Signcryption from Randomness Recoverable PKE Revisited

Angsuman Das[1] and Avishek Adhikari[2]

[1] Department of Mathematics,
St. Xavier's College, Kolkata, India
angsumandas054@gmail.com

[2] Department of Pure Mathematics,
University of Calcutta, Kolkata, India
avishek.adh@gmail.com

Abstract. A new generic construction of a signcryption scheme from randomness recoverable public key encryption (PKE-RR) is proposed. This paper modifies the 'Li & Wong' construction [Information Sciences 180 (2010)] to achieve better security from weaker building blocks and thereby making it open to a larger class of encryption and signature schemes. The proposed construction achieves multi-user insider security for confidentiality in random oracle model and authenticity in standard model. It is done by incorporating one extra hashing in both signcryption and unsigncryption phases than the original construction.

Keywords: Randomness Recoverable PKE, Signcryption, Sign-then-encrypt paradigm.

1 Introduction

Signcryption is a public-key primitive which addresses both the problem of privacy and authenticity within the same protocol such that it is better in terms of ciphertext expansion, computational cost and efficiency when compared to naive combination of public-key encryption and digital signature. From the day of its introduction by Zheng [15], it has been an area of active research and as a result, a lot of techniques and security models like [1], [2], [10] etc. have evolved till date. Targeting the same goal, Li & Wong [9] proposed a generic construction of a signcryption scheme from randomness recoverable public key encryption (PKE-RR).

Informally speaking, a Randomness Recoverable Public Key Encryption (PKE-RR) is a special type of probabilistic encryption scheme where not only the plaintext but also the randomness used in the encryption algorithm can be extracted from the ciphertext with the help of the private key.[1] The idea of using PKE-RR in constructing signcryption was first noticed in [9], where the authors used

[1] It is to be noted here that there exist probabilistic PKE's like [6],[12] where the ephemeral key is lost i.e., there is no obvious way to recover it even with the help of private key.

A. Bagchi and I. Ray (Eds.): ICISS 2013, LNCS 8303, pp. 78–90, 2013.

an Ω-IND-CCA2 secure PKE-RR and an UF-CMA secure uniformly-distributed signature scheme as components. But, not only there exist a few known practical constructions of Ω-uniform IND-CCA2 secure PKE-RR but also the notion of Ω-uniform IND-CCA2 security[2] is somewhat artificial. In our construction, we use a weaker encryption primitive i.e., an IND-CCA2 PKE-RR (not necessarily Ω-uniform IND-CCA2 secure as used in [9]) and an UF-CMA secure signature scheme (not necessarily uniformly-distributed as used in [9]), making it open to a larger class of encryption and signature schemes. It is also shown that this transformation is better than [9], in the sense that it offers an enhanced level of security both in terms of confidentiality and unforgeability with weaker building blocks.

1.1 Organisation of the Paper

The paper is organised as follows: In Section 2, some definitions and preliminaries are discussed. The construction by Li & Wong is briefly recalled in Section 3, whereas the proposed construction is given in Section 4.2 and its security analysis is done in Section 4.3. The comparison with existing Li & Wong conversion [9] is discussed in Section 5 and finally we conclude with some open problems in Section 6.

2 Definitions and Preliminaries

We begin by formally defining the notions of *Randomness Recoverable Public-Key Encryption* (PKE-RR) and Signcryption scheme *SC* and then briefly recalling the security notions in the context of signcryption schemes.

2.1 Randomness-Extractable Public-Key Encryption (PKE-RR)

A Randomness Recoverable Public Key Encryption (Π) (PKE-RR) [9] is a tuple of probabilistic polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ such that:

1. The key generation algorithm, Gen, takes as input a security parameter 1^n and outputs a public-key/ private-key pair (pk, sk).
2. The encryption algorithm Enc takes as input a message m from the underlying plaintext space and a random key r from the randomness space to output a ciphertext $c := \mathsf{Enc}_{pk}(m, r)$.
3. The decryption algorithm Dec takes as input a ciphertext c to output $\mathsf{Dec}_{sk}(c)$ $= (m, r)$.

It is required that for every n, every (pk, sk) and every message m in the corresponding plaintext space, it holds that

$$\mathsf{Dec}(\mathsf{Enc}(m, r)) = (m, r).$$

[2] For the definition of Ω-uniform IND-CCA2 security, see [9].

Remark 1. If we supress the decryption algorithm Dec to return only the plaintext m in the PKE-RR, we get a usual public-key scheme.

Remark 2. Paillier encryption scheme [13] and its variants like [5], OAEP [3] and its variants like OAEP+, certain lattice-based (like [8]) and code-based (variants of [11]) cryptosystems are some of the existing examples of PKE-RR.

Remark 3. Recently, in [4], an idea similar to that of PKE-RR was used while defining a new notion of security called Enhanced Chosen Ciphertext security. Our definition of PKE-RR matches with their definition of uniquely randomness recovering encryption.

Security Notions for Public-Key Encryption Scheme. Though there are various notions of security for public-key encryption schemes, but here only the relevant (CPA and CCA2) ones are discussed.

