A Modified An-Dodis-Rabin Construction

No Author Given

No Institute Given

Abstract. In Eurocrypt 2002, An, Dodis and Rabin proposed a Commit-then-Encrypt& Sign approach ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$) to construct a signcryption scheme. Their construction is generic and efficient since the Encryption and Signature algorithms can be run in parallel during the Signcryption phase and the Decryption and Verification algorithms can be run in parallel during the Designcryption phase. However, this construction yields a (generalized) fM-IND-iCCA secure signcryption scheme if the Encryption scheme is (generalized) IND-CCA secure and the Commitment scheme has hiding property. In this paper, we show that under a mild assumption, one can suitably modify (an instantiation of) the An-Dodis-Rabin construction to obtain a signcryption scheme that is fM-IND-iCCA secure even when the underlying Encryption scheme is One-Way secure.

Keywords: An-Dodis-Rabin construction, Signcryption, One Way Encryption

1 Introduction

Confidentiality and Authentication are two of the major goals in cryptography. One obvious way to achieve both is to use encryption and signature as black boxes. Some of the ways that this is done are Encrypt and Sign, Encrypt then Sign and Sign then Encrypt. It is known that the first two are not secure since they do not achieve confidentiality and unforgeability respectively. Sign then Encrypt approach achieves both confidentiality and unforgeability but at the expense of higher computational cost and ciphertext overhead.

In 1997, Zheng[12] proposed a new primitive *viz* signcryption in which encryption and signature are done simultaneously at a much lower computational cost and communication overhead than the Sign-then-Encrypt approach. The scheme in [12] was not formally proved to be secure since no formal notion of security was proposed then. It was only in PKC 2002 that Baek, Steinfeld and Zheng [2] introduced a formal notion of security for signcryption.

Since the introduction of the primitive, several schemes have been proposed [12, 1, 2, 8, 9, 4, 5, 7, 11, 10, 6]. Matsuda-Matsuura-Schuldt [10] and Chiba-Matsuda-Schuldt-Matsuura [6] gave several simple but efficient constructions of signcryption schemes using existing primitives. In one of the constructions, they introduced the notion of *signcryption composable* and show how, in this case, a signature scheme and an encryption scheme can be combined to achieve higher

efficiency than a simple composition. ([10, 6] gives a nice account of some previous work on signcryption and has an extensive bibliography.)

The simplest security model for a signcryption scheme considers the two two-user setting [1, 4] in which the interaction takes place between sender and receiver only. But this setting does not incorporate the real setting, as pointed out by [5], in which multiple senders may interact with the same receiver and multiple receivers may interact with the same sender. Hence, a more realistic setting is multi-user setting. Security of signcryption schemes can be further seen into two different attack models, namely *insider* and *outsider* attack model. In the outsider security model, adversary is not allowed to possess the secret keys of the sender and receiver bit in the insider security model, attacker may possess the secret keys of one of the parties. Currently, the strongest security model is insider attack model in the multi-user setting which was first introduce and used by [9]. Now, there are several schemes [8, 9, 5] which achieve the strongest security in the random oracle model [3]. There are several schemes [1, 11, 10] which are secure secure in the standard model but does not achieve the strongest security motion. Recently, Chiba-Matsuda-Schuldt-Matsuura [6] has given a generic construction of signcryption scheme which achieves the strongest security in the standard model.

Earlier, An, Dodis and Rabin [1] proposed a Commit-then-Encrypt& Sign approach ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$) to construct a signcryption scheme. The main feature of this approach is that both Encryption and Signature can be done in parallel in the Signcryption phase and Decryption and Verification can be done in parallel in the Designcryption phase. But from the point of security, this scheme achieves generalized indistinguishability against chosen ciphertext attack if *Commit* has the hiding property and *Encryption* is (generalized) IND-CCA secure(a slightly weaker notion); while it is unforgeable against chosen message attacks if *Commit* achieves the binding property and *Signature* is EUF-CMA secure i.e. existentially unforgeable under chosen message attacks.

