Identity Based Online/Offline Signcryption Scheme

S. Sharmila Deva Selvi, S. Sree Vivek*, C. Pandu Rangan*

Theoretical Computer Science Lab,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras, India.
{sharmila,svivek,prangan}@cse.iitm.ac.in

Abstract. Online/Offline signcryption is a cryptographic primitive where the signcryption process is divided into two phases - online and offline phase. Most of the computations are carried out offline (where the message and the receiver identity are unavailable). The online phase does not require any heavy computations like pairing, multiplication on elliptic curves and is very efficient. To the best of our knowledge there exists three online/offline signcryption schemes in the literature : we propose various attacks on all the existing schemes. Then, we give the first efficient and provably secure identity based online/offline signcryption scheme. We formally prove the security of the new scheme in the random oracle model [2]. The main advantage of the new scheme is, it does not require the knowledge of message or receiver during the offline phase. This property is very useful since it is not required to pre-compute offline signcryption for different receivers based on the anticipated receivers during the offline phase. Hence, any value generated during the offline phase can be used during the online phase to signcrypt the message to a receiver during the online phase. This helps in reducing the number of values stored during the offline phase. To the best of our knowledge, the scheme in this paper is the first provably secure scheme with this property.

Keywords: Online Offline Signcryption, Identity Based Cryptography, Confidentiality, Unforgeability, Random Oracle Model.

1 Introduction

Confidentiality and authenticity are two fundamental properties offered by public key cryptography which are achieved through encryption schemes and digital signatures respectively. In scenarios where both these properties are needed, a Sign-then-Encrypt approach was used earlier. In 1997, Zheng [15] introduced the concept of signcryption where both these properties are achieved in a single logical step, but in a more efficient way. The notion of identity based cryptography was introduced by Shamir [10] in 1984. It is a form of public key cryptography in which the users do not obtain certificates for their public keys. Instead, public keys are generated using arbitrary identifiers such as email addresses, telephone numbers and social security numbers that uniquely identifies a user in the system. This greatly reduces the problem of certificate management, considered to be cumbersome in PKI based systems. The private keys corresponding to the public keys are generated by a trusted authority called Private Key Generator (PKG). The first fully practical identity based encryption scheme was proposed by Boneh and Franklin [3] in 2001. Malone-Lee [7] proposed the first identity based signcryption scheme.

Even et al. in [5] introduced the concept of online/offline signatures. In this notion, the signing process can be divided into two phases, namely offline and online phases. The offline phase includes all the computations that can be done before the message to be signed is received. To ensure that both online signing and verification are efficient, most of the computational overhead is shifted to offline part. Once the message is available, the signature can be generated easily with the pre-computations done in offline phase. Due to this property, online /offline signatures are useful in applications where the signer must respond quickly once the message to be signed is presented, particularly for low power devices such as smart cards. Even et al. [5], proposed a generic construct which can be used to convert any signature scheme into an online/offline one.

* Work supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation sponsored by Department of Information Technology, Government of India

Their construction is inefficient as it increases the size of each signature by a quadratic factor. Shamir and Tauman [11] proposed an improved version which makes use of a new paradigm called "hash-sign-switch" to design more efficient online/offline signature schemes.

The notion of online/offline signcryption was first discussed in An et al. [1]. In their paper, they did not give any concrete method, but they have given general security proof notions for signcryption schemes. Zhang et al. [14] extended the work of An et al. [1] and provided a concrete scheme making use of short signatures. However, Zhang's scheme [14] is PKI based scheme and the focus of our paper is on identity based signcryption schemes. Sun et al. [12] were the first to propose an identity based online/offline signcryption scheme. In their paper, they formally defined the identity based online/offline signcryption and its security models and proposed a new scheme. The offline phase can be computed before the message is available and the online phase is done once the message is presented. After this, Sun et al. proposed another generic scheme in [13].

Motivation: The identity based cryptography finds application in systems like Ad-hoc Networks, Sensor Networks, Smart cards etc. However, entities in these systems have less powerful devices which limits their abilities to perform public key operations like encryption and signing. The computations aimed at use, in these devices should be very efficient to be made practical. In this scenario, identity based online/offline signcryption plays a vital role as it comprises the advantages of identity based cryptography and online/offline computation of the signcryption process.

1. Online/offline nature of the primitive allows expensive computation to be carried out in the offline phase.
2. Signcryption achieves confidentiality and authentication in a single logical step to obtain more efficiency.

All these desirable properties can be achieved using identity based online/offline signcryption which makes it suitable for less powerful devices as in many applications the signer has a very limited response time once the message is presented.

