C}$ sets public parameters as follows:

1. Set $g_1 = g^{\alpha}, g_2 = g^{\beta}$ where g^{α}, g^{β} are from the input of the DBDH problem instance.
2. Assign $u' = g_2^{p-kl+x'} g^{y'}$ and $u_i = g_2^{x_i} g^{y_i}$ and set $\vec{u} = (u_1, u_2, \ldots, u_n)$.
3. Set $\delta = g^a$ and $v = g^c$.

Note that from the viewpoint of the adversary $\mathcal{A}$, the public parameters assigned above share the same distribution with the real construction. Additionally, for any identity e, we have $u' \prod_{i=1}^{n} u_i^{e_i} = g_2^{F(\mathsf{e})} g^{J(e)}$.

Extract queries: Adversary $\mathcal{A}$ can issue at most q_e private key extraction queries. For a private key query for an identity e, the challenger $\mathcal{C}$ first checks if $F(\mathsf{e}) = 0$ and aborts with a random guess b' of the challenger's value b in this situation. Otherwise, it picks a random $r_e \in Z_p$ and responds $\mathcal{A}$ for the pair

$$d_e = (d_{e1}, d_{e2}) = (g_1^{\frac{-J(\mathsf{e})}{F(\mathsf{e})}} (u' \prod_{i=1}^{n_u} u_i^{e_i})^{r_e}, g_1^{\frac{-1}{F(\mathsf{e})}} g^{r_\mathsf{e}}).$$

Let $\hat{r}_e = r_e - \frac{\alpha}{F(\mathsf{e})}$, as shown by Waters [30], and the simulation is perfect since

$$\begin{aligned} d_{\mathsf{e}1} &= g_1^{\frac{-J(\mathsf{e})}{F(\mathsf{e})}} (g_2^{F(\mathsf{e})} g^{J(\mathsf{e})})^{r_e} \\ &= g_2^{\alpha} (g_2^{F(\mathsf{e})} g^{J(\mathsf{e})})^{\frac{-\alpha}{F(\mathsf{e})}} (g_2^{F(\mathsf{e})} g^{J(\mathsf{e})})^{r_e} \\ &= g_2^{\alpha} (g_2^{F(\mathsf{e})} g^{J(\mathsf{e})})^{r_e - \frac{\alpha}{F(\mathsf{e})}} \\ &= g_2^{\alpha} (g_2^{F(\mathsf{e})} g^{J(\mathsf{e})})^{\hat{r}_e} \end{aligned}$$

and

$$d_{\mathsf{e}2} = g_1^{\frac{-1}{F(\mathsf{e})}} g^{r_\mathsf{e}} = g^{r_\mathsf{e} - \frac{\alpha}{F(\mathsf{e})}} = g^{\hat{r}_e}.$$

$\mathcal{C}$ can generate a valid private key for e if and only if $F(\mathsf{e}) \neq 0 \pmod{l}$, for which it suffices to have $F(\mathsf{e}) \neq 0 \pmod{p}$ [30].

Signcryption queries: Adversary $\mathcal{A}$ can issue at most q_s signcryption queries on messages M under a sender's identity $\mathsf{e} = (e_1, \cdots, e_n)$ and a receiver's identity $\mathsf{f} = (f_1, \cdots, f_n)$. If $F(\mathsf{e}) \neq 0 \pmod{l}$,

$\mathcal{C}$ first generates a private key for e just as he did in the Extract query described above, and then runs the Signcrypt$(M, d_{\mathsf{e}}, \mathsf{f})$ algorithm, creates a valid ciphertext and forwards it to answer $\mathcal{A}$'s query. If $F(\mathsf{e}) = 0 \pmod{l}$, $\mathcal{C}$ will simply abort.

Unsigncryption queries: Adversary $\mathcal{A}$ can issue at most q_u unsigncryption queries on ciphertexts $c = (c_1, \cdots, c_5)$ for identities e and f. $\mathcal{C}$ performs the following steps.