Chosen Plaintext Attack: Chosen plaintext attack to a cryptosystem is defined as a game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ in a public-key encryption scheme PKE as follows:

1. Given the security parameter, $\mathcal{C}$ generates a pair (pk, sk).
2. $\mathcal{A}$ is given the public-key pk. $\mathcal{A}$ outputs a pair of messages (m_0, m_1) from the plaintext space associated with pk.
3. $\mathcal{C}$ chooses $b \in_R \{0,1\}$ and sends the ciphertext $c^* = \mathsf{Enc}_{pk}(m_b)$ to $\mathcal{A}$;
4. $\mathcal{A}$ outputs a bit b'.

The advantage $\mathbf{Adv}^{cpa}_{\mathcal{A},PKE}(n)$ is defined to be $|Pr[b' = b] - 1/2|$. The scheme PKE is said to be secure against chosen plaintext attack if for all probabilistic polynomial-time adversaries $\mathcal{A}$, the advantage $\mathbf{Adv}^{cpa}_{\mathcal{A},PKE}(\cdot)$ is negligible.

Chosen Ciphertext Attack: Adaptive chosen ciphertext attack [14] to a cryptosystem is defined as a game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ in a public-key encryption scheme PKE as follows:

1. Given the security parameter, $\mathcal{C}$ generates a pair (pk, sk).
2. $\mathcal{A}$ is given the public-key pk as well as oracle access to the decryption algorithm, $\mathsf{Dec}_{sk}(\cdot)$. $\mathcal{A}$ outputs a pair of messages (m_0, m_1) from the plaintext space associated with pk.
3. $\mathcal{C}$ chooses $b \in_R \{0,1\}$ and sends the ciphertext $c^* = \mathsf{Enc}_{pk}(m_b)$ to $\mathcal{A}$;
4. $\mathcal{A}$ continues to have oracle access to $\mathsf{Dec}_{sk}(\cdot)$ as in step 2, but with the restriction that it can not query c^*;
5. $\mathcal{A}$ outputs b'.

The advantage $\mathbf{Adv}^{cca2}_{\mathcal{A},PKE}(n)$ is defined to be $|Pr[b' = b] - 1/2|$. The scheme PKE is said to be secure against adaptive chosen ciphertext attack if for all probabilistic polynomial-time adversaries $\mathcal{A}$, the advantage $\mathbf{Adv}^{cca2}_{\mathcal{A},PKE}(\cdot)$ is negligible.

Remark 4. In case of a PKE-RR, the decryption oracle in the CCA2 game returns both the message and the randomness used in the encryption process.

2.2 Signature Scheme (SS)

A Signature Scheme (SS) is a tuple of probabilistic polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ such that:

1. The key generation algorithm, Gen, takes as input the security parameter 1^n and outputs a signing-key/ verification-key pair (pk_A, sk_A).
2. The signing algorithm Sign takes as input signer's secret key sk_A and a message m from the underlying plaintext space to output a signature
$$\sigma := \mathsf{Sign}(sk_A, m).$$
3. The verification algorithm Verify takes as input signer's verification key pk_A and a message-signature pair (m, σ) to output $\mathsf{Verify}(pk_A, m, \sigma) = 0$ or 1.

It is required that for every n, every (pk_A, sk_A) and every message m in the corresponding plaintext space, it holds that

$$\mathsf{Verify}(pk_A, m, \mathsf{Sign}(sk_A, m)) = 1.$$

Security Notions for Signature Scheme (SS). A Signature Scheme (SS) is said to existentially unforgeability against chosen message attack (UF-CMA) if any probabilistic polynomial-time adversary $\mathcal{A}$ has negligible chance of winning against a challenger $\mathcal{C}$ in the following game:

1. Given the security parameter, $\mathcal{C}$ generates a signer key-pair (pk_A, sk_A) using Gen.
2. $\mathcal{A}$ is given pk_A as well as oracle access to the signer's signing algorithm, $\mathsf{Sign}(sk_A, \cdot)$.
3. $\mathcal{A}$ outputs a message-signature pair (m^*, σ^*).

$\mathcal{A}$ wins the game if σ^* is a valid signature on m^* and if m^* was never submitted to the signing oracle $\mathsf{Sign}(sk_A, \cdot)$.

2.3 Signcryption Scheme (SC)

A Signcryption Scheme (SC) is a tuple of probabilistic polynomial-time algorithms $(\mathsf{Setup}, \mathsf{KeyGen_A}, \mathsf{KeyGen_B}, \mathsf{Signcrypt}, \mathsf{Unsigncrypt})$ such that:

1. The setup algorithm Setup, takes as input a security parameter 1^n and returns common parameters *par* required by the signcryption scheme.
2. The key generation algorithm for the sender A, $\mathsf{KeyGen_A}$, takes as input the common parameters *par* and outputs a public-key/ private-key pair (pk_A, sk_A).
3. The key generation algorithm for the receiver B, $\mathsf{KeyGen_B}$, takes as input the common parameters *par* and outputs a public-key/ private-key pair (pk_B, sk_B).