Our Contribution: To the best of our knowledge there are three online/offline signcryption schemes in the literature : two schemes by sun et al. [13], [12] and one scheme by Liu et al. [6]. In this paper, we point out some weaknesses in the generic scheme by Sun et al. [13] and forgeability attack on the specific scheme by Sun et al [12]. We show an attack against sender anonymity of the scheme proposed by Liu et al. [6], we also point out the weakness in the security proof of [6]. Then, we present an efficient online/offline identity based signcryption scheme. The online phase only includes modular addition operations and an XOR operation. The striking feature of our scheme is that the sender does not require the knowledge of receiver identity as well as the message in the offline phase. In the existing identity based online/offline signcryption schemes, the offline phase can be performed only if the receiver is known. In practical scenarios, the devices should anticipate the probable receivers and compute the offline phase accordingly. If the message is to be signcrypted for a new receiver, then the offline phase has to be recomputed where the very idea of offline phase itself becomes irrelevant. Our scheme can avoid this overhead as the output of the offline phase can be used irrespective of the receiver and the message. The security of the scheme is proved under random oracle model. Thus our scheme becomes the only existing efficient and provably secure identity based online/offline signcryption scheme in the literature.

2 Preliminaries

2.1 Bilinear Pairing

Let $\mathbb{G}_1$ be an additive cyclic group generated by P, with prime order q, and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order q. Let $\hat{e}$ be a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

2.2 Computational Assumptions

In this section, we recall the computational assumptions related to bilinear maps[4] that are relevant to the security of our scheme.

The q-Computation Diffie-Hellman Inverse problem (q-CDHIP): Given an additive group $\mathbb{G}_1$ and a multiplicative group $\mathbb{G}_2$, all with prime order p and $(q+1)$ tuples $(G, sG, s^2G, \ldots, s^qG)$, computing $(1/s)P$ is the q-Computation Diffie-Hellman Inverse problem.

The q-Bilinear Diffie-Hellman Inversion problem (q-BDHIP): Given an additive group $\mathbb{G}_1$ and a multiplicative group $\mathbb{G}_2$, all with prime order p and $(q+1)$ tuples $(G, sG, s^2G, \ldots, s^qG)$, computing $\hat{e}(G,G)^{1/s} \in \mathbb{G}_2$ is the q-Bilinear Diffie-Hellman Inversion problem.

3 Identity Based Online/Offline Signcryption

3.1 Framework of Identity Based Online/Offline Signcryption

Identity based online/offline signcryption scheme consists of the following algorithms.

Setup(κ) **:** Given a security parameter κ, the Private Key Generator (PKG) generates the systems public parameters *params* and the corresponding master private key *msk* that is kept secret by PKG.

Key Extract(ID_i) **:** Given a user identity ID_i by user U_i, the PKG computes the corresponding private key D_i and sends D_i to U_i via. a secure channel.

OffSigncrypt$(ID_{\mathbb{S}}, D_{\mathbb{S}})$ **:** Given the sender identity $ID_{\mathbb{S}}$ and the private key $D_{\mathbb{S}}$ of $ID_{\mathbb{S}}$, this algorithm outputs an offline signcryption σ'. This is executed by the sender with identity $ID_{\mathbb{S}}$.

OnSigncrypt$(m, ID_{\mathbb{S}}, ID_{\mathbb{R}}, \sigma')$ **:** This algorithm takes as input a message $m \in \mathcal{M}$, the sender identity $ID_{\mathbb{S}}$, the receiver identity $\mathrm{ID}_{\mathbb{R}}$ and the offline signcryption σ' by $ID_{\mathbb{S}}$ as input and outputs the signcryption σ. This algorithm is executed by the sender with identity $ID_{\mathbb{S}}$.

Unsigncrypt$(\sigma, ID_{\mathbb{S}}, ID_{\mathbb{R}}, D_{\mathbb{R}})$ **:** This algorithm takes as input the signcryption σ, sender's identity $\mathrm{ID}_{\mathbb{S}}$, the receiver identity $ID_{\mathbb{R}}$ and the receiver's private key $D_{\mathbb{R}}$ as input and produces the plaintext m, if σ is a valid signcryption of m from the sender $\mathrm{ID}_{\mathbb{S}}$ to $ID_{\mathbb{R}}$ or "Invalid" otherwise.

3.2 Security Model for ID-Based Online Offline Signcryption

Definition 1. *(Confidentiality) An identity based online/offline signcryption (IBOOSC) is indistinguishable against adaptive chosen ciphertext attacks (IND-IBOOSC-CCA2) if there exists no polynomially bounded adversary having non-negligible advantage in the following game:*

