Identity Based Public Verifiable Signcryption Scheme

S. Sharmila Deva Selvi, S. Sree Vivek * and 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. Signcryption as a single cryptographic primitive offers both confidentiality and authentication simultaneously. Generally in signcryption schemes, the message is hidden and thus the validity of the ciphertext can be verified only after unsigncrypting the ciphertext. Thus, a third party will not be able to verify whether the ciphertext is valid or not. Signcryption schemes that allow any user to verify the validity of the ciphertext without the knowledge of the message are called public verifiable signcryption schemes. Third Party verifiable signcryption schemes allow the receiver to convince a third party, by providing some additional information along with the signcryption other than his private key with/without exposing the message.

In this paper, we show the security weaknesses in three existing schemes [2], [14] and [4]. The schemes in [2] and [14] are in the Public Key Infrastructure (PKI) setting and the scheme in [4] is in the identity based setting. More specifically, [14] is based on elliptic curve digital signature algorithm (ECDSA). We also, provide a new identity based signcryption scheme that provides public verifiability and third party verification. We formally prove the security of the newly proposed scheme in the random oracle model.

Keywords: Signcryption, Public verifiable Signcryption, Cryptanalysis, Identity Based, Bilinear Pairing, Random Oracle Model.

1 Introduction

Secure communication through an insecure channel requires both confidentiality and authenticity as security goals. Encryption schemes are used to achieve confidentiality and digital signature schemes offer unforgeability. Signcryption scheme is a cryptographic primitive that achieves both these properties together in an efficient way. Zheng [17] proposed the first digital signcryption scheme that offers both confidentiality and authentication in a single logical step with lower computational cost and communication overhead than sign then encrypt (StE) or encrypt then sign (EtS) approach. Since then, many signcryption schemes were proposed. Baek et al. [1] gave the formal security model for digital signcryption schemes and provided the security proof for Zheng's scheme [17] in the random oracle model.

Adi Shamir [11] introduced the concept of identity based cryptography and proposed the first identity based signature scheme. The idea of identity based cryptography is to enable one to use any arbitrary string that uniquely identifies him as his public key. Identity based cryptography serves as an efficient alternative to Public Key Infrastructure (PKI) based systems. Digital signcryption in the identity based setting was first studied by Malone-Lee et al. [8]. Later, Libert et al. [7] pointed out that the scheme proposed by Malone-Lee [8] is not semantically secure, since the signature of the message is visible in the signcryption and thus cannot achieve CCA security. Following that many signcryption schemes were proposed in both PKI setting as well as identity based setting [10, 2, 9, 13, 15, 3, 4, 6].

Normally, in a signcryption scheme, the message is hidden and thus the validity of the ciphertext can be verified only after unsigncrypting the ciphertext. Thus, a third party who is unaware of the receiver's private key will not be able to verify whether a ciphertext is valid or not. Public verifiable signcryption schemes are applicable in filtering out the spams in a secure email system. The spam filter should be able to verify the

* 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

authenticity of the ciphertext without knowing the message (i.e., check whether the signcryption is generated from the claimed sender or not). Moreover, in applications such as private contract signing, made between two parties, the receiver of the signcryption should be able to convince the third party that indeed the sender has signed the corresponding message hidden in the signcryption. In this case, the receiver should not reveal his secret key in order to convince the third party, instead he reveals the message and some component computable with his private key required for the signature verification. In literature, signcryption schemes in which a third party can verify the validity of the ciphertext without the knowledge of the hidden message, or without knowing the receiver private key are called third party verifiable signcryption schemes.

Related Work: To the best of out knowledge, Bao et al. [2] proposed the first public verifiable signcryption scheme in the PKI based setting. Following that, a number of schemes [14, 16, 12, 5] were proposed in the PKI based setting. Chow et al. [4] proposed an identity based signcryption scheme that provides both public verifiability and forward security. To the best of our knowledge the scheme in [4] is the only identity based scheme providing public verifiability and third party verification.

Our Contribution : In this paper, we have upgraded the model for public verifiable and third party verifiable identity based signcryption scheme by providing additional power to the adversary. This is provided by giving the adversary the access to a new oracle called third party verifiable oracle which provides the information necessary for the third party verification. Next, we show that the scheme in [4] is not secure. We have demonstrated a CCA2 and forgeability attack on []. In the next section, we have shown that scheme in [2] is not CPA secure. Also, we have shown CCA2 attack on the forward security of []. Finally, we have proposed a new identity based signcryption scheme that offers the property of public verifiability and third party verification linking message to the ciphertext and we have formally proved the security of the new scheme in the newly proposed security model. Our scheme also incorporates the forward secrecy property.

2 Formal Model for Identity Based Signcryption Schemes With Public Verifiability

2.1 Generic scheme

An identity based signcryption scheme consists of the following algorithms.

- ***Setup***(1^κ) *: Given a security parameter κ, the Private Key Generator(PKG) generates a master private key msk and public parameters Params. Params is made public while msk is kept secret by the PKG.*
- ***Extract***(ID) *: Given an identity ID, the PKG executes this algorithm to generate the private key D_{ID} corresponding to ID and transmits D_{ID} to the user with identity ID via. secure channel.*
- ***Signcrypt***(m, ID_A, D_A, ID_B) *: A sender with identity ID_A and private key D_A to send a message m to a receiver whose identity is ID_B, runs this algorithm to generate the signcryption σ of message m.*
- ***Unsigncrypt***$(\sigma, ID_A, ID_B, D_B)$ *: On receiving the ciphertext σ from sender with identity ID_A, receiver with identity ID_B and private key D_B executes this algorithm to obtain the message m if σ is a valid signcryption of m from ID_A to ID_B or "$Invalid''$ indicating that the ciphertext is not valid.*
- ***Public-Verify(***σ, ID_A, ID_B***)*** *: This algorithm allows receiver ID_B to verify the authenticity of the signcryption σ without knowing the message used for the signcryption of σ. This algorithm takes as input the signcryption σ, the sender identity ID_A and the receiver identity ID_B and outputs "$Valid$", if σ is a valid signcryption. Otherwise, outputs "$Invalid$".*
- ***TP-Verify(***ϕ, ID_A, ID_B***)*** *: This algorithm allows the user ID_B to prove the authenticity of the signcryption σ to third party by providing additional information needed other than the private key D_B. This algorithm run by the third party takes as input ϕ(σ and additional information provided by ID_B), the sender identity ID_A and receiver identity ID_B and outputs "$Valid$", if σ is a valid signcryption from ID_A to ID_B. Otherwise, outputs "$Invalid$". Here, it should be noted that $TP - Verify$ has two types. First type, is to prove the validity without exposing the message(similar to Public-Verify but receiver concern is involved) and the second type, is to prove that the ciphertext is indeed a valid signcryption of the message(done by exposing the message being signcrypted)*