4. The signcryption algorithm $\mathsf{Signcrypt}$ takes as input common parameters *par*, sender's secret key sk_A, receiver's public key pk_B, a message m from the underlying plaintext space to output a signcryptext
$$c := \mathsf{Signcrypt}(par, sk_A, pk_B, m).$$
5. The unsigncryption algorithm $\mathsf{Unsigncrypt}$ takes as input common parameters *par*, receiver's secret key sk_B, sender's public key pk_A, a signcryptext c to output a message $m := \mathsf{Unsigncrypt}(par, sk_B, pk_A, c)$ or an error symbol $\perp$.

It is required that there exists a negligible function negl such that for every n, every (pk_A, sk_A), (pk_B, sk_B) and every message m in the corresponding plaintext space, it holds that

$$\mathsf{Pr}[\mathsf{Unsigncrypt}(sk_B, pk_A, (\mathsf{Signcrypt}(sk_A, pk_B, m)) \neq m] \leq \mathsf{negl}(n).$$

Security Notions for Signcryption Scheme (SC). We recall the insider security notions for signcryption schemes in multi-user setting. By multi-user setting, we mean the strongest notion of dynamic multi-user model (*d*-MU)[10] (and not the fixed multi-user model), where the adversary can freely choose all user keys, except the challenge receiver key in the confidentiality game and choose all user keys, except the challenge sender key in the unforgeability game.

Confidentiality: A Signcryption Scheme (SC) is said to achieve multi-user insider confidentiality in *d*-MU-IND-SC-*i*CCA2 sense if any probabilistic polynomial-time adversary $\mathcal{A}$ has negligible advantage against a challenger $\mathcal{C}$ in the following game:

1. Given the security parameter, $\mathcal{C}$ generates common parameters *par* and a receiver key-pair (pk_B, sk_B) using $\mathsf{KeyGen}_\mathsf{B}$.
2. $\mathcal{A}$ is given par, pk_B as well as oracle access to B's (flexible) unsigncryption algorithm, $\mathsf{Unsigncrypt}(\cdot, sk_B, \cdot)$. Each unsigncryption query consists of a pair $(pk_{A'}, c)$ where $pk_{A'}$ is a sender's public-key. Unsigncryption oracle answers it with $\mathsf{Unsigncrypt}(pk_{A'}, sk_B, c)$.
3. $\mathcal{A}$ outputs a sender key pair (pk_A, sk_A) and a pair of messages (m_0, m_1) from the associated plaintext space.
4. $\mathcal{C}$ chooses $b \in_R \{0, 1\}$ and sends the challenge signcryptext $c^* = \mathsf{Signcrypt}(sk_A, pk_B, m_b)$ to $\mathcal{A}$;
5. $\mathcal{A}$ continues to have oracle access to $\mathsf{Unsigncrypt}(\cdot, sk_B, \cdot)$ but with the restriction that it can not query (pk_A, c^*); Note that $\mathcal{A}$ can query $(pk_{A'}, c^*)$ with $pk_{A'} \neq pk_A$ and (pk_A, c) with $c \neq c^*$.
6. $\mathcal{A}$ outputs a bit b'.

The advantage $\mathbf{Adv}^{cca2}_{\mathcal{A},SC}(n)$ is defined to be $|Pr[b' = b] - 1/2|$.

Unforgeability: A Signcryption Scheme (SC) is said to achieve multi-user insider existential signcryptext unforgeability against chosen message attack in

d-MU-UF-SC-iCMA sense if any probabilistic polynomial-time adversary $\mathcal{A}$ has negligible chance of winning against a challenger $\mathcal{C}$ in the following game:

1. Given the security parameter, $\mathcal{C}$ generates common parameters par and a sender key-pair (pk_A, sk_A) using $\mathsf{KeyGen_A}$.
2. $\mathcal{A}$ is given par, pk_A as well as oracle access to A's (flexible) signcryption algorithm, $\mathsf{Signcrypt}(sk_A, \cdot, \cdot)$. Each signcryption query consists of a pair $(pk_{B'}, m)$ where $pk_{B'}$ is a receiver's public-key. Signcryption oracle answers it with $\mathsf{Signcrypt}(sk_A, pk_{B'}, m)$.
3. $\mathcal{A}$ outputs a receiver key pair (pk_B, sk_B) and a signcryptext c^*.

$\mathcal{A}$ wins the game if c^* is a valid signcryptext from A to B and if its underlying plaintext m^* of c^* was never submitted to the signcryption oracle $\mathsf{Signcrypt}(sk_A, pk_B, \cdot)$.