In this paper, we revisit the approach proposed by An et. al. We obtain an instantiation of it by instantiating the commitment scheme with a standard commitment scheme using hash functions. This construction does not yield IND-CCA security if the underlying Encryption scheme is taken to be One-Way-Encryption (OWE) secure (see [1]). Thus a suitable transformation has to be made for lifting to a stronger security model. We thus suitably modify the preceding construction and show that the modified scheme will achieve indistinguishability against chosen ciphertext attacks, in the random oracle model, even when the Encryption scheme is OWE secure. Hence, a suitable modification of the An-Dodis-Rabin construction can achieve IND-CCA security even when the underlying encryption scheme is taken to be OWE secure.

2 Preliminaries

2.1 Formal Model for Commitment Scheme

Throughout this paper, by a Commitment Scheme we shall mean a non-interactive Commitment Scheme. A Commitment Scheme consists of three algorithms:

- **Setup :** A probabilistic polynomial time algorithm that takes a security parameter as input and outputs a Commitment Key CK (possibly empty) and public parameters.
- **Commit :** A probabilistic polynomial time algorithm which takes a message m, public parameters and a commitment key CK and outputs a pair (c, d), where c is the commitment and d is the decommitment.
- **Open :** A deterministic polynomial time algorithm which takes a commitment-decommitment pair (c, d) together with the commitment key CK as input and returns m if (c, d) is a valid pair for m, else $\perp$.

For consistency, it is required that $\text{Open}_{CK}(\text{Commit}_{CK}(m)) = m$ for all messages $m \in \mathcal{M}$.

2.2 Properties of Commitment

1. **Hiding Property** : There exists no probabilistic polynomial time adversary $\mathcal{A} = (A_1, A_2)$ which can distinguish the commitment to any two messages of its choice with non-negligible probability.
   Formally, a commitment scheme is said to have the hiding property if $\Pr[b = \bar{b} | CK \leftarrow \mathit{Setup}(1^k), (m_0, m_1, st) \leftarrow A_1(CK), b \overset{R}{\leftarrow} \{0,1\}, (c, d) \leftarrow \mathit{Commit}_{CK}(m_b), \bar{b} \leftarrow A_2(c, st)] = \frac{1}{2} + \epsilon$,
   where ϵ is a negligible quantity.

2. **Binding Property** : There exists no probabilistic polynomial time adversary $\mathcal{A}$, having knowledge of CK, that can come up with (c, d, d') such that (c, d) and (c, d') are valid commitment pairs for m and m' with $m \neq m'$.

3. **Relaxed Binding Property**: There exists no probabilistic polynomial time adversary $\mathcal{A}$, having knowledge of CK, that can come up with a message m and $\mathcal{A}(c, d, CK)$ produces with non-negligible probability a value d' for the output of $\mathit{Commit}(m)$, say (c, d), such that (c, d') is a valid commitment to some $m' \neq m$. Namely, $\mathcal{A}$ cannot find a collision using a randomly generated $c(m)$, even for m of its choice.

2.3 Formal Model for Encryption Scheme

An encryption scheme is given by the following algorithm:

- **KG(1^λ):** A probabilistic polynomial time algorithm which takes security parameter 1^λ as input and outputs a public-private key pair (PK, SK).

- **ENC(m, PK):** A probabilistic polynomial time algorithm which takes a message m and public key PK as input and returns ciphertext $\mathcal{C}$.
- **DEC$(\mathcal{C}, SK, PK)$:** A deterministic polynomial time algorithm which takes ciphertext $\mathcal{C}$, secret key SK and public key PK as input and returns a message m if C is a valid ciphertext else $\perp$.

For consistency, it is required that for all $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$ and all messages m, $m = \mathrm{DEC}(\mathrm{ENC}(m, PK), SK, PK)$.