2.2 Security Notions

Definition 1. *An ID-Based signcryption scheme is said to be indistinguishable against adaptive chosen ciphertext attacks (IND-IBSC-CCA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. ***Setup :*** The challenger $\mathcal{C}$ runs the *Setup* algorithm with a security parameter κ and obtains public parameters *Params* and the master private key *msk*. $\mathcal{C}$ sends *Params* to the adversary $\mathcal{A}$ and keeps *msk* secret.
2. ***Phase I :*** The adversary $\mathcal{A}$ performs a polynomially bounded number of queries to $\mathcal{C}$. The queries made by $\mathcal{A}$ may be adaptive, i.e. current query may depend on the answers to the previous queries. The various oracles and the queries made to these oracles are defined below:
   - ***Key extraction queries(Oracle*** $\mathcal{O}_{Extract}(ID)$***) :*** $\mathcal{A}$ produces an identity ID and receives the private key D_{ID}.
   - ***Signcryption queries(Oracle*** $\mathcal{O}_{Signcrypt}(m, ID_A, ID_B)$***) :*** $\mathcal{A}$ produces two identities ID_A, ID_B and a plaintext m. $\mathcal{C}$ computes $D_A = \mathcal{O}_{Extract}(ID_A)$ and generates the signcryption σ of the message m using D_A following the signcryption protocol and sends σ to $\mathcal{A}$.
   - ***Unsigncryption queries(Oracle*** $\mathcal{O}_{Unsigncrypt}(\sigma, ID_A, ID_B)$***) :*** $\mathcal{A}$ produces the sender identity ID_A and the receiver identity ID_B and the ciphertext σ as input to this algorithm and requests the unsigncryption of σ. $\mathcal{C}$ generates the private key D_B and performs the unsigncryption of σ using D_B and sends the result to $\mathcal{A}$. The result of unsigncryption will be "$Invalid''$ if σ is not a valid signcryption. It returns the message m if σ is a valid signcryption.
   - ***TP-Verify queries(Oracle*** $\mathcal{O}_{TP-Verify}(\sigma, ID_A, ID_B)$***) :*** $\mathcal{A}$ submits the information ϕ, the sender identity ID_A and the receiver identity ID_B. $\mathcal{C}$ generates the private key D_B corresponding to ID_B, unsigncrypts σ using D_B and returns the information required for TP - verify corresponding to σ, if σ is a valid signcryption otherwise returns "$Invalid''$.
3. ***Challenge :*** $\mathcal{A}$ chooses two plaintexts, m_0 and m_1 of equal length, the sender identity $ID_{\mathbb{S}}$, the receiver identity $ID_{\mathbb{R}}$and submits them to $\mathcal{C}$. However, $\mathcal{A}$ should not have queried the private key corresponding to $ID_{\mathbb{R}}$ in Phase I. $\mathcal{C}$ now chooses $\delta \in_R \{0, 1\}$ and computes $\sigma^* = \mathcal{O}_{Signcrypt}(m_\delta,\ ID_{\mathbb{S}},\ ID_{\mathbb{R}})$ and sends σ^* to $\mathcal{A}$.
4. ***Phase II :*** $\mathcal{A}$ is allowed to interact with $\mathcal{C}$ as in Phase-I with the following restrictions.
   - $\mathcal{A}$ should not query the extract oracle for the private key corresponding to the receiver identity $ID_{\mathbb{R}}$.
   - $\mathcal{A}$ should not query the unsigncrypt oracle with $(\sigma^*, ID_{\mathbb{S}}, ID_{\mathbb{R}}$ as input, i.e. a query of the form $\mathcal{O}_{Unsigncrypt}(\sigma^*,\ ID_{\mathbb{S}},\ ID_{\mathbb{R}})$ is not allowed.
5. ***Guess :*** Finally, $\mathcal{A}$ produces a bit $\delta^{'}$ and wins the game if $\delta^{'} = \delta$.

Advantage of $\mathcal{A}$ in the above game is defined by Adv$(\mathcal{A}) = 2\left|Pr\left[\delta^{'} = \delta\right] - 1\right|$ *where* $Pr\left[\delta^{'} = \delta\right]$ denotes the probability that $\delta^{'} = \delta$.

The confidentiality game described above deals with insider security since the adversary is given access to the private key of the sender $ID_{\mathbb{S}}$ used for the challenge phase.