3 Li and Wong Construction

Li & Wong in [9] gave the first construction of signcryption scheme using a randomness recoverable public key encryption (PKE-RR) scheme. Their construction $\mathcal{SC}'$=(Setup', $\mathsf{KeyGen_A}'$, $\mathsf{KeyGen_B}'$, $\mathsf{Signcrypt}'$, $\mathsf{Unsigncrypt}'$) from a PKE-RR scheme Π'=(Gen, Enc, Dec) and a signature scheme $\mathcal{S}'$=(Gen', Sign, Verify) was as follows:

1. Setup:
   (a) $\mathsf{Setup}(1^n) \rightarrow par$. ($par$ denotes the common parameters required by the signcryption scheme.)
   (b) Publish par globally.
2. $\mathsf{KeyGen_A}$:
   (a) $\mathsf{Gen}'(par) \rightarrow (pk_A, sk_A)$
   (b) A publishes pk_A and keeps sk_A as his signing key.
3. $\mathsf{KeyGen_B}$:
   (a) $\mathsf{Gen}(par) \rightarrow (pk_B, sk_B)$
   (b) B publishes pk_B and keeps sk_B as his decryption key.
4. $\mathsf{Signcrypt}$: For a given message m to be sent by A to B,
   (a) $\sigma = \mathsf{Sign}_{sk_A}(m)$.
   (b) $\mathsf{Signcrypt}(m) := c = \mathsf{Enc}(m, \sigma)$.
5. $\mathsf{Unsigncrypt}$: For a given signcryptext c,
   (a) $(m', \sigma') := \mathsf{Dec}(c)$.
   (b) If $\mathsf{Verify}(m', \sigma') = 1$, then return m', else output $\perp$.

In [9], authors proved the following theorem:

Theorem 1. *The signcryption scheme $\mathcal{SC}'$ is*

1. *two user outsider SC-IND-CCA secure if Π' is Ω-uniform CCA2 secure and $\mathcal{S}'$ is uniformly-distributed.*
2. *two user outsider SC-UF-CCA secure if $\mathcal{S}'$ is UF-CMA secure.*

We now discuss the proposed construction which uses an weaker encryption primitive i.e., an IND-CCA2 PKE-RR and an UF-CMA secure signature scheme to achieve the same goal. It also turns out that this transformation is better than [9], in the sense that it achieves better security both in terms of confidentiality and unforgeability starting from weaker cryptographic primitives as building blocks.

4 Idea Behind the Construction

The basic idea behind the proposed construction is Fujisaki-Okamoto transformation [7] on PKE-RR. To be more specific, we discuss the utility of applying Fujisaki-Okamoto transformation [7] on an IND-CPA secure PKE-RR to achieve chosen ciphertext security with better efficiency and then translate the same to construct a secure signcryption scheme from an IND-CCA2 secure PKE-RR.

4.1 Fujisaki-Okamoto Transform on PKE-RR

In this section, as the first step, we propose a generic conversion of an IND-CPA secure PKE-RR into an IND-CCA2 secure PKE-RR. The computational overhead due to the conversion is only one hashing in both the encryption and decryption stages.

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure PKE-RR. We construct an IND-CCA2 secure PKE-RR $\overline{\Pi} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ using Π as follows:

1. Key Generation ($\overline{\mathsf{Gen}}$):
   (a) $\mathsf{Gen}(1^n) \rightarrow (pk, sk)$.
   (b) Choose a hash funstion $H : \{0,1\}^k \rightarrow \{0,1\}^l$.
2. Encryption ($\overline{\mathsf{Enc}}$): For a message $m \in \{0,1\}^{k-t}$ and public key pk,
   (a) Choose $r \in_R \{0,1\}^t$ and set $M = m||r$.
   (b) $c = \overline{\mathsf{Enc}}_{pk}(m) = \mathsf{Enc}_{pk}(M, H(m||r))$.
3. Decryption ($\overline{\mathsf{Dec}}$): For a ciphertext c and secret key sk,
   (a) $(M, \overline{r}) := \mathsf{Dec}_{sk}(c)$ and parse $M = m||r$.
   (b) If $\overline{r} = H(M)$, return (m, r), else return $\perp$.

Remark 5. Though this is exactly the transformation used in [7], but, in the decryption phase, re-encryption is not required to check the validity in comparison to that in [7]. It is sufficient here to check the hashed value only.

We do not give a proof of IND-CCA2 security of this Fujisaki-Okamoto variant, as it is just an application of the F-O transform in [7]. In the next section, for our main construction, we will be using this technique to improve the Li & Wong [9] construction.

4.2 The Proposed Generic Construction

In this section, we construct a signcryption scheme $\mathcal{SC}$=(Setup, $\mathsf{KeyGen_A}$, $\mathsf{KeyGen_B}$, $\mathsf{Signcrypt}$, $\mathsf{Unsigncrypt}$) from an IND-CCA2 secure PKE-RR scheme Π=(Gen, Enc, Dec), an UF-CMA secure signature scheme $\mathcal{S}$=(Gen', Sign, Verify) and a hash function $H : \{0,1\}^{k+k'} \to \{0,1\}^l$, where k denotes the bit-length of plaintext in Π, k' denotes the bit-length of IDs and l denote the bit-length of signatures in $\mathcal{S}$, as follows:

1. Setup:
   (a) $\mathsf{Setup}(1^n) \to par$. ($par$ denotes the common parameters required by the signcryption scheme.)
   (b) Choose a hash function $H : \{0,1\}^{k+k'} \to \{0,1\}^l$.
   (c) Publish par, H globally.
2. $\mathsf{KeyGen_A}$:
   (a) $\mathsf{Gen}'(par) \to (pk_A, sk_A)$
   (b) A publishes pk_A and keeps sk_A as his signing key.
3. $\mathsf{KeyGen_B}$:
   (a) $\mathsf{Gen}(par) \to (pk_B, sk_B)$
   (b) B publishes pk_B and keeps sk_B as his decryption key.
4. $\mathsf{Signcrypt}$: For a given message $m \in \{0,1\}^{k-t}$ to be send by A to B,
   (a) $\sigma = \mathsf{Sign}_{sk_A}(m||ID_B)$.
   (b) Choose $r \in_R \{0,1\}^t$.
   (c) $c := \mathsf{Enc}_{pk_B}(m||r, \sigma \oplus H(m||r||ID_A))$.
   (d) $\mathsf{Signcrypt}(par, sk_A, pk_B, m) := (c||ID_A||ID_B)$
5. $\mathsf{Unsigncrypt}$: For a given signcryptext $(c||ID_A||ID_B)$,
   (a) $(m'||r', \tau) := \mathsf{Dec}(c)$.
   (b) Compute $\sigma' = \tau \oplus H(m'||r'||ID_A)$.
   (c) If $\mathsf{Verify}(m'||ID_B, \sigma') = 1$, then return m', else output $\perp$.

4.3 Security Analysis of Signcryption Scheme $\mathcal{SC}$

We analyze the security of the proposed construction $\mathcal{SC}$ in the following way:

1. dynamic multi-user insider confidentiality in d-MU-IND-SC-iCCA2 sense in random oracle model;
2. dynamic multi-user insider existential signcryptext unforgeability in d-MU-UF-SC-iCMA sense in standard model;

Theorem 2. *$\mathcal{SC}$ is d-MU-IND-SC-iCCA2 secure in the sense of multi-user insider confidentiality in random oracle model if Π is IND-CCA2 secure.*

Proof. Let $\mathcal{A}_{\mathcal{SC}}$ be a d-MU-IND-SC-iCCA2 adversary against $\mathcal{SC}$. We construct an IND-CCA2 adversary $\mathcal{A}_{\Pi}$ against Π which uses $\mathcal{A}_{\mathcal{SC}}$ as a sub-routine. As an input, $\mathcal{A}_{\Pi}$ is fed with pk_B of Π and given the decryption oracle $\mathcal{O}\mathsf{Dec}$ of Π. $\mathcal{A}_{\Pi}$ simulates $\mathcal{A}_{\mathcal{SC}}$ with pk_B. Moreover, the oracle access to H-values and unsigncryption algorithm $\mathcal{SC}$ needed by the adversary $\mathcal{A}_{\mathcal{SC}}$ will be provided by $\mathcal{A}_{\Pi}$.

Simulation of H-Oracle: When $\mathcal{A}_{\mathcal{SC}}$ submits an H-query $(m_i||r_i||ID_{A_i})$, $\mathcal{A}_{\Pi}$ chooses a random $\alpha_i \in \{0,1\}^l$ and returns α_i to $\mathcal{A}_{\mathcal{SC}}$. Also, for each returned value, $\mathcal{A}_{\Pi}$ maintains a list called H-list containing $(m_i||r_i||ID_{A_i}, \alpha_i)$

Simulation of Unsigncryption Oracle ($\mathcal{O}\mathsf{Unsigncrypt}$): In unsigncryption queries, when a query $(c'||ID_{A'}||ID_B, pk_{A'})$ is asked, $\mathcal{A}_{\Pi}$ queries $\mathcal{O}\mathsf{Dec}$ with c' to get (M', β') and parses M' as $m'||r'$. $\mathcal{A}_{\Pi}$ then checks H-list whether $m'||r'||ID_{A'}$ has been previously queried or not. If it has not been queried, $\mathcal{O}\mathsf{Unsigncrypt}$ outputs $\perp$ i.e., "invalid". Whereas if $(m'||r'||ID_{A'}, \alpha')$ appears in the H-list, $\mathcal{A}_{\Pi}$ finds $\sigma' = \beta' \oplus \alpha'$ and checks whether $(m'||ID_B, \sigma')$ is a valid message-signature pair or not, using $pk_{A'}$. If it is a valid pair, $\mathcal{O}\mathsf{Unsigncrypt}$ outputs m', else outputs $\perp$.