1. ***Setup Phase*** : The challenger $\mathcal{C}$ runs the **Setup** algorithm with the security parameter κ as input and sends the system parameters **params** to the adversary $\mathcal{A}$ and keeps the master private key **msk** secret.
2. ***Phase-I*** : $\mathcal{A}$ performs polynomially bounded number of queries to the oracles provided to $\mathcal{A}$ by $\mathcal{C}$. The description of the queries in the first phase are listed below:
   - ***Key Extract query*** **:** $\mathcal{A}$ produces an identity ID_i and receives the private key D_i corresponding to ID_i.
   - ***Signcryption query*** **:** $\mathcal{A}$ produces a message m, the sender identity $ID_{\mathbb{S}}$, and the receiver identity $ID_{\mathbb{R}}$ to the challenger $\mathcal{C}$. $\mathcal{C}$ computes $ID_{\mathbb{S}}$'s private key $D_{\mathbb{S}}$ and runs the algorithm **OffSigncrypt**$(ID_{\mathbb{S}}, D_{\mathbb{S}})$ to obtain an offline signcryption σ'. Finally $\mathcal{C}$ returns $\sigma =$ **OnSigncrypt**$(m, ID_{\mathbb{R}}, \sigma')$ to $\mathcal{A}$.
   - ***Unsigncryption query*:** $\mathcal{A}$ produces the signcryption σ, the sender identity $ID_{\mathbb{S}}$, and the receiver identity $ID_{\mathbb{R}}$ to $\mathcal{C}$. $\mathcal{C}$ generates the private key $D_{\mathbb{R}}$ by querying the **Key Extraction oracle**. $\mathcal{C}$ unsigncrypts σ using $D_{\mathbb{R}}$ and returns m if σ is a valid signcryption from $ID_{\mathbb{S}}$ to $ID_{\mathbb{R}}$, else outputs "Invalid".

   $\mathcal{A}$ can present its queries adaptively, i.e. every request may depend on the response to the previous queries.
3. ***Challenge*** : $\mathcal{A}$ chooses two plaintexts $\{m_0, m_1\} \in \mathcal{M}$ of equal length and ID_A and ID_B as the sender and receiver identities on which $\mathcal{A}$ wishes to be challenged. The restriction is that $\mathcal{A}$ should not have queried the private key corresponding to ID_B in Phase-I. $\mathcal{C}$ now chooses a bit $\bar{\delta} \in_R \{0,1\}$ and computes the challenge signcryption σ^* of $\mathrm{m}_{\bar{\delta}}$ and sends σ^* to $\mathcal{A}$.
4. ***Phase-II*** : $\mathcal{A}$ performs polynomially bounded number of requests just like the Phase-I, with the restrictions that $\mathcal{A}$ cannot make **Key Extraction query** on ID_B and should not query for unsigncryption query on C^*.

5. ***Guess*** : Finally, $\mathcal{A}$ produces a bit $\bar{\delta}'$ and wins the game if $\bar{\delta}' = \bar{\delta}$. The success probability is defined by:

$$\text{Succ}_{\mathcal{A}}{}^{IND-IBOOSC-CCA2}(\kappa) = \frac{1}{2} + \epsilon$$

Here, ϵ is called the advantage for the adversary in the above game.

Definition 2. *(Unforgeability) An identity based online/offline signcryption scheme (IBOOSC) is said to be existentially unforgeable against adaptive chosen messages attacks (EUF-IBOOSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game:*

1. ***Setup Phase*** : The challenger runs the **Setup** algorithm with a security parameter κ and gives the system parameters **params** to the adversary $\mathcal{A}$ and keeps **msk** secret.
2. ***Training Phase*** : $\mathcal{A}$ performs polynomially bounded number of queries as described in Phase-I of **Definition 2**. The queries may be adaptive, i.e. the current query may depend on the previous query responses.
3. ***Existential Forgery*** : Finally, $\mathcal{A}$ produces a new triple $(ID_{\mathbb{A}},\ ID_{\mathbb{B}},\ C^*)$ (i.e. a triple that was not produced by the signcryption oracle), where the private key of $ID_{\mathbb{A}}$ was not queried in the **training phase**. $\mathcal{A}$ wins the game if the result of the unsigncryption of $(ID_{\mathbb{A}},\ ID_{\mathbb{B}},\ C^*)$ is $\neq$ "Invalid", in other words C^* is a valid signcrypt of some message $m \in \mathcal{M}$.

4 Review and Attack of Identity Based Online/Offline Signcryption by Sun et al.[12]

In this section, we recall the identity based online/offline scheme by Sun et al.[12] and demonstrate that the scheme is not secure under existential unforgeability attack.

4.1 Overview of the Scheme

Their scheme consists of five algorithms - $Setup$, $Extract$, $OffSign$, $Onsigncrypt$ and $UnSigncrypt$. A secure symmetric key encryption scheme $(\mathcal{E}, \mathcal{D})$ is employed in this scheme where $\mathcal{E}$ and $\mathcal{D}$ are the secure symmetric encryption and decryption algorithms respectively.

1. **Setup** : Given security parameters κ, n and $\mathbb{G}_1$,$\mathbb{G}_2$ of order q and generator P of $\mathbb{G}_1$, PKG picks a random $s \in \mathbb{Z}_q^*$, ands sets $P_{pub} = sP$. Choose cryptographic hash functions $H_0 : \{0,\ 1\}^* \rightarrow \mathbb{G}_1$, $H_1 : \{0,\ 1\}^* \times \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_2 : Z_q^* \rightarrow \{0,\ 1\}^n$, $H_3 : \mathbb{G}_2 \rightarrow \mathbb{Z}_q^* \times \mathbb{Z}_q^*$. The system parameters are $\langle P, P_{pub}, H_0, H_1, H_2, H_3 \rangle$. The master secret key is s.