1. Compute $h = H(\mathsf{e}, \mathsf{f}, c_2, c_3, c_4, c_5)$.
2. Check if the following equality holds. If it holds, go to next step. Otherwise, reject the ciphertext:

$$\hat{e}(c_1, g) = \hat{e}(g_1, g_2)\hat{e}(u' \prod_{i=1}^{n} u_i^{e_i}, c_5)\hat{e}(\delta \cdot v^h, c_3).$$

3. Check if $F(\mathsf{f}) \neq 0 \pmod{l}$ holds. If it holds, $\mathcal{C}$ firstly generates a private key (d_{f_1}, d_{f_2}) for the receiver f, and then computes the plaintext $c_2\hat{e}(d_{f_2}, c_4)\hat{e}(d_{f_1}, c_3)^{-1} \rightarrow M$ and forwards it to $\mathcal{A}$. Otherwise, the simulation aborts.

Challenge: After a polynomially bounded number of queries, $\mathcal{A}$ outputs two equal-length plaintexts $M_0, M_1 \in \mathbb{G}_T$ together with a pair of identities $\mathsf{e}^*, \mathsf{f}^*$ on which he wishes to be challenged. $\mathcal{C}$ fails the simulation if $\mathcal{A}$ has queried a key extraction query on f^* during the first stage and $\mathcal{C}$ will abort if $F(\mathsf{f}^*) \neq 0 \pmod{l}$. Otherwise, $\mathcal{C}$ picks a random bit b and constructs the challenging ciphertext on M_b using the input of the DBDH problem (g, A, B, C, Z) as follows:

1. Pick a random number $r_e^* \in Z_p$,
2. Compute $c_2^* = ZM_b$,
3. Set $c_3^* = C$,
4. Compute $c_4^* = C^{J(f^*)}$,
5. Compute $c_5^* = g_1^{\frac{-1}{F(e^*)}} g^{r_e^*}$,
6. Compute $h^* = H(\mathsf{e}^*, \mathsf{f}^*, c_2^*, c_3^*, c_4^*, c_5^*) \in Z_p$,
7. Compute $c_1^* = g_1^{\frac{-J(\mathsf{e}^*)}{F(\mathsf{e}^*)}} (g_2^{F(\mathsf{e}^*)} g^{J(\mathsf{e}^*)})^{r_e^*} C^{a+ch^*}$,
8. Output the challenge ciphertext $c^* = (c_1^*, c_2^*, c_3^*, c_4^*, c_5^*)$.

Suppose that the simulator was given a valid BDH tuple, which is $Z = \hat{e}(g, g)^{\alpha\beta\gamma}$, and we can see that c^* is a valid signcryption ciphertext on M_b. Otherwise, if Z is a random element of $\mathbb{G}$, the challenging ciphertext gives no information about the simulator's choice of b.

Adversary $\mathcal{A}$ then issues a second series of queries adaptively that are treated in the same way as in the first stage. The restriction in this phase is that $\mathcal{A}$ is forbidden to make a key extraction query on identity f^* and make an unsigncryption query on the challenging ciphertext c^* to get the corresponding plaintext. At the end of the game, $\mathcal{A}$ outputs a guess b' of b. If $b' = b$, $\mathcal{C}$ answers 1 indicating that $Z = \hat{e}(g, g)^{\alpha\beta\gamma}$. Otherwise, $\mathcal{C}$ answers 0 to denote that $Z \neq \hat{e}(g, g)^{\alpha\beta\gamma}$. We now analyze $\mathcal{C}$'s probability of success. The simulation can be completed without aborting on the condition that all extraction queries on identities e satisfy $F(\mathsf{e}) \neq 0 \pmod{l}$, all signcryption queries $(\mathsf{e}, \mathsf{f}, M)$ satisfy $F(\mathsf{e}) \neq 0 \pmod{l}$, all unsigncryption satisfy $(c, \mathsf{e}, and \mathsf{f})$ satisfy$F(\mathsf{f}) \neq 0 \pmod{l}$. In addition, in the DBDH problem solving phase, $F(\mathsf{e}^*) \neq 0 \pmod{l}$ and $F(\mathsf{f}^*) = 0 \pmod{l}$. Assume the identities queried in either extract queries or in signcryption queries and unsigncryption queries, not including the challenging identity, are $\mathsf{e}_1, \mathsf{e}_2, \cdots, \mathsf{e}_{q_I}$. Obviously, we have $q_I < q_e + q_s$. The events A_i and A^* are defined as follows:

$$A_i : F(\mathsf{e}_i) \neq 0 \pmod{l}, \quad A^* : F(\mathsf{f}^*) = 0 \pmod{l}.$$

The probability that $\mathcal{C}$ does not abort is

$$Pr[\neg abort] > Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*].$$

This probability can be assessed by utilizing Waters' technique [30]. The computation is not repeated here since it is similar to Waters' process and the final lower bound is

$$Pr[\neg abort] \quad > \quad \frac{1}{8(q_e+q_s+q_u)(n+1)}.$$

The bound of $\mathcal{C}$'s computation time comes from the fact that $O(n_u)$ multiplications and $O(1)$ exponentiations are required in each extract query, $O(n_u)$ multiplications and $O(1)$ exponentiations are needed in each signcryption query, and $O(n_u)$ multiplications and $O(1)$ pairings are required in each unsigncryption query.

Theorem 2. *Assume that there exists an adversary $\mathcal{F}$ that can $(t, q_e, q_s, q_u, \epsilon)$ forge a valid signcryption ciphertext on a message M. Then, we can construct a new algorithm $\mathcal{C}$ to solve the CDH problem.*

Proof. This proof also proceeds by the reduction approach. Assuming a forger $\mathcal{F}$ for our scheme exists, we will construct a challenger $\mathcal{C}$, who runs $\mathcal{F}$ as a subroutine, to solve an instance of the CDH problem, which contradicts the CDH assumption. Specifically, given a group G, a generator g and two elements $g^{\alpha}, g^{\beta} \in G$, $\mathcal{C}$'s goal is to output $g^{\alpha\beta}$. Firstly, $\mathcal{C}$ sets the public parameters of the proof in the same way as he did in the proof 1. Note that $\mathcal{C}$ assigns $g_1 = g^{\alpha}$, $g_2 = g^{\beta}$, $\delta = g^{a}$ and $v = g^{c}$, and for an identity $\mathsf{e} = (e_1, \cdots, e_n)$, we have $u' \prod_{i=1}^{n} u_i^{e_i} = g_2^{F(\mathsf{e})} g^{J(e)}$. □

Then, $\mathcal{A}$ will issue a polynomial number of queries including extraction queries, signcryption queries and unsigncryption queries. C responds to $\mathcal{A}$'s query in the same way as he does in Theorem 1. Finally, if $\mathcal{C}$ does not abort during the simulation, $\mathcal{A}$ will output a valid forgery ciphertext $c^* = (c_1^*, c_2^*, c_3^*, c_4^*, c_5^*)$ on message M^* under a sender e^* and a receiver f^*. If $F(\mathsf{e}^*) \neq 0$, $\mathcal{C}$ will abort. Otherwise, $\mathcal{C}$ computes $h^* = H(\mathsf{e}^*, \mathsf{f}^*, c_2^*, c_3^*, c_4^*, c_5^*)$ and because the forgery is valid, then

$$\begin{aligned} \hat{e}(c_1^*, g) &= \hat{e}(g_1, g_2)\hat{e}(u' \textstyle\prod_{i=1}^{n} u_i^{e_i}, c_5^*)\hat{e}(\delta \cdot v^{h^*}, c_3^*) \\ &= \hat{e}(g^{\alpha}, g^{\beta})\hat{e}(g_2^{F(\mathsf{e}^*)} g^{J(\mathsf{e}^*)}, c_5^*)\hat{e}(g^{a} \cdot (g^{c})^{h^*}, c_3^*) \\ &= \hat{e}(g, g^{\alpha\beta})\hat{e}(g, (c_5^*)^{J(\mathsf{e}^*)})\hat{e}(g, (c_3^*)^{a+ch^*}). \end{aligned} \tag{3}$$