One thing should be noted here that $\mathcal{A}_{\Pi}$ should be consistent in declaring a signcryptext to be "invalid": *Suppose, $\mathcal{A}_{\Pi}$ has declared a signcryptext c' to be "invalid" as the corresponding $m'||r'||ID_{A'}$ has not been H-queried till then. Let us look into $\mathcal{A}_{\Pi}$'s view towards c': $\mathcal{A}_{\Pi}$ queries $\mathcal{O}\mathsf{Dec}$ with c' to get $(m'||r', \beta')$, where β' is of the form $\sigma' \oplus \hat{\alpha}$, σ' being a signature on $m'||ID_B$ and $\hat{\alpha}$ is a random string chosen by $\mathcal{A}_{\mathcal{SC}}$. Though $\mathcal{A}_{\mathcal{SC}}$ knows both σ' and $\hat{\alpha}$, none of them are known to $\mathcal{A}_{\Pi}$. (As, in most of the cases, $\mathcal{S}$ is a probabilistic signature scheme, m' can have many valid signatures.) Now suppose $\mathcal{A}_{\mathcal{SC}}$ submits an H-query for that same $m'||r'||ID_{A'}$ in a later stage to receive α' as response and submits $\hat{c} = \mathsf{Enc}(pk_B, m'||r', \sigma'' \oplus \alpha')$ as an unsigncryption query. Observe that $\hat{c}$ is a valid-signcryptext for m' according to $\mathcal{B}$ where σ'' is another signature on $m'||ID_B$, other than σ'. So, the simulated unsigncryption oracle will return m'. This will lead to an inconsistency, in part of $\mathcal{A}_{\Pi}$ if $\alpha' = \hat{\alpha}$ and it will occur only when $\mathcal{A}_{\Pi}$'s response α' matches with the random string $\hat{\alpha}$ chosen by $\mathcal{A}$ while generating c'. (As $\mathcal{A}_{\Pi}$ does not know $\hat{\alpha}$, he can not choose α' to be different from $\hat{\alpha}$ while responding to the H-query.)* So, the probability of one such inconsistency of unsigncryption oracle of $\mathcal{A}_{\Pi}$ is $1/2^l$.

This provides an almost perfect simulation since the probability of producing a valid signcryptext without previously making the corresponding H-query is $1/2^l$, which is negligible. If q_U is the total number of unsigncryption queries, then $\mathcal{A}_{\Pi}$ will be consistent in responding to the unsigncryption queries with probability $\geq (1 - 1/2^l)^{q_U}$.

Once the first query phase is over, $\mathcal{A}_{\mathcal{SC}}$ returns two plaintexts $m_0, m_1 \in \{0,1\}^{k-t}$ and an attacked sender key-pair (pk_A, sk_A) to $\mathcal{A}_{\Pi}$. $\mathcal{A}_{\Pi}$ randomly chooses $r_0, r_1 \in_R \{0,1\}^t$ and submits $m_0||r_0, m_1|||r_1$ to the IND-CCA2 challenger $\mathcal{C}$ of Π. $\mathcal{C}$ randomly chooses a bit $b \in \{0,1\}$, $r \in_R \{0,1\}^l$. $\mathcal{C}$ returns $\mathcal{A}_{\Pi}$ the challenge ciphertext $c^* = \mathsf{Enc}(pk_B, m_b||r_b, r)$ and $\mathcal{A}_{\Pi}$ passes c^* to $\mathcal{A}_{\mathcal{SC}}$ as the challenge signcryptext.

In the second query phase, $\mathcal{A}_{\mathcal{SC}}$ is allowed to make any H-query and any unsigncryption query other than the challenge signcryptext c^*. If $\mathcal{A}_{\mathcal{SC}}$ makes an H-query with $m_b||r_b||ID_A$ with $b \in \{0,1\}$, $\mathcal{A}_{\Pi}$ returns b to $\mathcal{C}$ and stops the game. If $m_b||r_b||ID_A$ is not queried, then $\mathcal{A}_{\Pi}$ outputs b' (the output of $\mathcal{A}_{\mathcal{SC}}$) after the second query phase is over.

The theorem now follows immediately from the following lemma.

Lemma 1. *If ϵ be the probability that given a valid signcryptext, $\mathcal{A}_{\mathcal{SC}}$ can correctly guess the bit b, then $\mathcal{A}_{\Pi}$ can win the IND-CCA2 game with a probability greater or equal to*

$$\epsilon - \left(\frac{q_H}{2^t} + \frac{q_U}{2^l}\right)$$

Proof. Let $\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}$ denote the probability of $\mathcal{A}_{\mathcal{SC}}$ returning the correct bit b and $\mathsf{Succ}\mathcal{A}_{\Pi}$ be that of $\mathcal{A}_{\Pi}$. Let E_0 be the event that $\mathcal{A}_{\mathcal{SC}}$ queries H-oracle with $m_b||r_b||ID_A$, where b is the encrypted bit and E_1 be the event that $\mathcal{A}_{\mathcal{SC}}$ queries H-oracle with $m_{\overline{b}}||r_{\overline{b}}||ID_A$, where $\overline{b}$ is the complement of b. Then

$$\begin{aligned} Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}] = Pr[&\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|\mathsf{E}_0] \cdot Pr[\mathsf{E}_0] \\ &+ Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \cdot Pr[(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \\ &+ Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)] \cdot Pr[(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)]. \end{aligned}$$

and

$$\begin{aligned} Pr[\mathsf{Succ}\mathcal{A}_{\Pi}] = Pr[&\mathsf{Succ}\mathcal{A}_{\Pi}|\mathsf{E}_0] \cdot Pr[\mathsf{E}_0] \\ &+ Pr[\mathsf{Succ}\mathcal{A}_{\Pi}|(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \cdot Pr[(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \\ &+ Pr[\mathsf{Succ}\mathcal{A}_{\Pi}|(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)] \cdot Pr[(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)]. \end{aligned}$$