Definition 2. *An ID-Based signcryption scheme is said to be existentially unforgeable against adaptive chosen message attacks (EUF-IBSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. ***Setup :*** The challenger $\mathcal{C}$ runs the Setup algorithm with security parameter κ and obtains public parameters *Params* and a master private key *msk*. $\mathcal{C}$ sends *Params* to the adversary $\mathcal{A}$ and keeps *msk* secret.
2. ***Training Phase :*** The adversary $\mathcal{A}$ performs a polynomially bounded number of queries adaptively as in Phase I of confidentiality game (IND-IDSC-CCA).
3. ***Forgery :*** After a sufficient amount of training, $\mathcal{A}$ produces a signcryption $(\sigma,\ ID_{\mathbb{S}},\ ID_{\mathbb{R}})$ to $\mathcal{C}$. Here, $\mathcal{A}$ should not have queried the private key of $ID_{\mathbb{S}}$ during the training phase and σ is not the output of signcrypt oracle with $(m, ID_{\mathbb{S}}, ID_{\mathbb{R}})$ as input(m=$\mathcal{O}_{Unsigncrypt}(\sigma,\ ID_{\mathbb{S}},\ ID_{\mathbb{R}})$). $\mathcal{A}$ wins the game, if *Unsigncrypt*$(\sigma,\ ID_{\mathbb{S}},\ ID_{\mathbb{R}},\ D_{\mathbb{R}})$ is valid.

The security model discussed above captures the notion of insider security since the adversary is provided access to the private key of receiver with identity $ID_{\mathbb{R}}$ used for generating the signcryption σ during the forgery phase.

3 Review and Attacks of the Signcryption Scheme in [4]

Chow et al. [4] have proposed the first identity based signcryption scheme which offers public verifiability. [4] claims to be insider secure during both confidentiality and unforgeability proof, which is the strongest notion of security for signcryption schemes. In this section, we review the identity based signcryption scheme proposed in [4] and demonstrate attacks on both CCA2 security as well as the existential unforgeability of the scheme. As the scheme was claimed to be insider secure we demonstrate the attack on confidentiality in the security model that captures insider security for signcryption schemes. However, the attack on unforgeability does not require the private key corresponding to the receiver associated with the forgery generated.

3.1 Review of Scheme in [4]

Let $\mathbb{G}_1, \mathbb{G}_2$ be two cyclic groups of prime order q and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be the bilinear pairing. Let $\mathcal{H}_1 : \{0,1\}^{\bar{n}} \rightarrow \mathbb{G}_1, \mathcal{H}_2 : \mathbb{G}_2 \rightarrow \{0,1\}^{\bar{n}}$ and $\mathcal{H}_3 : \{0,1\}^{\bar{n}} \times \mathbb{G}_2 \rightarrow \mathbb{F}_q^*$ be three cryptographic hash functions. Let $(\mathcal{E}, \mathcal{D})$ be the encryption and decryption algorithms of a secure symmetric cipher which takes a plaintext / ciphertext of length n respectively, and also a key of length $\bar{n}$.

Setup(1^κ) **:**

- $P \in_R \mathbb{G}_1$
- $s \in_R \mathbb{F}_q^*$
- $P_{Pub} = sP$
- $Params = \langle \mathbb{G}_1, \mathbb{G}_2, q, n, P, P_{Pub}, \hat{e}(.,.),$
- $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, (\mathcal{E}, \mathcal{D})\rangle$

Extract(ID_A)

- $Q_A = \mathcal{H}_1(ID_A)$
- $S_A = s^{-1}Q_A$
- $D_A = sQ_A$

Signcrypt(m, ID_A, S_A, ID_B)

- $x \in_R \mathbb{F}_q^*$
- $X_A \leftarrow xQ_A$
- $k_1 = \hat{e}(X_A, P)$
- $k_2 = \mathcal{H}_2(\hat{e}(X_A, Q_B))$
- $c = \mathcal{E}_{k_2}(m)$
- $r = \mathcal{H}_3(c, k_1)$
- $S = (x - r)S_A$
- Signcryption $\sigma = \langle c, r, S\rangle$

Unsigncrypt$(\sigma, ID_A, ID_B, D_B)$

- $X'_A = rQ_A$
- $k'_1 = \hat{e}(S, P_{Pub})\hat{e}(X'_A, P)$
- $k'_2 = \mathcal{H}_2(\hat{e}(S, D_B)\hat{e}(X'_A, Q_B))$
- $m' = \mathcal{D}_{k'_2}(c)$
- $r' = \mathcal{H}_3(c, k'_1)$
- Output $\sigma' = \langle k'_2, m, \sigma\rangle$ iff $r = r'$ else, return "$Invalid$"

TP-Verify(σ', ID_A, ID_B)

- $k'_1 = \hat{e}(S, P_{Pub})\hat{e}(X'_A, P)$
- $r' = \mathcal{H}_3(c, k'_1)$
- Accept σ iff $r = r'$
- Accept authenticity of m iff $m = \mathcal{D}_{k'_2}(c)$
- Return "$Valid$" iff the above two test holds, else return "$Invalid$"

3.2 Attack on Scheme in [4]

We show the attacks on [4] with respect to the confidentiality and the unforgeability in this section.

Attack on Confidentiality : This scheme does not provide insider security during the confidentiality game due to the following fact, stated informally: During the confidentiality game, the attacker knows the private key corresponding to the sender identity used for generating the challenge signcryption. The attacker can make use of this information, alter the challenge ciphertext in a meaningful manner and get the unsigncryption of the altered ciphertext during the second phase (Phase-II) of interaction with the challenger during the confidentiality game. This reveals the message used for generation of challenge signcryption. The details of the attack follows:

- During the challenge phase the attacker $\mathcal{A}$ chooses two message (m_0, m_1) of equal length, the sender identity $ID_{\mathbb{S}}$ and the receiver identity $ID_{\mathbb{R}}$, and submits them to the challenger $\mathcal{C}$.
- $\mathcal{C}$ chooses a random bit $\delta \in \{0,1\}$ and generates the signcryption $\sigma^* = \langle c^*, r^*, S^*\rangle = \mathcal{O}_{Signcrypt}(m_\delta, ID_{\mathbb{S}}, ID_{\mathbb{R}})$
- $\mathcal{C}$ issues σ^* as the challenge signcryption to $\mathcal{A}$.