2.4 Security Notions of Encryption Scheme

An asymmetric encryption scheme is said to be **OWE (One Way Encryption)** secure if no probabilistic polynomial time algorithm $\mathcal{A}$ has a non-negligible advantage, where the advantage of $\mathcal{A}$ is defined as

$$\Pr[(PK, SK) \leftarrow \mathrm{KG}(1^\lambda); y \leftarrow \mathrm{ENC}(m, PK); \mathcal{A}(y, PK) = \mathrm{DEC}(y, SK, PK)].$$

An asymmetric encryption scheme is said to be **IND-CCA (indistinguishable against chosen ciphertext attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game. In this game, $\mathcal{A}$ has access to a decryption oracle $\mathcal{O} = \{Decryption\}$

- *Decryption*: Given a ciphertext $\mathcal{C}$, except the challenge ciphertext, the oracle returns $m \leftarrow \mathrm{DEC}(\mathcal{C}, SK, PK)$.

$\underline{\mathbf{Game}^{IND-CCA}_{ENC,\mathcal{A}}(1^\lambda)}$

- $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(PK)$
- $b \xleftarrow{R} \{0, 1\}$
- $y \leftarrow \mathrm{ENC}(m_b, PK)$
- $b' \leftarrow \mathcal{A}_2^{\mathcal{O}}(y, PK, st)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}|$

Remark: There is a weaker notion of IND-CCA, known as **IND-CPA (indistinguishable against chosen plaintext attack)** in which $\mathcal{A}$ does not have any oracle.

2.5 Formal Model for Signature Scheme

A signature scheme is given by following algorithms:

- **KG(1^λ):** A probabilistic polynomial time algorithm which takes security parameter 1^λ as input and outputs a public-private key pair (PK, SK).

- **SIG**(m, SK, PK)**:** A probabilistic polynomial time algorithm which takes a message m, a secret key SK, public key PK as input and outputs a signature σ.
- **VER**(m, σ, PK)**:** A deterministic polynomial time algorithm which takes a message m, a signature σ, and public key PK as input and outputs true if σ is a valid signature on message m, else it returns false.

2.6 Security Notion of Signature Scheme

A signature scheme is said to be **EUF-CMA (existentially unforgeable against chosen message attack)** secure if no probabilistic polynomial time algorithm has a non-negligible advantage in the following game. In this game, $\mathcal{A}$ has access to a signature oracle $\mathcal{O} = \{Signature\}$

- $Signature$: Given a message m, oracle returns $\sigma \leftarrow \text{SIG}(m, SK, PK)$ and adds (m, σ) to the list L.

$\underline{\textbf{Game}^{SUF-CMA}_{SIG,\mathcal{A}}(1^\lambda)}$

- $L \leftarrow \phi$
- $(PK, SK) \leftarrow \text{KG}(1^\lambda)$
- $(m, \sigma) \leftarrow \mathcal{A}^{\mathcal{O}}(SK, PK)$
- $x \leftarrow \text{VER}(m, \sigma, PK)$

Advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = \Pr(x = true \wedge m \notin L)$

2.7 Formal Model for Signcryption Scheme

A signcryption scheme is given by following algorithms:

- **Setup**(1^λ)**:** A probabilistic polynomial time algorithm which takes a security parameter as input and outputs the public parameters $Params$.
- **KG**$_{Rec}(Params)$**:** A probabilistic polynomial time algorithm which takes $Params$ as input and outputs the public-private receiver key pair (PK_{Rec}, SK_{Rec}).
- **KG**$_{Sen}(Params)$**:** A probabilistic polynomial time algorithm which takes $Params$ as input and outputs the public-private sender key pair (PK_{Sen}, SK_{Sen}).
- **SC**$(m, PK_{Rec}, SK_{Sen}, Params)$**:** A probabilistic polynomial time algorithm which takes a message m, a receiver's public key PK_{Rec}, a sender's private key SK_{Sen} and public parameters $Params$ as input and returns ciphertext $\mathcal{C}$.
- **DSC**$(\mathcal{C}, SK_{Rec}, PK_{Sen}, Params)$**:** A deterministic polynomial time algorithm which takes a ciphertext $\mathcal{C}$, a receiver's secret key SK_{Rec}, a sender's public key PK_{Sen} and public parameters $Params$ and returns either a message m if $\mathcal{C}$ is a valid ciphertext, else it returns $\perp$.