2. **Key Extract** : Given an identity ID_i, the algorithm computes the public key as $Q_i = H_0(ID_i)$ and the corresponding private key as $D_i = sH_0(ID_i)$. The private key is returned to the user via a secure channel.

3. **OffSigncrypt** : To send a message m to user $U_{\mathbb{R}}$ with identity $ID_{\mathbb{R}}$, the sender $U_{\mathbb{S}}$ with identity $ID_{\mathbb{S}}$ follows the steps below.
   (a) Computes $Q_{\mathbb{R}} = H_0(ID_{\mathbb{R}})$.
   (b) Picks random x, y $\in \mathbb{Z}_q^*$, and sets $k = H_3(e(P_{pub}, Q_{\mathbb{R}})^x)$.
   (c) Splits k into k_1, k_2 such that $k_1 \in \mathbb{Z}_q^*$ and $k_2 \in \mathbb{Z}_q^*$, then stores them for future use.
   (d) Using the private key $D_{\mathbb{S}}$, $U_{\mathbb{S}}$ outputs the offline signcryption (S, U), where $S = D_{\mathbb{S}} - xP_{Pub}$, $U = (y - k_1)P$; also stores x, y for future use.

4. **OnSigncrypt** : Given a message $m \in \mathbb{Z}_q^*$, and an off-line signcryption (S, U), this algorithm sets $k_3 = H_2(k_2)$ first. The message encryption is done with k_3 and a symmetric-key encryption algorithm $\mathcal{E}$ such as AES. The ciphertext is $c = \mathcal{E}_{k_3}(m)$. Computes $r = H_1(c, S, U)$ and on-line signcryption $\sigma = rx + y$; returns signcryption (c, S, U, σ).

5. **UnSigncrypt** : Given a signcryption (c, S, U, σ), the receiver with identity $ID_{\mathbb{R}}$ does the following :

(a) Computes $T = e(-S, Q_{\mathbb{R}})e(Q_{\mathbb{S}}, D_{\mathbb{R}})$.
(b) Sets $k = H_3(T)$,then splits k into k_1, k_2.
(c) Sets $k_3 = H_2(k_2)$ and decrypts the message $\mathcal{D}_{k_3}(c) = m$. m is valid if $e(\sigma P_{pub} + rS, P) \stackrel{?}{=} e(U + k_1 P + rQ_{ID_A}, P_{pub})$ holds, where $r = H_1(c, S, U)$.

4.2 Forgeability attack on the Scheme

This scheme is not secure against existential forgery. A forger $\mathcal{F}$ can forge a signcryption for an identity whose private key is not queried. This can be done as follows:

- $\mathcal{F}$ sets an identity ID_A as the target identity for which the forged signcryption is to be generated.
- During unforgeability game, a forger is allowed to extract the private key of receiver (used for generating the forgery) according to the model given by Sun et al [12]
- During the Training phase, $\mathcal{F}$ asks for the signcryption of a message m from ID_A to an arbitrary receiver ID_B. Let the response be (c, S, U, σ). On receiving this, $\mathcal{F}$ computes the following
  - Gets the private key of ID_B using a Key_Extract query on ID_B.
  - Computes $T = \hat{e}(-S, Q_B)\hat{e}(Q_A, D_B)$
  - Sets $k = H_3(T)$ and divides k into two parts : k_1 and k_2.
- $\mathcal{F}$ can now modify the above ciphertext (c, S, U, σ) so that it becomes a valid signcryption on some message m' from ID_A to an arbitrary ID_C. For achieving this $\mathcal{F}$ computes following:
  - $T' = \hat{e}(-S, Q_C)\hat{e}(Q_A, D_C)$
  - $k' = H_3(T')$ and it is divided into two parts : k'_1 and k'_2
  - $\Delta k = k'_1 - k_1$ and $\sigma' = rx + y + \Delta k$
  - Outputs the new signcryption (c, S, U, σ')

This will pass through the verification because

$$\begin{aligned}
\text{LHS} &= \hat{e}(\sigma' P_{pub} + rS, P) \\
&= \hat{e}((rx + y + \Delta k)P_{pub} + r(D_A - xP_{pub}), P) \\
&= \hat{e}((y + \Delta k)P_{pub} + rsQ_A, P) \\
&= \hat{e}((y + k'_1 - k_1)P + rQ_A, sP) \\
&= \hat{e}((y - k_1)P + k'_1 P + rQ_A, P_{pub}) \\
&= \hat{e}(U + k'_1 P + rQ_A, P_{pub}) \\
&= \text{RHS}
\end{aligned}$$