Accordingly, $\mathcal{C}$ can output $\frac{c_1^*}{(c_5^*)^{J(\mathsf{e}^*)} \cdot (c_3^*)^{a+ch^*}} \rightarrow g^{\alpha\beta}$ as the solution to the instance of the given CDH problem.

5. Conclusions

In this paper, we put forth a novel identity-based signcryption scheme secure in the standard model since the existing schemes were showed to be insecure. The new construction makes use of the tricks of Boneh–Boyen selective identity-based encryption, Waters' identity-based encryption, and Paterson–Schuldt's identity-based signature. The proposed scheme outperforms the previous ones in terms of stronger security, higher performance efficiency and shorter system parameters. We also show that the new scheme achieves the CCA security under the decisional bilinear Diffie–Hellman assumption and the existential unforgeability against adaptive chosen messages attacks under the computational Diffie–Hellman assumption.

Author Contributions: Yueying Huang designed the protocol and proved the security of the protocol; Junjie Yang conducted the security and efficiency comparisons. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin, Germany, 1985; pp. 47–53.

2. Boneh, D.; Franklin, M. *Identity-Based Encryption from the Weil Pairing*; Springer: Berlin, Germany, 2001; pp. 213–229.
3. An, J.; Dodis, Y.; Rabin, T. On the security of joint signature and encryption. In *Advances in Cryptology—EUROCRYPT 2002*; Knudsen, L., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2332, pp. 83–107.
4. Zheng, Y. Digital signcryption or how to achieve cost(signature & encryption) < cost(signature) + cost(encryption). In Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO 97, Santa Barbara, CA, USA, 17–21 August 1997; pp. 165–179.
5. Malone-Lee, J. Identity Based Signcryption. Cryptology ePrint Archive. 2002. Available online: http://eprint.iacr.org/2002/098 (accessed on 17 May 2017).
6. Huang, Q.; Wong, D.S.; Yang, G. Heterogeneous signcryption with key privacy. *Comput. J.* **2011**, *54*, 525–536.
7. Li, F.; Xin, X.; Hu, Y. Indentity-based broadcast signcryption. *Comput. Stand. Interfaces* **2008**, *30*, 89–94.
8. Duan, S.; Cao, Z. Efficient and provably secure multireceiver identity-based signcryption. In Proceedings of the 11th Australasian conference on Information Security and Privacy, ACISP 06, Melbourne, Australia, 3–5 July 2006; pp. 195–206.
9. Wei, G.Y.; Shao, J.; Xiang, Y.; Zhu, P.; Lu, R. Obtain confidentiality or authenticity in Big Data by ID-based generalized signcryption. *Inf. Sci.* **2015**, *318*, 111–122.
10. Li, X.; Qian, H.; Weng, J.; Yu, Y. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model. *Math. Comput. Model.* **2013**, *57*, 503–511.
11. Li, F.; Han, Y.; Jin, C. Certificateless online/offline signcryption for the Internet of Things. *Wirel. Netw.* **2017**, *23*, 145–158.
12. Li, F.; Han, Y.; Jin, C. Practical signcryption for secure communication of wireless sensor networks. *Wirel. Pers. Commun.* **2016**, *89*, 1391–1412.
13. Choo, K.K.R.; Nam, J.; Won, D. A mechanical approach to derive identity-based protocols from Diffie–Hellman-based protocols. *Inf. Sci.* **2014**, *281*, 182–200.
14. Libert, B.; Quisquater, J.J. A new identity based signcryption scheme from pairings. In Proceedings of the IEEE Information Theory Workshop, Paris, France, 31 March–4 April 2003; pp. 155–158.