For consistency, it is required that for all $Params \leftarrow \text{Setup}(1^\lambda)$, all $(PK_{Rec}, SK_{Rec}) \leftarrow \text{KG}_{Rec}(Params)$, all $(PK_{Sen}, SK_{Sen}) \leftarrow \text{KG}_{Sen}(Params)$ and all messages m, $m = \text{DSC}(\text{SC}(m, PK_{Rec}, SK_{Sen}, Params), SK_{Rec}, PK_{Sen}, Params)$.

2.8 Security Notion of Signcryption Scheme

We define the security notions in fixed multi-user insider security model. In the fixed multi-user model, public-private key pair of receiver and sender are generated at the beginning of the game. In the insider security model, adversary knows the private key of the sender.

Confidentiality: A signcryption scheme S_{SC} is said to be fM-IND-iCCA (indistinguishable against insider chosen ciphertext attack under fixed multi-user model) secure if no probabilistic polynomial time adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game. In this game the adversary $\mathcal{A}$ has access to a designcryption oracle $\mathcal{O} = \{Designcryption\}$

- $Designcryption$: Given a ciphertext $\mathcal{C}$, except the challenge ciphertext, the oracle returns $m/\perp \leftarrow \text{DSC}(\mathcal{C}, SK_{Rec}, PK_{Sen}, Params)$, where SK_{Rec} and PK_{Sen} are generated in the beginning of the game.

Game$^{fM-IND-iCCA}_{S_{SC},\mathcal{A}}$

- $Params \leftarrow \text{Setup}(1^\lambda)$
- $(PK_{Rec}, SK_{Rec}) \leftarrow \text{KG}_{Rec}(Params)$
- $(PK_{Sen}, SK_{Sen}) \leftarrow \text{KG}_{Sen}(Params)$
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(PK_{Rec}, PK_{Sen}, SK_{Sen}, Params)$
- $b \overset{R}{\leftarrow} \{0, 1\}$
- $\mathcal{C} \leftarrow \text{SC}(m_b, PK_{Rec}, SK_{Sen}, Params)$
- $b' \leftarrow \mathcal{A}_2^{\mathcal{O}}(\mathcal{C}, PK_{Rec}, PK_{Sen}, SK_{Sen}, Params, st)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}|$

Unforgeability: A signcryption scheme S_{SC} is said to be **fM-EUF-iCMA (existentially unforgeable against insider chosen message attack under fixed multi-user model)** secure if no probabilistic polynomial time adversary $\mathcal{A}$ has a non-negligible advantage in the following game. In this game, adversary $\mathcal{A}$ has access to a signcryption oracle $\mathcal{O} = \{Signcryption\}$

- $Signcyption$: Given a message m, the oracle returns $\mathcal{C} \leftarrow \text{SC}(m, PK_{Rec}, SK_{Sen}, Params)$ where PK_{Rec} and SK_{Sen} are generated in the beginning of the game. The oracle then adds m to the list L.

Game$^{fM-EUF-iCMA}_{S_{SC},\mathcal{A}}$

- $L \leftarrow \phi$
- $Params \leftarrow \text{Setup}(1^k)$
- $(PK_{Rec}, SK_{Rec}) \leftarrow \text{KG}_{Rec}(Params)$
- $(PK_{Sen}, SK_{Sen}) \leftarrow \text{KG}_{Sen}(Params)$
- $\mathcal{C} \leftarrow \mathcal{A}_1^{\mathcal{O}}(PK_{Rec}, PK_{Sen}, SK_{Rec}, Params)$
- $m \leftarrow \text{DSC}(\mathcal{C}, SK_{Rec}, PK_{Sen}, Params)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = \Pr(m \neq \perp \wedge m \notin L)$

3 The An-Dodis-Rabin Scheme

In this section we shall consider the signcryption scheme of An, Dodis and Rabin[1]. They have given a generic construction of a signcryption scheme. In this scheme, the Signcryption phase consists of three algorithms *viz* Commit, Encryption and Signature, while the Designcryption phase consists of three algorithms *viz* Decryption, Verification and Open. An et. al. proved that if Encryption is *generalised* IND-CCA secure and Commit has the hiding property, then the signcryption scheme is *generalized* fM-IND-iCCA secure(cf [1]). Also, it was proved that if the Signature scheme is EUF-CMA secure and Commit has the relaxed binding property, then the Signcryption scheme is fM-EUF-iCMA secure.