5 Review of Generic Identity Based Online/Offline Signcryption Scheme by Sun et al.[13]

5.1 Review of the Scheme

1. **Systems Parameter Generation** : Let t be a prime power, and $E(\mathbb{F}_t)$ an elliptic curve over finite field $\mathbb{F}_t$. Let $\#E(\mathbb{F}_t)$ be the number of points of $\#E(\mathbb{F}_t)$, and P be a point of $E(\mathbb{F}_t)$ with prime order q where $q|\#E(\mathbb{F}_t)$. $\mathbb{G}_1$ is the subgroup generated by P. $\mathbb{G}_2$ is a finite group of order q. Choose cryptographic hash function $H_1 : \mathbb{G}_2 \rightarrow \{0,1\}^n$. Let $(\mathcal{L}, \mathcal{H})$ be the chameleon hash family, which will be sent to the designated user on request, based on the discrete logarithm assumption and $(\mathcal{G}, \mathcal{S}, \mathcal{V})$ be any identity-based signature scheme. The system parameters are $SP = (\#E(\mathbb{F}_t), t, q, P, \mathbb{G}_1, \mathbb{G}_2, (\mathcal{G}, \mathcal{S}, \mathcal{V}), H_1)$.
2. **Key Extract**:
   - Given an identity ID, run the key extract algorithm of the original identity-based signature scheme to obtain the private/public key pair (D_{ID}, Q_{ID}).
   - On input 1^k , the sender runs the key generation algorithm of the trapdoor hash family $(\mathcal{L}, \mathcal{H})$ to obtain the hash/trapdoor key pair $(Y = xP, x)$.

   Assume user $U_{\mathbb{S}}$ with identity $ID_{\mathbb{S}}$ sends m to user $U_{\mathbb{R}}$ with identity $ID_{\mathbb{R}}$. $U_{\mathbb{S}}$ obtains private key and hash/trapdoor key $\{D_{\mathbb{S}}, Y, x\}$. $U_{\mathbb{R}}$ obtains private key $D_{\mathbb{R}}$. $\{Q_{\mathbb{S}}, Q_{\mathbb{R}}\}$ are public to both of them.
3. **OffSigncrypt**

- Choose at random $(m, r) \in_R \mathcal{M} \times \mathcal{R}$, where $\mathcal{M}$ is a message space and $\mathcal{R}$ is a finite space, and compute the chameleon hash value $h = H_Y(m', r') = m'P + r'Y$.
- Run the signing algorithm $\mathcal{S}$ with the signing key $D_{\mathbb{S}}$ to sign the hash value h. Let the output be $\sigma = S_{D_{\mathbb{S}}}(h||H_Y)$, where H_Y is the description of the chameleon hash.
- Choose at random $y \in_R Z_q^*$ and compute $X = yP$ then compute $\omega = e(yP_{pub}, Q_{\mathbb{R}})$. Finally set $y' = H_1(\omega)$.
- Store the pair (m', r') and y' for future use.

4. **OnSigncrypt**
   - For a given message m, retrieve from the memory x^{-1} and the pair (m, r).
   - Compute $r = x^{-1}(m' - m) + r' \bmod q$.
   - The message encryption is done with y' and a symmetric-key encryption algorithm such as AES. The ciphertext is $c = Enc_{y'}(\sigma||ID_{\mathbb{S}}||m||r||H_Y)$.
   - Final ciphertext is (c, X).
5. **Unsigncrypt**
   - Given ciphertext (c, X), compute $\omega = e(X, d_{ID_B})$ and $y' = H_1(\omega)$.
   - Decrypt c as $\sigma||ID_{\mathbb{S}}||m||r||H_Y = Dec_{y'}(c)$.
   - Compute $h = H_Y(m, r) = mP + rY$.
   - Verify that σ is indeed a signature of the value $h||H_Y$ with respect to the verification key $Q_{\mathbb{S}}$.

5.2 Security Analysis

In the scheme proposed by Sun et al. [13], there is no binding between the encryption and the signature. Therefore, a signcryption on a message m from ID_A to ID_B can be changed to a valid signcryption on the same message m from ID_A to ID_C. This can be done as follows:

- Get the signcryption of message m from the sender ID_A to receiver ID_B and decrypt it using the secret key D_B of ID_B to get $\sigma||ID_A||m||r||H_Y$.
- Choose $\eta \in_R Z_q^*$ and compute $\omega^* = \hat{e}(P_{pub}, Q_C)^\eta$ and set $X^* = \eta P$ and $y^* = H_1(\omega)$.
- Compute $c^* = Enc_{y^*}(\sigma||ID_A||m||r||H_Y)$
- Output the signcryption as $(c^*,\ X^*)$

Note that Q_C is the public key of the user with identity ID_C whose private key is not known. The new signcryption $(c^*,\ X^*)$ is a valid signcryption from ID_A to ID_C.

6 Analysis of the Scheme by Liu et al. [6]

The scheme in [6] is available in public archive we do not review the scheme here. In this section, we present the attack on sender anonymity of the scheme. We also, point out the weakness in the security proof of [6].