Now, as per the simulation, we have $Pr[\mathsf{Succ}\mathcal{A}_{\Pi}|\mathsf{E}_0] = 1$, $Pr[\mathsf{Succ}\mathcal{A}_{\Pi}|(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] = 0$ and $Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)] = Pr[\mathsf{Succ}\mathcal{A}_{\Pi}|(\sim \mathsf{E}_0) \wedge (\sim \mathsf{E}_1)]$. So,

$$\begin{aligned} Pr[\mathsf{Succ}\mathcal{A}_{\Pi}] - Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}] &= (1 - Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|\mathsf{E}_0]) \cdot Pr[\mathsf{E}_0] \\ &\quad - Pr[\mathsf{Succ}\mathcal{A}_{\mathcal{SC}}|(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \cdot Pr[(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] \\ &\geq -Pr[(\sim \mathsf{E}_0) \wedge \mathsf{E}_1] = -\frac{q_H}{2^t}. \end{aligned}$$

Thus, $Pr[\mathsf{Succ}\mathcal{A}_{\Pi}] \geq Pr[\mathsf{Succ}_{\mathcal{SC}}] - \frac{q_H}{2^t}$

Thus, $\mathcal{A}_{\Pi}$ can win the IND-CCA2 game with probability

$$\epsilon\left(1 - \frac{1}{2^l}\right)^{q_U} - \frac{q_H}{2^t} \geq \epsilon - \left(\frac{q_H}{2^t} + \frac{q_U}{2^l}\right)$$

□

Theorem 3. *$\mathcal{SC}$ is d-MU-UF-SC-iCMA secure in the sense of multi-user insider existential signcryptext unforgeability in standard model if $\mathcal{S}$ is UF-CMA secure.*

Proof. To prove this, we will construct a UF-CMA forger ζ against $\mathcal{S}$ using a d-MU-UF-SC-iCMA forger $\mathcal{F}$ against $\mathcal{SC}$. As an input, ζ is fed with pk_A of $\mathcal{S}$ and given the signing oracle $\mathcal{O}\mathsf{Sign}(sk_A, \cdot)$ of $\mathcal{S}$. ζ simulates $\mathcal{F}$ with pk_A. In addition to this, ζ publishes a hash function $H : \{0,1\}^{k+k'} \rightarrow \{0,1\}^l$.

Simulation of Signcryption Oracle ($\mathcal{O}\mathsf{Signcrypt}(sk_A, \cdot, \cdot)$): When $\mathcal{F}$ submits a signcryption query $(pk_{B'}, m)$, ζ queries $\mathcal{O}\mathsf{Sign}(sk_A, \cdot)$ with $m||ID_{B'}$ to receive a signature σ on $m||ID_{B'}$. Then, ζ chooses $r \in_R \{0,1\}^t$ and outputs $c = \mathsf{Enc}(pk_{B'}, m||r, \sigma \oplus H(m||r||ID_A))$ to $\mathcal{F}$.

After the query phase is over, $\mathcal{F}$ outputs a receiver key pair (pk_B, sk_B) and a signcryptext (c^*, ID_A, ID_B) to ζ. ζ decrypts c^* with $\mathsf{Dec}(sk_B, c^*)$ to get $(m^*||r^*, \beta^*)$ and compute $\sigma^* = \beta^* \oplus H(m^*||r^*||ID_A)$. ζ outputs σ^*.

Now, the theorem follows from the following lemma.

Lemma 2. *The following are true:*

1. *If c^* is a valid signcryptext from A to B, then σ^* is a valid signature of A on $m^*||ID_B$.*
2. *If m^*, the underlying message of c^*, have not been submitted to the signcryption oracle $\mathcal{O}\mathsf{Signcrypt}(sk_A, pk_B, \cdot)$, then $m^*||ID_B$ have not been queried to the signing oracle $\mathcal{O}\mathsf{Sign}(sk_A, \cdot)$.*

Proof. 1. If c^* is a valid signcryptext from A to B, then $\mathsf{Ver}(sk_A, \sigma^*, m^*||ID_B) = 1$. Hence, the result.
2. If m^*, the underlying message of c^*, have not been submitted to the signcryption oracle $\mathcal{O}\mathsf{Signcrypt}(sk_A, pk_B, \cdot)$, then, as per the simulation, $m^*||ID_B$ have not been queried to the signing oracle $\mathcal{O}\mathsf{Sign}(sk_A, \cdot)$. □

Theorem 4. *$\mathcal{SC}$ is d-MU-IND-SC-iCCA2 secure in the sense of multi-user insider confidentiality in random oracle model and d-MU-UF-SC-iCMA secure in the sense of multi-user insider existential signcryptext unforgeability in standard model if Π is IND-CCA2 secure and $\mathcal{S}$ is UF-CMA secure.*