- On receiving σ^*, $\mathcal{A}$ generates the signcryption $\widehat{\sigma} \neq \sigma^*$ by performing the following computations :
  - Let $ID_A \neq ID_{\mathbb{S}}$ be any user identity for which $\mathcal{A}$ knows the signcryption key S_A.
  - According to the definition of confidentiality with insider security, $\mathcal{A}$ also knows the signcryption key $S_{\mathbb{S}}$ of $ID_{\mathbb{S}}$
  - Set $\hat{c} = c^*$, $\hat{r} = r^*$
  - $\hat{S} = S^* + r^* S_{\mathbb{S}} - r^* S_A = x^* S_{\mathbb{S}} - r^* S_A$. Here $r^* \in \sigma^*$ and $S^* \in \sigma^*$
  - $\widehat{\sigma}$ is the signcryption of m_δ from ID_A to $ID_{\mathbb{R}}$
- Now, $\mathcal{A}$ queries the unsigncryption oracle for the unsigncryption of $\widehat{\sigma}$ i.e. $\mathcal{O}_{Unsigncrypt}(\widehat{\sigma}, ID_A, ID_{\mathbb{R}})$

The unsigncryption of σ^* (the signcryption of m_δ from $ID_{\mathbb{S}}$ to $ID_{\mathbb{R}}$) and the unsigncryption of $\widehat{\sigma}$ (the signcryption from $ID_{\mathbb{S}}$ to $ID_{\mathbb{R}}$ derived from σ^*) yields the same output m_δ. This can be shown by the following :

$$\begin{aligned}
\hat{k}_1 &= \hat{e}(\hat{S}, P_{Pub})\hat{e}(\hat{r}Q_A, P)\\
&= \hat{e}(x^*S_{\mathbb{S}} - r^*S_A, P_{Pub})\hat{e}(\hat{r}Q_A, P)\\
&= \hat{e}(s^{-1}(x^*Q_{\mathbb{S}} - r^*Q_A), sP)\hat{e}(\hat{r}Q_A, P)\\
&= \hat{e}(x^*Q_{\mathbb{S}} - r^*Q_A, P)\hat{e}(\hat{r}Q_A, P)\\
&= \hat{e}(x^*Q_{\mathbb{S}}, P)\hat{e}(r^*Q_A, P)^{-1}\hat{e}(\hat{r}Q_A, P)\\
&= \hat{e}(x^*Q_{\mathbb{S}}, P)\\
&= k_1^*.
\end{aligned}$$

This clearly shows that, the key k_2^* of σ^* and $\hat{k}_2$ of $\widehat{\sigma}$ are the same.

$$\begin{aligned}
\hat{k}_2 &= \mathcal{H}_2(\hat{e}(\hat{S}, D_{\mathbb{R}})\hat{e}(\hat{r}Q_A, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(s^{-1}(x^*Q_{\mathbb{S}} - r^*Q_A), sQ_{\mathbb{R}})\hat{e}(\hat{r}Q_A, Q_{\mathbb{R}}))\\
&\qquad (\text{Since } \hat{S} = x^*S_{\mathbb{S}} - r^*S_A)\\
&= \mathcal{H}_2(\hat{e}(x^*Q_{\mathbb{S}} - r^*Q_A, Q_{\mathbb{R}})\hat{e}(\hat{r}Q_A, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(x^*Q_{\mathbb{S}}, Q_{\mathbb{R}})\hat{e}(r^*Q_A, Q_{\mathbb{R}})^{-1}\hat{e}(\hat{r}Q_A, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(x^*Q_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= k_2^*
\end{aligned}$$

From this, it is clear that the value k_1^* of σ^* and $\hat{k}_1$ of $\widehat{\sigma}$ are the same.

According to the computations done by $\mathcal{A}$ it is clear that $c^* = \hat{c}$. When $c^* = \hat{c}, k_1^* = \hat{k}_1$ and $k_2^* = \hat{k}_2$ then $r^* = \hat{r}$.

This clearly shows that irrespective of the modifications done to $\widehat{\sigma}$ with respect to σ^* (sender $ID_{\mathbb{S}}$ of σ^* changed to sender ID_A of $\widehat{\sigma}$ and $S^* \neq \hat{S}$), the unsigncryption of σ^* and $\hat{\sigma}$ will be the same. This allows $\mathcal{A}$ to know the message m_δ by making use of the unsigncrypt oracle during Phase-II of the confidentiality game by querying the unsigncryption of $\hat{\sigma}$. Hence $\mathcal{C}$ will not be able to gain any advantage, if $\mathcal{A}$ responds with the correct $\delta' = \delta$.

Attack on Unforgeability : During the training phase of unforgeability game, $\mathcal{A}$ queries the signcrypt oracle fof the signcryption of message $\hat{m}$ from sender $ID_{\mathbb{S}}$ to receiver ID_B. Here, it should be noted that $\mathcal{A}$ does not know the private key (both signcryption key and designcryption key) of $ID_{\mathbb{S}}$ to ID_B. Let this signcryption be $\sigma = \langle c, r, S \rangle$. Now, $\mathcal{A}$ submits $\sigma^* = \sigma$(i.e. $c^* = c, r^* = r$ and $S^* = S$) as forgery with $ID_{\mathbb{S}}$ as sender and $ID_{\mathbb{R}}$ as receiver to $\mathcal{C}$. σ^* is a valid signcryption of some message m^*. It should be noted that, even $\mathcal{A}$ is not aware of the message m^*. The correctness and validity of $\sigma^* = \langle c^*, r^*, S^* \rangle$(signcryption of m^* from sender $ID_{\mathbb{S}}$ to receiver $ID_{\mathbb{R}}$) is shown below:

$$\begin{aligned}
k_1^* &= \hat{e}(S^*, P_{Pub})\hat{e}(r^*Q_{\mathbb{S}}, P)\\
&= \hat{e}(S, P_{Pub})\hat{e}(rQ_{\mathbb{S}}, P)\\
&\qquad (\text{since } S^* = S)\\
&= \hat{e}((x-r)S_{\mathbb{S}}, sP)\hat{e}(rQ_{\mathbb{S}}, P)\\
&= \hat{e}((x-r)s^{-1}Q_{\mathbb{S}}, sP)\hat{e}(rQ_{\mathbb{S}}, P)\\
&= \hat{e}((x-r)Q_{\mathbb{S}}, P)\hat{e}(rQ_{\mathbb{S}}, P)\\
&= \hat{e}(xQ_{\mathbb{S}}, P)\hat{e}(rQ_{\mathbb{S}}, P)^{-1}\hat{e}(rQ_{\mathbb{S}}, P)\\
&= \hat{e}(xQ_{\mathbb{S}}, P)\\
&= k_1
\end{aligned}$$

(Therefore, k_1^* of σ^* is equal to k_1 of σ).

$$\begin{aligned}
k_2^* &= \mathcal{H}_2(\hat{e}(S^*, D_{\mathbb{R}})\hat{e}(r^*Q_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(S, D_{\mathbb{R}})\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&\qquad (\text{Since } S^* = S)\\
&= \mathcal{H}_2(\hat{e}((x-r)S_{\mathbb{S}}, sQ_{\mathbb{R}})\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}((x-r)s^{-1}Q_{\mathbb{S}}, sQ_{\mathbb{R}})\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}((x-r)Q_{\mathbb{S}}, Q_{\mathbb{R}})\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(xQ_{\mathbb{S}}, Q_{\mathbb{R}})\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}})^{-1}\hat{e}(rQ_{\mathbb{S}}, Q_{\mathbb{R}}))\\
&= \mathcal{H}_2(\hat{e}(xQ_{\mathbb{S}}, Q_{\mathbb{R}})\\
&\neq k_2 \ (\text{since } k_2 = \mathcal{H}_2(\hat{e}(xQ_{\mathbb{S}}, Q_B)))
\end{aligned}$$

(Therefore, k_2^* of σ^* is not equal to k_2 of σ).

From the above computation it is clear that $k_1^* = k_1$ and $c^* = c$(from the definition of σ^*). Hence the check $r^* = r$ holds. Since $k_2 \neq k_2^*$, c^* will get decrypted to some message m^* and not to message m(used for the generation of σ). Now, this clearly shows that the $\mathcal{C}$ will accept σ^* as a valid signcryption of m^* from sender $ID_{\mathbb{S}}$ to receiver $ID_{\mathbb{R}}$. Also, it does not violate the definition of unforgeability game that the forgery generated by $\mathcal{A}(\sigma^*)$ is not the output of signcrypt oracle for message m^* with $ID_{\mathbb{S}}$ as sender and $ID_{\mathbb{R}}$ as receiver. Thus, $\mathcal{A}$ can successfully forge the signcryption on some message m^*(not known to $\mathcal{A}$) without doing any computation or breaking any hard problem assumption.

4 Review and Attack of Signcryption Scheme in [2]

In [2], Bao et al. proposed a PKI based signcryption scheme that provides public verifiability. In this section, we show that the scheme in [2] is not secure against chosen plaintext attack. This is due to the fact that the adversary knows that the message hidden in the signcryption is one among two messages chosen by him during the challenge phase. During the confidentiality game of the scheme in [2], the adversary is capable of verifying the signature component of the signcryption. In this section, we review the scheme in [2] and show that the scheme is not CPA secure.

4.1 Review of Scheme in [2]

Public Parameters(κ) :

- p : a large prime.
- q : a large prime factor of $p-1$.
- g : an element of $\mathbb{Z}_q^*$ of order q.
- $\mathcal{H}$: a one-way hash function.
- $\mathcal{KH}$: a keyed one-way hash function.
- $(\mathcal{E}, \mathcal{D})$: the encryption and decryption algorithms of a symmetric key cipher.

User Key :

- A : Sender.
- B : receiver.
- x_A : private key of sender A.
- x_B : private key of receiver B.
- Y_A : public key of sender A ($Y_A = g^{x_A}$).
- Y_B : public key receiver B. ($Y_B = g^{x_B}$).

Signcrypt(m, Y_A, x_A, Y_B)

- $q \in_R \mathbb{Z}_q^*$.
- $k_1 = \mathcal{H}(Y_B^x \, mod \, p)$.
- $k_2 = \mathcal{H}(g^x \, mod \, p)$.
- $c = \mathcal{E}_{k_1}(m)$.
- $r = \mathcal{KH}_{k_2}(m)$.
- $s = \dfrac{x}{r + x_A}$.
- Output $\sigma = \langle c, r, s \rangle$

Unsigncrypt(σ, Y_A, Y_B, y_B)

- $t_1 = (Y_A g^r)^s$
- $t_2 = t_1^{x_B}$
- $k_2' = \mathcal{H}(t_1 \, mod \, p)$.
- $k_1' = \mathcal{H}(t_2 \, mod \, p)$.
- $m = \mathcal{D}_{k_1'}(m)$.
- Output m iff $r = \mathcal{KH}_{k_2'}(m)$.