6.1 Attack on Sender Anonymity

The scheme in [6] is claimed to be sender anonymous, in the sense that no party other than the receiver will be able to know the actual sender of the signcryption. According to the security model for sender anonymity in [6] the adversary $\mathcal{A}$ knows the private keys $D_{ID_{s,0}}$ and $D_{ID_{s,1}}$ of two senders $ID_{s,0}$ and $ID_{s,1}$, chosen for the challenge phase. $\mathcal{A}$ does not know the private key D_{ID_R} of the receiver ID_R. Let $\pi = \langle U, t, c, T_0, T_1, T_2, t'_1, t'_2 \rangle$ be the challenge signcryption. $\mathcal{A}$ performs the following computation to trace the sender of π:

- Computes $X_0 = \hat{e}(g^t U, g^{H_1(ID_{s,0})} g_1)\hat{e}(g, g)^{-1}$ and $X_1 = \hat{e}(g^t U, g^{H_1(ID_{s,1})} g_1)\hat{e}(g, g)^{-1}$.
- Computes $Y_0 = U D^{-1}_{ID_{s,0}} g^t$ and $Y_1 = U D^{-1}_{ID_{s,1}} g^t$.
- Computes $Z_0 = \hat{e}(Y_0, g^{H_1(ID_{s,0})} g_1)$ and $Z_1 = \hat{e}(Y_1, g^{H_1(ID_{s,1})} g_1)$.
- Check whether $X_i \stackrel{?}{=} Z_i$ for $i = 0, 1$. Output the value of i for which the test holds.

6.2 Note on the Security Proof

It is to be noted that, the simulation of the unsigncryption oracle in the security proof (both confidentiality and unforgeability) does not capture the real scenario. The description follows:

- Let ID_s be a sender whose private key D_s is known to $\mathcal{A}$. Let ID_r be the receiver whose private key D_r is not known to $\mathcal{A}$ (the target identity).
- $\mathcal{A}$ computes a signcryption $\pi = \langle U, t, c, T_0, T_1, T_2, t_1', t_2' \rangle$ of a message m as follows:
  - Picks $T_0, T_1, T_2 \in_R \mathbb{G}$ and picks $x, u, t_1', t_2' \in_R \mathbb{Z}_q^*$.
  - Computes $R = (G_{ID_s})^x$, where $G_{ID_s} = \hat{e}(g^{H_1(ID_s)} g_1, g)$.
  - Sets $U = D_s g^{-u}$.
  - $\mathcal{A}$ queries the H_2 oracle with $(m, ID_s, R, T_0, T_1, T_2, t_1', t_2', U)$ as input and obtains h_2.
  - Computes $t = (h_2 x + u)\ mod\ q$ and computes the H_3 oracle with (R, T_1, T_2, U) as input to obtain h_3 and computes $c = m || ID_s \oplus h_3$.

  It should be noted that π is an invalid ciphertext since T_0, T_1, T_2, t_i' and t_2' are chosen randomly, therefore, $R' = \hat{e}(T_0 T_1^{t_1'} T_2^{t_2'}, D_r)$ and $R'^{h_2} \neq R^{h_2} = \hat{e}(g^t U, g^{H_1(ID_s)} g_1)$. In reality, this condition this condition gets satisfied, i.e. an invalid signcryption does not pass the verification but in the simulation for unsigncryption oracle, $\mathcal{C}$ checks only with R obtained from the list and thus $\mathcal{C}$ is unable to verify whether the original R' obtained using private key D_r is the same as R.

7 Identity Based Online/Offline Signcryption Scheme

In this section we present the first provably secure identity based online/offline signcryption scheme which consists of the following algorithms

***Setup*(1^κ) :** Given the security parameter 1^κ as input, PKG chooses two groups $\mathbb{G}_1$, $\mathbb{G}_2$ of prime order q, a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and a generator $P \in_R \mathbb{G}_1$. The PKG chooses a random $s \in_R \mathbb{Z}_q^*$ and sets master secret key $msk = s$ and also sets master public key $P_{pub} = sP$. PKG then computes $\alpha = \hat{e}(P,\ P)$ and defines five hash functions :

- $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$.
- $H_2 : \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_1 \times \{0,1\}^{n_1} \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.
- $H_3 : \{0,1\}^{n_1} \times \{0,1\}^* \times \mathbb{G}_1 \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.
- $H_4 : \mathbb{G}_2 \rightarrow \{0,1\}^{n_1+n_m}$. where n_m is the message size n_1 is the number of random bits concatenated to message.
- $H_5 : \{0,1\}^{n_m} \times \mathbb{G}_2 \times \{0,1\}^{n_1} \times \mathbb{Z}_q^* \times \mathbb{Z}_q^* \times \{0,1\}^{n_1+n_m} \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

The public parameters *Params* of the system are set to be $Params = \langle \mathbb{G}_1,\ \mathbb{G}_2,\ \hat{e},\ P,\ R,\ P_{pub},\ H_1,\ H_2,\ H_3,\ H_4,\ \alpha\ \rangle$.

***Key Extract*(ID_i) :** On input of identity ID_i of user U_i, the private key D_i is computed as $D_i = (\frac{1}{q_i+s})P)$, where $q_i = H_1(ID_i)$. D_i is given to user by PKG via. secure channel.

***Off-Signcrypt*$(ID_\mathbb{S},\ D_\mathbb{S})$:** This algorithm is run by the sender $U_\mathbb{S}$ with identity $ID_\mathbb{S}$ for sending any message to any receiver. Note that the sender carries out these computations without the knowledge message and receiver information.