Proof. The proof follows from Theorems 2 & 3. □

5 Comparison with Li and Wong Construction [9]

It is to be noted that the proposed conversion relies on weaker buliding blocks both in terms of the encryption and signature primitives than [9], as the authors in [9] used an Ω-uniform IND-CCA2 secure PKE-RR and an UF-CMA secure uniformly-distributed signature scheme as components. But, not only there exist a few known constructions of Ω-uniform IND-CCA2 secure PKE-RR but also the notion of Ω-uniform IND-CCA2 security is somewhat artificial. In our construction, we use an weaker encryption primitive i.e., an IND-CCA2 secure PKE-RR and a UF-CMA secure signature scheme (not necessarily uniformly-distributed), making it open to a larger class of encryption and signature schemes by incorporating just one hashing (described above) in each of signcryption/ unsigncryption phases. Moreover the proposed construction is secure in dynamic multi-user insider setting whereas [9] is only secure in two-user outsider model.

One can point out that the security in the Li-Wong construction was in standard model, whereas in the proposed one, confidentiality relies on random oracle model[3]. But, we argue that relying on a more general primitive (like IND-CCA2

[3] It is to be noted that we still managed to achieve unforgeability in standard model.

security) in random oracle model is better than to depend on a ‘less-common’ primitive (like Ω-uniform IND-CCA2 security) in standard model, keeping in mind the generic nature of the conversion and the enhanced level of security that we achieved.

6 Conclusion and Open Issues

In this paper, we have presented a provably secure generic construction of signcryption scheme $\mathcal{SC}$ from an IND-CCA2 randomness recoverable public-key encryption scheme (PKE-RR) Π and a UF-CMA secure signature scheme $\mathcal{S}$. The construction is shown to be d-MU-IND-SC-iCCA2 secure in random oracle model and d-MU-UF-SC-iCMA secure in standard model, both in dynamic multi-user insider setting. The proposed scheme $\mathcal{SC}$ is more acceptable than its obvious counterpart [9] due to its reliance on weaker building blocks. As a by-product, we also showed that Fujisaki-Okamoto transform on PKE-RR can yield better efficiency than using it on a normal PKE.

Clearly, the proposed construction can not achieve efficiency like [10], but the main objective of this paper is to demonstrate the fact that the novel idea of using PKE-RR in constructing signcryption schemes, introduced in [9], can be modified to achieve enhanced security and to make it open to a larger class of cryptographic primitives. As future research, it can be a novel issue to design a generic conversion that uses a one-way PKE-RR rather than an IND-CCA2 one.

Acknowledgements. The authors would like to thank Summit Kumar Pandey of C.R.Rao Institute, Hyderabad, India and Partha Sarathi Roy and Sabyasachi Dutta of Department of Pure Mathematics, University of Calcutta, India for several fruitful comments and discussions in the initial phase of the work.

References

1. An, J.H., Dodis, Y., Rabin, T.: On the security of joint signature and encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 83–107. Springer, Heidelberg (2002)
2. Baek, J., Steinfeld, R., Zheng, Y.: Formal proofs for the security of signcryption. Journal of Cryptology 20(2), 203–235 (2007)
3. Bellare, M., Rogaway, P.: Optimal Asymmetric Encryption. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995)
4. Dachman-Soled, D., Fuchsbauer, G., Mohassel, P., O’Neill, A.: Enhanced Chosen-Ciphertext Security and Applications. Eprint archive (2012), `http://eprint.iacr.org/2012/543`
5. Das, A., Adhikari, A.: An Efficient IND-CCA2 secure Paillier-based cryptosystem. Information Processing Letters 112, 885–888 (2012)
6. Elgamal, T.: A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms. IEEE Trans. on Information Theory, IT-31(4), 469–472 (1985)
7. Fujisaki, E., Okamoto, T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost. In: Imai, H., Zheng, Y. (eds.) PKC 1999. LNCS, vol. 1560, pp. 53–68. Springer, Heidelberg (1999)

8. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
9. Li, C.K., Wong, D.S.: Signcryption from randomness recoverable public key encryption. Information Sciences 180, 549–559 (2010)
10. Matsuda, T., Matsuura, K., Schuldt, J.C.N.: Efficient Constructions of Signcryption Schemes and Signcryption Composability. In: Roy, B., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 321–342. Springer, Heidelberg (2009)
11. McEliece, R.: A public key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, 114–116 (1978)
12. Nieto, J.M.G., Boyd, C., Dawson, E.: A Public Key Cryptosystem Based On A Subgroup Membership Problem. Designs, Codes and Cryptography 36, 301–316 (2005)
13. Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
14. Rackoff, C., Simon, D.: Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. In: 22nd Annual ACM Symposium on Theory of Computing, pp. 427–437 (1990)
15. Zheng, Y.: Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption). In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 165–179. Springer, Heidelberg (1997)