4.2 Attack on the Scheme in [2]

Attack on Confidentiality : The scheme in [2] is not CPA secure. For the adversary, who knows that the challenge signcryption corresponds to one of the messages chosen by him during the challenge phase will be able to distinguish the challenge signcryption. The formal attack follows:

- During the confidentiality game, after getting sufficient training in Phase-I, the adversary $\mathcal{A}$ chooses two messages of equal length m_0 and m_1, the sender public key $Y_{\mathbb{S}}$, the receiver public key $Y_{\mathbb{R}}$ and submits them to the challenger $\mathcal{C}$.
- $\mathcal{C}$ generates the signcryption $\sigma^* = \langle c^*, r^*, s^* \rangle$ of the randomly chosen message $m_\delta \in_R \{m_0, m_1\}$ with $\mathbb{S}$ as sender and $\mathbb{R}$ as receiver.
- $\mathcal{C}$ delivers σ^* as challenge to $\mathcal{A}$.
- On receiving σ^* as challenge, $\mathcal{A}$ does the following to distinguish whether σ^* is the signcryption of m_0 or m_1 :
  - Computes $t_1 = (Y_{\mathbb{S}} g^{r^*})^{s^*}$
  - Computes $k_2' = \mathcal{H}(t_1 \, mod \, p)$
  - Checks

$$if\ r^* = \begin{cases} \mathcal{KH}_{k_2'}(m_0) & \text{output } \delta'{=}0 \\ \mathcal{KH}_{k_2'}(m_1) & \text{output } \delta'{=}1 \end{cases}$$

It is to be noted that a similar attack can also be launched against the modified scheme in [2].

5 Review and Attack of Signcryption Scheme in [14]

Tso et al. in [14] proposed a PKI based signcryption scheme that offers forward security and public verifiability. The scheme offers public verifiability, in the sense that, a receiver can prove the authenticity of the signcryption from a sender by providing some additional information other than his private key and the message being signcrypted. They have given formal proofs for confidentiality and unforgeability, and informally argued that their schemes offers the property of forward security even if the additional information required for third party verification and private key of the sender are known to the adversary. We have reviewed the scheme in [14] and showed that the scheme does not provide confidentiality when the private key of sender and the information required for third party verification are known to the adversary.

5.1 Review of the Scheme[14]

Public Parameters(κ) :

- q : a large prime $> 2^{160}$.
- $\mathbb{F}_q$: finite field.
- $\mathbb{E}(\mathbb{F}_q)$: Elliptic curve defined over $\mathbb{F}_q$.
- P : a point on $\mathbb{E}(\mathbb{F}_q)$, $|P| = n$.
- $\mathcal{H}$: a cryptographic one-way hash function.
- $\mathcal{T}$: a secure hash function.
- $bind_{A,B}$: concatenation of identities of A and B.
- $PointComp()$: point compress function.
- $PointDecomp()$: point decompress function.
- $(\mathcal{E}, \mathcal{D})$: the encryption and decryption algorithms of a symmetric key cryptosystem(CPA secure).
- $params = \langle q, P, n, (\mathcal{E}, \mathcal{D}), \mathcal{H}, \mathcal{T} \rangle$

User Key :

- A : Sender.
- B : receiver.
- x_A : private key of sender A.
- x_B : private key of receiver B.
- Y_A : public key of sender A ($Y_A = x_A P$).
- Y_B : public key receiver B. ($Y_B = x_B P$).

Signcrypt(m, Y_A, x_A, Y_B)

- $k \in_R \{1, \ldots, (n-1)\}$.
- $R = kP = (\hat{x}_1, \hat{y}_1)$.
- $(\hat{x}_1, \alpha_1) = PointComp(\mathbb{E}(\mathbb{F}_q), R)$.
- $r = \hat{x}_1 \, mod \, n$. I $r = 0$ goto step 1.
- $K = kY_B = (\hat{x}_2, \hat{y}_2)$.
- $\alpha_2 = \mathcal{H}(\hat{x}_2)$.
- $(\alpha_e, u) = \mathcal{T}(\alpha_2)$, where $u \in \{1, \ldots, (n-1)\}$.
- $U = uR$.
- $\hat{c} = \mathcal{E}_{\alpha_e}(m)$ and $c = \hat{c} \| \alpha_1$.
- $h = \mathcal{H}(c \| bind_{A,B}, \hat{x}_1 \| U)$.
- $v = (ku)^{-1}(h + rx_A) \, mod \, n$.
- Output $\sigma = \langle c, \hat{x}_1, v \rangle$

Unsigncrypt(σ, Y_A, Y_B, x_B)

- $R' = PointDecomp(\mathbb{E}(\mathbb{F}_q), \hat{x}_1, \alpha_1)$.
- $K' = x_B R = (\hat{x}'_2, \hat{y}'_2)$ and $\alpha'_2 = \mathcal{H}(\hat{x}'_2)$.
- $(\alpha'_e, u') = \mathcal{T}(\alpha'_2)$.
- $U' = u'R$ and $h' = \mathcal{H}(c \| bind_{A,B} \| \hat{x}_1 \| U')$.
- $r' = \hat{x}_1 \, mod \, n$.
- $e'_1 = h'/v \, mod \, n$ and $e_1 = e'_1 (u')^{-1}$.
- $e'_2 = r'/v \, mod \, n$ and $e_1 = e'_2 (u')^{-1}$.
- $\tilde{R} = e_1 P + e_2 Y_A = (\hat{x}'_1, \hat{y}'_1)$.
- Accept σ iff $\hat{x}_1 = \hat{x}'_1$, otherwise, output "$Invalid$"
- Output $m' = \mathcal{D}_{\alpha'_e}(\hat{c})$.