1. Selects $\delta \in_R \{0,1\}^{n_1}$ and $b, x, y, z, r \in_R \mathbb{Z}_q^*$.
2. Computes $U_1 = \alpha^r \in \mathbb{G}_2$, $U_2 = yP \in \mathbb{G}_1$ and $U_3 = zP \in \mathbb{G}_1$.
3. Computes $V = (r + h_2)D_\mathbb{S} \in \mathbb{G}_1$, where $h_2 = H_2(U_1,\ U_2,\ U_3,\ \delta,\ ID_S)$.
4. Computes $a = H_3(\delta,\ V,\ ID_\mathbb{S})$.
5. Computes $C_1 = a^{-1}xP$, $C_2 = x(b + s)P$.
6. Sets $k = H_4(\omega = \alpha^x)$.

Outputs the offline signcryption $\sigma' = \langle C_1, C_2, V, U_1, U_2\rangle$, while $\sigma_{secret} = \langle k,\, \omega,\, a,\, b,\, y,\, z\rangle$ are kept as secret for future use in online phase and they are not made public. Note here that the output of the $Off - Signcrypt$ algorithm can be used only once to generate an online signcryption.

Remark : It should be noted that above offline signcryption σ' does not require the knowledge of the message or the receiver.

On-Signcrypt$(\boldsymbol{m},\ \boldsymbol{ID}_{\mathbb{S}},\ \boldsymbol{ID}_{\mathbb{R}},\ \sigma',\ \sigma_{secret})$ **:** This algorithm is run by the sender, once the message $m \in \mathcal{M}$ and the receiver identity $\mathrm{ID}_{\mathbb{R}}$ are available and makes use of the offline signature $\sigma' = \langle C_1, C_2, V, U_1, U_2\rangle$, along with the stored values $\sigma_{secret} = \langle k,\, \omega,\, a,\, b,\, y,\, z\rangle$.

1. Compute $C_3 = a(q_{\mathbb{R}} - b) \bmod q$.
2. Compute $C_4 = (m \| \delta) \oplus k$.
3. Compute $v = yh + z \bmod q$ where $h = H_5(m,\, \omega,\, \delta,\, h_2,\, C_3,\, C_4,\, ID_{\mathbb{S}}, ID_{\mathbb{R}})$.
4. Outputs the signcryption $\sigma = \langle \{C_i\}_{i=1\,to\,4},\, U_1,\, U_2,\, U_3 V,\, v\rangle$.

Remark : Here, the $On - Signcrypt$ phase includes only one hash computation.

Unsigncrypt$(\sigma,\ \boldsymbol{ID}_{\mathbb{S}},\ \boldsymbol{ID}_{\mathbb{R}},\ \boldsymbol{D}_{\mathbb{R}})$ **:** When the receiver $U_{\mathbb{R}}$ with identity $ID_{\mathbb{R}}$ is provided with the signcryption $\langle \sigma,\, U_{\mathbb{S}},\, U_{\mathbb{R}}\rangle$ uses the following steps to unsigncrypt the signcryption $\sigma = \langle \{C_i\}_{i=1\,to\,4},\, U_1,\, U_2,\, U_3,\, V,\, v\rangle$ from $ID_{\mathbb{R}}$:

1. Computes $\omega' = \hat{e}(C_3 C_1 + C_2, D_{\mathbb{R}})$ and $k' = H_3(\omega')$.
2. $(m' \| \delta') = C_4 \oplus k'$.
3. Computes $h_2' = H_2(U_1,\, U_2,\, U_3,\, \delta',\, ID_S)$ and $h' = H_5(m',\, \omega',\, \delta',\, h_2',\, C_3,\, C_4,\, ID_{\mathbb{S}}, ID_{\mathbb{R}})$.
4. Verify $U_2 h' + U_3 \stackrel{?}{=} vP$, $\hat{e}(P, C_1)^{H_3(\delta',\, V,\, ID_{\mathbb{S}})} \stackrel{?}{=} \omega'$ and $\hat{e}(V, (q_{\mathbb{S}} + s)P)\alpha^{-h_2'} \stackrel{?}{=} U_1$
5. If all the checks in the above step holds, then output the message m', else output "$Invalid''$.

Correctness : We show the correctness of the unsigncryption algorithm here.

$$\begin{aligned}
\omega' \ = \ \hat{e}(C_3 C_1 + C_2, D_{\mathbb{R}}) &= \hat{e}((q_{\mathbb{R}} - b)xp + x(b+s)P, \tfrac{1}{q_{\mathbb{R}}+s}P) \\
&= \hat{e}((q_{\mathbb{R}} + s)xP, \tfrac{1}{q_{\mathbb{R}}+s}P) \\
&= \hat{e}(xP, P) \\
&= \hat{e}(P, P)^x \\
&= \alpha^x \\
&= \omega
\end{aligned}$$

The correctness of the verification tests $U_2 h' + U_3 \stackrel{?}{=} vP$, $\hat{e}(P, C_1)^{H_3(\delta',\, V,\, ID_{\mathbb{S}})} \stackrel{?}{=} \omega'$ and $\hat{e}(V, (q_{\mathbb{S}} + s)P)\alpha^{-h'} \stackrel{?}{=} U_1$ is shown below :