15. Chow, S.; Yiu, S.; Hui, L.; Chow, K. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In *Information Security and Cryptology—ICISC 2003*; Lim, J.I., Lee, D.H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2971, pp. 352–369.
16. Boyen, X. Multipurpose identity-based signcryption—A swiss army knife for identity-based cryptography. In *CRYPTO 2003*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 383–399.
17. Chen, L.; Malone-Lee, J. Improved identity-based signcryption. In *Public Key Cryptography—PKC 2005*; Vaudenay, S., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3386, pp. 362–379.
18. Liu, Z.; Hu, Y.; Zhang, X.; Ma, H. Certificateless signcryption scheme in the standard model. *Inf. Sci.* **2010**, *180*, 452–464.
19. Weng, J.; Yao, G.; Deng, R.H.; Chen, M.R.; Li, X. Cryptanalysis of a certificateless signcryption scheme in the standard model. *Inf. Sci.* **2011**, *181*, 661–667.
20. Baek, J.; Steinfeld, R.; Zheng, Y. Formal proofs for the security of signcryption. *J. Cryptol.* **2007**, *20*, 203–235.
21. Bellare, M.; Rogaway, P. The exact security of digital signatures-how to sign with RSA and Rabin. In Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT 96, Saragossa, Spain, 12–16 May 1996; pp. 399–416.
22. Canetti, R.; Goldreich, O.; Halevi, S. The random oracle methodology, revisited. *J. ACM* **2004**, *51*, 557–594.
23. Yu, Y.; Yang, B.; Sun, Y.; Zhu, S.L. Identity based signcryption scheme without random oracles. *Comput. Stand. Interfaces* **2009**, *31*, 56–62.
24. Jin, Z.; Wen, Q.; Du, H. An improved semanticallysecure identity-based signcryption scheme in the standard model. *Comput. Electr. Eng.* **2010**, *36*, 545–552.
25. Li, F.; Liao, Y.; Qin, Z. Analysis of an identity-based signcryption scheme in the standard model. *IEICE Trans.* **2011**, *94*, 268–269.
26. Zhang, B. Cryptanalysis of an identity based signcryption scheme without random oracles. *Comput. Inf. Syst.* **2010**, *6*, 1923–1931.

27. Li, F. Further improvement of an identity-based signcryption scheme in the standard model. *Comput. Electr. Eng.* **2012**, *38*, 413–421.
28. Selvi, S.S.D.; Vivek, S.S.; Vinayagamurthy, D.; Rangan, C.P. On the Security of ID Based Signcryption Schemes. Ology ePrint Archive, Report 2011/664. Available online: http://eprint.iacr.org/ (accessed on 17 May 2017).
29. Li, F.; Muhaya, F.B.; Zhang, M.; Takagi, T. Efficient identity-based signcryption in the standard model. In Proceedings of the 5th International Conference on Provable Security, ProvSec 11, Xi'an, China, 16–18 October 2011; pp. 120–137.
30. Waters, B. Efficient identity-based encryption without random oracles. In *Advances in Cryptology—Eurocrypt 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 114–127.
31. Paterson, K.; Schuldt, J. Efficient identity-based signatures secure in the standard model. In *Information Security and Privacy;* Batten, L., Safavi-Naini, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4058, pp. 207–222.
32. Boneh, D.; Boyen, X. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology—EUROCRYPT 2004*; Cachin, C., Camenisch, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3027, pp. 223–238.
33. Guillevic, A. Comparing the Pairing Efficiency over Composite-Order and Prime-Order Elliptic Curves. In *Applied Cryptography and Network Security*; Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7954, pp. 357-372.