Public-Verify(σ, h, Y_A, Y_B)

- $\bar{r} = \hat{x}_1 \, mod \, n$.
- $\bar{e}_1 = h/v \, mod \, n$ and $\bar{e}_2 = \bar{r}/v \, mod \, n$.
- $\bar{U} = \bar{e}_1 P + \bar{e}_2 Y_A$.
- Accept and output "$Valid$ iff $h = \mathcal{H}(c \| bind_{A,B} \| \hat{x}_1 \| \bar{U})$. Otherwise, output "$Invalid$"

5.2 Attack on the Scheme [14]

In [14], Tso et al. have proposed a signcryption scheme with the properties non-repudiation, public verifiability and forward security in addition to the security properties provided by the signcryption primitive. The forward security property of the scheme is not formally proved in [14]. But it was informally argued that the signcryption generated between sender $\mathbb{S}$ with public key $Y_{\mathbb{S}}$ and receiver $\mathbb{R}$ with public key $Y_{\mathbb{R}}$ is confidential even if the private key ($x_{\mathbb{S}}$) of $\mathbb{S}$ is compromised(known to the adversary). This is equivalent to the insider security notion of confidentiality game in signcryption. We show that, the scheme in [14] does not provide confidentiality when sender private key is compromised. This can be clearly shown by :

- Let (m_0, m_1) be the two messages chosen by the adversary $\mathcal{A}$ and, $\mathbb{S}$ be the sender and $\mathbb{R}$ be the receiver chosen by adversary during the challenge phase.
- Let σ^* be the challenge signcryption generated by the challenger $\mathcal{C}$ on message m_δ(where $\delta \in \{0,1\}$) from sender $\mathbb{S}$ to receiver $\mathbb{R}$.
- Now, $\mathcal{A}$ cooks up a signcryption $\tilde{\sigma}$ from σ^* on message m_b(chosen by $\mathcal{C}$ for generation of σ^*) from sender C to receiver $\mathbb{R}$ as follows :
  - Obtain h^* from $\mathcal{C}$ by requesting third party signature verification(as mentioned in their discussion).
  - Computes $(k^*u^*) = ({v^*}^{-1}(r^* + h^* x_{\mathbb{S}}))$.
  - Computes $\tilde{U} = k^*u^*P$.
  - Computes $\tilde{h} = \mathcal{H}(c \| bind_{C,\mathbb{S}} \| \hat{x}_1^* \| \tilde{U})$
  - Computes $\tilde{v} = (k^*u^*)^{-1}(r^* + \tilde{h}x_C)$
  - Sets $\tilde{c} = c^*$ and $\hat{x}_1' = \hat{x}_1^*$
- $\mathcal{A}$ now submits $\tilde{\sigma} = \langle \tilde{c}, \hat{x}_1', \tilde{v} \rangle$ to the unsigncrypt oracle as if $\tilde{\sigma}$ is a signcryption from sender C to receiver $\mathbb{R}$ during Phase-II. It should be noted that unsigncryption of $\tilde{\sigma}$ will output the message m_δ(used for generation of σ^*) and it will pass the signature verification. The correctness of the signcryption $\tilde{\sigma}$ can be shown as follows :

6 Identity Based Signcryption Scheme With Public Verifiability(IDPVS)

In this section, we propose a new identity based signcryption that offers public verifiability, third party verification(proving the binding of message to the signcryption with the help of additional information provided by the receiver) and forward security. We have formally proved the security of our scheme in the newly proposed security model. Our security model captures insider notion of security of signcryption schemes.
Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two cyclic groups of prime order q and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map. Let $\mathcal{M}$ be the message space and $\Im$ be the ciphertext space and $\mathcal{H}_i$ (i=1 to 4) be four cryptographic hash functions.

6.1 IDPVS Scheme

Setup(1^κ) **:**

- $P \in_R \mathbb{G}_1$
- $s \in_R \mathbb{Z}_q^*$
- $P_{Pub} = sP$
- $Params = \langle \mathbb{G}_1, \mathbb{G}_2, q, n, P, P_{Pub}, \hat{e}(.,.),$
- $(\mathcal{E}, \mathcal{D}) \rangle$ be the CPA secure symmetric key cipher.
- $\mathcal{H}_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$.
- $\mathcal{H}_2 : \mathbb{G}_2 \rightarrow \{0,1\}^{|\Im|}$.
- $\mathcal{H}_3 : \{0,1\}^{|\Im|} \times \mathbb{G}_1^3 \rightarrow \mathbb{G}_1$.
- $\mathcal{H}_4 : \{0,1\}^{|\mathcal{M}|} \times \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_1^2 \rightarrow \{0,1\}^{\hat{n}}$

Extract(ID_A)

- $Q_A = \mathcal{H}_1(ID_A)$
- $D_A = sQ_A$

Signcrypt(m, ID_A, D_A, ID_B)

- $x \in_R \mathbb{Z}_q^*$
- $U = xP$
- $\hat{\alpha} = \hat{e}(P_{Pub}, Q_B)^x$
- $\alpha_2 = \mathcal{H}_2(\hat{\alpha})$
- $r = \mathcal{H}_4(m, \hat{\alpha}, U, Q_A, Q_B)$
- $c = \mathcal{E}_{\alpha_2}(m \| r)$
- $R = \mathcal{H}_3(c, U, Q_A, Q_B)$
- $V = xR + D_A$
- Signcryption $\sigma = \langle U, V, c \rangle$

Unsigncrypt$(\sigma, ID_A, ID_B, D_B)$

- If Public-Verify$(\sigma, ID_A, ID_B) \neq$ "$Valid$", output "$Invalid$"
- $\hat{\alpha}' = \hat{e}(U, D_B)$
- $\alpha_2' = \mathcal{H}_2(\hat{\alpha}')$
- $m' \| r' = \mathcal{D}_{\alpha_2'}(c)$
- Output $\phi = \langle m', r', \hat{\alpha}', \sigma \rangle$ iff $r' = \mathcal{H}_4(m', \hat{\alpha}', U, Q_A, Q_B)$ else, return "$Invalid$"

Public-Verify(σ, ID_A, ID_B)

- $\bar{R} = \mathcal{H}_4(c, U, Q_A, Q_B)$
- If $\hat{e}(V, P) = \hat{e}(U, \bar{R})\,\hat{e}(Q_A, P_{Pub})$, then return "$Valid$". Otherwise, return "$Invalid$"

TP-Verify(ϕ, ID_A, ID_B)