Correctness of $U_2 h' + U_3 \stackrel{?}{=} vP$:

$$\begin{aligned}
h' U_3 + U_1 &= h'(yP) + rP \\
&= (h'y + r)P \\
&= vP
\end{aligned}$$

Correctness of $\hat{e}(P, C_1)^{H_3(\delta',\, V,\, ID_{\mathbb{S}})} \stackrel{?}{=} \omega'$:

$$\begin{aligned}
\hat{e}(P, C_1)^{H_3(\delta',\, V,\, ID_{\mathbb{S}})} &= \hat{e}(P, a^{-1}xP)^a \\
&= \hat{e}(P, P)^x \\
&= \omega' = \omega
\end{aligned}$$

Correctness of $\hat{e}(V, (q_{\mathbb{S}} + s)P)\alpha^{-h'} \stackrel{?}{=} U_1$:

$$\begin{aligned}
\hat{e}(V, (q_{\mathbb{S}} + s)P)\alpha^{-h_2'} &= \hat{e}((r + h_2)D_{\mathbb{S}}, (q_{\mathbb{S}} + s)P)\hat{e}(P, P)^{-h_2'} \\
&= \hat{e}((r + h_2)\frac{1}{q_{\mathbb{S}} + sP}, (q_{\mathbb{S}} + s)P)\hat{e}(P, P)^{-h_2'} \\
&= \hat{e}(P, P)^{r + h_2}\hat{e}(P, P)^{-h_2'} \\
&= \hat{e}(P, P)^r \\
&= U_1
\end{aligned}$$

8 Security Analysis of Identity Based Online/Offline Signcryption Scheme

In the new identity based online/offline signcryption scheme proposed above, we are not directly signing the message, instead two randomness are signed which are acting as the public keys for signing the message using a one-time schnorr signature[9].

8.1 Confidentiality of IBOOSC(IND-IBOOSC-CCA2)

Theorem 1. *If there exists an IND-IBOOSC-CCA2 attacker $\mathcal{A}$, making q_{h_i} queries to the random oracles H_i, for $(i = 1, 2, 3, 4, 5)$, q_s queries to the signcryption oracle and q_us queries to the unsigncryption oracle, and that can break the confidentiality of IBOOSC with advantage ϵ, then there exists an algorithm $\mathcal{C}$ that is able to solve the q-SDHIP for $q = q_{h_1}$ with advantage ϵ'.*

Proof of Theorem 1 : The proof of this theorem will be added soon.

8.2 Unforgeability of IBOOSC(EUF-IBOOSC-CMA)

Theorem 2. *If there exists an EUF-IBOOSC-CMA attacker $\mathcal{A}$, making q_{h_i} queries to the random oracles H_i, for $(i = 1, 2, 3, 4, 5)$, q_s queries to the signcryption oracle and q_u queries to the unsigncryption oracle, and produces a forgery with probability $\epsilon \geq 10(q_s + 1)(q_s + q_{h_2})/2^{\kappa}$, then there exists an algorithm $\mathcal{C}$ that is able to solve the q-CDHIP for $q = q_{h_1}$.*

Proof of Theorem 2 : The proof of this theorem will be added soon.

9 Conclusion

In this paper, we showed security weaknesses in all existing identity based online/offline signcryption schemes[12, 13, 6]. Also, we proposed the first provably secure identity based online/offline signcryption scheme which does not require the knowledge of the message and receiver. We proved the security of our scheme in the random oracle model.

References

1. Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer, 2002.
2. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, 1993.
3. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
4. Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptographic protocols: A survey. In *In Cryptology ePrint Archive, Report 2004/064*, 2004.
5. Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *J. Cryptology*, 9(1), 1996.
6. Joseph K. Liu, Joonsang Baek, and Jianying Zhou. Online/offline identity-based signcryption re-visited. Cryptology ePrint Archive, Report 2010/274, 2010. http://eprint.iacr.org/.
7. John Malone-lee. Identity-based signcryption. In *In Proceedings of Public Key Cryptography - PKC 2005, LNCS 3386*, pages 362–379. Springer, 2002.
8. David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, Vol.13(No.3):361–396, 2000.
9. Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3), 1991.
10. Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.
11. Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 355–367. Springer, 2001.
12. Dongdong Sun, Xinyi Huang, Yi Mu, and W. Susilo. Identity-based on-line/off-line signcryption. In *Network and Parallel Computing, 2008. NPC 2008. IFIP International Conference on*, pages 34–41, 2008.
13. Dongdong Sun, Yi Mu, and Willy Susilo. A generic construction of identity-based online/offline signcryption. In *ISPA*, pages 707–712. IEEE, 2008.

14. Fangguo Zhang, Yi Mu, and Willy Susilo. Reducing security overhead for mobile networks. In *AINA '05: Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, pages 398–403. IEEE Computer Society, 2005.
15. Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In *CRYPTO*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.