We now consider below their scheme by instantiating Commit with a simple standard commitment scheme and discuss the security implications. We denote Commitment scheme as $(\text{Setup}^C, \text{Commit}, \text{Open})$, Encryption scheme as $(\text{KG}^E, \text{ENC}, \text{DEC})$ and Signature scheme as $(\text{KG}^S, \text{SIG}, \text{VER})$.

Setup(1^λ)

- $(H_1, H_2) \leftarrow \text{Setup}^C(1^\lambda)$
  $H_1, H_2 : \{0,1\}^* \rightarrow \{0,1\}^*$ be two secure hash functions.
- $Params \leftarrow (H_1, H_2, 1^\lambda)$

KG$_{Rec}(Params)$ **and KG**$_{Sen}(Params)$

- $(PK^E, SK^E) \leftarrow \text{KG}^E(1^\lambda)$
- $(PK^S, SK^S) \leftarrow \text{KG}^S(1^\lambda)$
- $PK_{Rec} = (PK^E_{Rec}, PK^S_{Rec})$
- $SK_{Rec} = (SK^E_{Rec}, SK^S_{Rec})$
- $PK_{Sen} = (PK^E_{Sen}, PK^S_{Sen})$
- $SK_{Sen} = (SK^E_{Sen}, SK^S_{Sen})$

SC$(m, PK_{Rec}, SK_{Sen}, Params)$

1. Commit(m)
   - $r \rightarrow \mathcal{R}$
   - $h_1 = H_1(m, r)$
   - $h_2 = H_2(r)$
   - $c = h_2 \oplus m$
   - Return $(h_1, r||c)$
2. $c' \rightarrow ENC(r||c, PK^E_{Rec})$
3. $\sigma \rightarrow SIG(h_1, SK^S_{Sen}, PK^S_{Sen})$

Ciphertext $\mathcal{C} \equiv (c', h_1, \sigma)$

DSC$(\mathcal{C} \equiv (c', h_1, \sigma), SK_{Rec}, PK_{Sen}, Params)$

1. $r||c \rightarrow DEC(c', SK^E_{Rec}, PK^E_{Rec})$
2. $x \rightarrow VER(h_1, \sigma, PK^S_{Sen})$. If x is false, return $\perp$, else goto next step.
3. Open$((r||c, h_1, \sigma))$

- $h_2 = H_2(r)$
- $m = h_2 \oplus c$
- if $h_1 = H_1(m, r)$, return m; else return $\perp$.

As pointed out above, to obtain a (generalized) fM-IND-iCCA secure signcryption one needs to consider an IND-CCA secure encryption scheme along with a commitment scheme that has the hiding property. Note that the commitment scheme that we have considered has the hiding property in the random oracle model. Thus if in the above construction the encryption scheme is IND-CCA secure, the resulting signcryption would be (generalized) fM-IND-iCCA secure. A natural question is whether one can weaken this condition i.e. can one take an encryption scheme which is secure in a weaker model. We shall show below that relaxing the security assumption of the encryption scheme can lead to an insecure signcryption scheme. Consider the following encryption scheme which is OWE secure under the RSA assumption. We first define an RSA assumption and then present an OWE secure encryption scheme.

RSA Assumption : Let n be the product of two prime numbers p and q, i.e. $n = pq$. Let e be an odd integer that is relatively prime to $\phi(n)$. Then the RSA assumption states that given (n, e) and C where $C \equiv M^e \pmod{n}$ for some randomly chosen $M \in \mathbb{Z}_n$, it is hard to calculate M.