- If Public-Verify$(\sigma, ID_A, ID_B) \neq$ "$Valid$", output "$Invalid$"
- $\bar{\alpha_2} = \mathcal{H}_2(\hat{\alpha}')$
- $\bar{m} \| \bar{r} = \mathcal{D}_{\bar{\alpha_2}}(c)$
- Accept σ and output "$Valid$" iff $\bar{r} = \mathcal{H}_4(\bar{m}, \hat{\alpha}', U, Q_A, Q_B)$ and $\bar{r} = r'$. Otherwise, output "$Invalid$"

Proof of Correctness of IDPVS : The correctness of signature verification and the consistency of signcrypt and unsigncrypt algorithm are shown below:

Correctness of signature verification :

$$\begin{aligned} \text{LHS} = \hat{e}(V, P) &= \hat{e}(xR + D_A, P) \\ &= \hat{e}(xR, P)\hat{e}(D_A, P) \\ &= \hat{e}(R, P)^x \hat{e}(sQ_A, P) \\ &= \alpha_1 \hat{e}(Q_A, P_{Pub}) \\ &= \text{RHS} \end{aligned}$$

Correctness of $\hat{\alpha}'$:

$$\begin{aligned} \hat{\alpha}' &= \hat{e}(U, D_B) = \hat{e}(xP, sQ_B) \\ &= \hat{e}(P_{Pub}, Q_B)^x = \hat{\alpha} \end{aligned}$$

(Therefore, $\hat{\alpha}'$ of $Unsigncrypt$ is same as $\hat{\alpha}$ of $Signcrypt$).

6.2 Security Analysis of IDPVS

Proof for Unforgeability of IDPVS Scheme

Theorem 1. *If there exists an adversary $\mathcal{A}$ who can break the EUF-CMA$_{IDPVS}$ security of IDPVS scheme with advantage ϵ then there exists another algorithm which can break the $CDHP$ with advantage $\epsilon' \geq \epsilon$.*

Proof for Confidentiality of IDPVS Scheme

Theorem 2. *If there exists an adversary $\mathcal{A}$ who can break the IND-IBSC-CCA2 security of IDPVS scheme with advantage ϵ then there exists another algorithm which can break the $CDHP$ with advantage $\epsilon' \geq \epsilon$.*

Note: Security proofs will be available soon.

7 Conclusion

In this paper, we have shown the security weaknesses in three existing public verifiable signcryption schemes that appear in [2], [14] and [4]. The schemes in [2] and [14] are in the Public Key Infrastructure (PKI) setting and the scheme in [4] is an identity based scheme. More specifically, [14] is based on elliptic curve digital signature algorithm (ECDSA). We have also provided a new identity based signcryption scheme that provides public verifiability and third party verification. We have formally proved the security of the newly proposed scheme in the random oracle model.

References

1. Joonsang Baek, Ron Steinfeld, and Yuliang Zheng. Formal proofs for the security of signcryption. In *Public Key Cryptography - PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 80–98. Springer, 2002.
2. Feng Bao and Robert H. Deng. A signcryption scheme with signature directly verifiable by public key. In *Public Key Cryptography*, volume 1431 of *Lecture Notes in Computer Science*, pages 55–59. Springer, 1998.
3. Xavier Boyen. Multipurpose identity-based signcryption (a swiss army knife for identity-based cryptography). In *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2003.
4. Sherman S. M. Chow, Siu-Ming Yiu, Lucas Chi Kwong Hui, and K. P. Chow. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In *ICISC*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2004.
5. Chandana Gamage, Jussipekka Leiwo, and Yuliang Zheng. Encrypted message authentication by firewalls. In *Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, March 1-3, 1999, Proceedings*, volume 1560 of *Lecture Notes in Computer Science*, pages 69–81. Springer, 1999.
6. Benoît Libert and Jean-Jacques Quisquater. Efficient signcryption with key privacy from gap diffie-hellman groups. In *Public Key Cryptography - PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 187–200. Springer, 2004.
7. Benot Libert and Jean-Jacques Quisquater. A new identity based signcryption scheme from pairings. In *In IEEE Information Theory Workshop*, pages 155–158, 2003.
8. John Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002.

9. Yi Mu and Vijay Varadharajan. Distributed signcryption. In *Progress in Cryptology - INDOCRYPT 2000*, volume 1977 of *Lecture Notes in Computer Science*, pages 155–164. Springer, 2000.
10. Josef Pieprzyk and David Pointcheval. Parallel authentication and public-key encryption. In *Information Security and Privacy, 8th Australasian Conference, ACISP 2003*, volume 2727 of *Lecture Notes in Computer Science*, pages 387–401. Springer, 2003.
11. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, CRYPTO - 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.
12. Jun-Bum Shin, Kwangsu Lee, and Kyungah Shim. New dsa-verifiable signcryption schemes. In *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 35–47. Springer, 2003.
13. Ron Steinfeld and Yuliang Zheng. A signcryption scheme based on integer factorization. In *Information Security, Third International Workshop, ISW 2000*, volume 1975 of *Lecture Notes in Computer Science*, pages 308–322. Springer, 2000.
14. Raylin Tso, Takeshi Okamoto, and Eiji Okamoto. Ecdsa-verifiable signcryption scheme with signature verification on the signcrypted message. In *Information Security and Cryptology(Inscrypt 07)*, volume 4990 of *Lecture Notes in Computer Science*, pages 11–24. Springer, 2008.
15. Guomin Yang, Duncan S. Wong, and Xiaotie Deng. Analysis and improvement of a signcryption scheme with key privacy. In *Information Security, 8th International Conference, ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 2005.
16. Dae Hyun Yum and Pil Joong Lee. New signcryption schemes based on kcdsa. In *Information Security and Cryptology - ICISC 2001, 4th International Conference Seoul, Korea, December 6-7, 2001, Proceedings*, volume 2288 of *Lecture Notes in Computer Science*, pages 305–317. Springer, 2002.
17. Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) $< <$ cost(signature) + cost(encryption). In *Advances in Cryptology, CRYPTO - 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.