An OWE secure Encryption Scheme

1. KeyGeneration algorithm (KG) is the same as in RSA, where e, d are the encryption and decryption exponents and n is the RSA modulus.
2. ENC(m, PK_{Rec})
   - $r \rightarrow \mathcal{R}$
   - $C \equiv (r^e \pmod{n}, mr \pmod{n})$
3. DEC$(C \equiv (r^e \pmod{n}, mr \pmod{n})), SK_{Rec}, PK_{Rec})$
   - $r^{ed} \equiv r \pmod{n}$
   - $m \equiv mrr^{-1} \pmod{n}$

We now prove that the above scheme is OWE secure under the RSA assumption.

Proposition 1. *The above encryption scheme is OWE secure provided the RSA assumption holds for the parameters* (n, e).

Proof. Suppose an adversary $\mathcal{A}$ can break the OWE security of above scheme (whose parameters are (n, e)) with non-negligible probability. We shall simulate a game in which a *Challenger*$\mathcal{B}$ is given an instance of the RSA problem *viz* (n, e) and $C \equiv M^e \pmod{n}$. $\mathcal{B}$, with the help of $\mathcal{A}$, solves the RSA problem as follows. $\mathcal{B}$ chooses a number $\bar{C}$ from $\mathbb{Z}_n^*$ uniformly at random and sends the ciphertext $(C, \bar{C})$ along with the public parameters (n, e) to the adversary $\mathcal{A}$. Suppose $\mathcal{A}$ returns m. $\mathcal{B}$ then computes $M = \bar{C}m^{-1} \pmod{n}$. Note that to $\mathcal{A}'s$ view, $\bar{C} = mM \pmod{n}$ and with non-negligible probabilty obtains m and hence M .

Remark : The above scheme is malleable in the sense that an adversary can create a ciphertext distinct from a given ciphertext such that both the ciphertexts yield the same message after decryption. For example, given $\mathcal{C}_1 = (r^e, mr)$ one can construct $\mathcal{C}_2 = (s^e r^e, smr)$, where s is random. Then it is easy to see that $DEC(\mathcal{C}_1, d, n) = DEC(\mathcal{C}_2, d, n) = m$.

3.1 OWE SECURE ENCRYPTION and An-Dodis-Rabin SCHEME

We shall now show that if the OWE secure encryption scheme given above is used in the An-Dodis-Rabin construction of Section 3, then one ends up with an insecure signcryption scheme.

Assume that the above OWE secure Encryption scheme is used in the An -Dodis -Rabin construction. Consider now the corresponding IND-CCA game where the adversary $\mathcal{A}$ is given the challenge ciphertext $\mathcal{C}_1$. Note that $\mathcal{C}_1$ is of the form (c', h_1, σ), where c' is the encryption of the decommitment part and σ is the signature of h_1 . Having obtained $\mathcal{C}_1$, $\mathcal{A}$ then creates another ciphertext $\mathcal{C}_2 = (c'', h_1, \sigma)$ such that $DEC(c', SK^E_{Rec}, PK^E_{Rec}) = DEC(c'', SK^E_{Rec}, PK^E_{Rec})$. Note that $\mathcal{C}_2$ will be a valid ciphertext distinct from $\mathcal{C}_1$. The adversary then queries the Decryption Oracle with $\mathcal{C}_2$. Using the output obtained from the Decryption Oracle, it is not hard to see that $\mathcal{A}$ can easily win the indistinguishability game.
Remark : Note that the above An-Dodis-Rabin construction can be modified in another way by considering the encryption of r instead of $r||c$ and sending c as part of the ciphertext. Even for this scheme, the observation made above holds.

3.2 Extending An-Dodis-Rabin Scheme

It is now natural to ask if the generic construction of Section 3 can suitably be modified so as to obtain an IND-CCA secure signcryption *even when the underlying encryption scheme is only OWE secure* To answer this we present below a variant of the An-Dodis-Rabin generic construction by making a suitable transformation. We then prove that even if the encryption scheme used in the generic construction is OWE secure, the resulting signcryption scheme that we obtain would be IND-CCA secure in the random oracle model.

The Extended An-Dodis-Rabin Scheme
Setup(1^λ), $\text{KG}_{Rec}(Params)$ and $\text{KG}_{Sen}(Params)$ are same as defined in section 3.
SC$(m, PK_{Rec}, SK_{Sen}, Params)$

- $r \rightarrow \mathcal{R}$
- $h_1 = H_1(m, r)$
- $c' \rightarrow ENC(r, PK^E_{Rec})$
- $\sigma \rightarrow SIG(h_1, SK^s_{Sen}, PK^S_{Sen})$

- $h_2 = H_2(r, c', h_1, \sigma)$
- $c = h_2 \oplus m$

Ciphertext $\mathcal{C} \equiv (c, c', h_1, \sigma)$

DSC$(\mathcal{C} \equiv (c, c', h_1, \sigma), SK_{Rec}, PK_{Sen}, Params)$

- $r \rightarrow DEC(c', SK^E_{Rec}, PK^E_{Rec})$
- $x \rightarrow VER(h_1, \sigma, PK^S_{Sen})$. If x is false, return $\perp$; else go to the next step.
- $h_2 = H_2(r, c', h_1, \sigma)$
- $m = h_2 \oplus c$
- if $h_1 = H_1(m, r)$, return m; else return $\perp$.

Note that the scheme is no longer an instantiation of the An-Dodis-Rabin scheme and the input to the hash function H_2 is (r, c', h_1, σ). We will now prove that if the encryption scheme is OWE secure, then our Signcryption scheme is fM-IND-iCCA secure in the Random Oracle Model. We would also show that if the signature scheme is EUF-CMA secure in the standard model, then our Signcryption scheme is fM-EUF-CMA secure in the standard model.

4 Security

4.1 Message Confidentiality

Theorem 1. *In the random oracle model, if there exists an fM-IND-iCCA adversary $\mathcal{A}$ which can distinguish ciphertexts during the relevant game with a non-negligible advantage, then there exists an algorithm $\mathcal{B}$ which can break the OWE security of the parent encryption scheme ENC with a non-negligible advantage. Formally,*

$$\mathcal{A}dv(\mathcal{B}) \geq \frac{1}{q_{Dec}}\left(\frac{\mathcal{A}dv(\mathcal{A})}{q_{H_1} + q_{H_2} + \mathcal{A}dv(\mathcal{A})}\right) \geq \frac{1}{2q_{Dec}}\left(\frac{\mathcal{A}dv(\mathcal{A})}{q_{H_1} + q_{H_2}}\right),$$

where q_{Dec} is the number of decryption queries, q_{H_1} and q_{H_2} the number of H_1 and H_2 queries respectively, $\mathcal{A}dv(\mathcal{A})$ and $\mathcal{A}dv(\mathcal{B})$ being the advantages of $\mathcal{A}$ and $\mathcal{B}$ respectively.

Proof has been given in appendix $A.1$.

4.2 Ciphertext Unforgeability

Theorem 2. *In the standard model, if there exists an fM-EUF-CMA adversary $\mathcal{A}$ which is able to produce a forged ciphertext during the game with a non-negligible advantage, then there exists an algorithm $\mathcal{B}$ which can forge the signature scheme S_{SIG} in the EUF-CMA game or finds a collision on hash function H_1 with a non-negligible probability. Formally,*

$$\mathcal{A}dv(\mathcal{A}) \leq Pr(Collision\ on\ H_1) + Pr(forging\ S_{SIG})$$

where $\mathcal{A}dv(\mathcal{A})$ is the advantage of $\mathcal{A}$.

Proof has been given in appendix $A.2$.

References

1. J.H. An, Y. Dodis and T. Rabin. On the security of joint signature and encryption. In Advances in Cryptology-EUROCRYPT 2002, LNCS 2332, pp. 83-107, Springer Verlag 2002.
2. J. Baek, R. Steinfeld and Y. Zheng. Formal Proofs for the Security of Signcryption. In Public Key Cryptography-PKC 2002, LNCS 2274, pp. 80-98, Springer Verlag 2002.
3. M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols In ACM Conference on Computer and Communications Security, pp. 62-73, ACM 1993
4. A.W. Dent. Hybrid Signcryption Schemes with Outsider Security. In Information Security-ISC 2005, LNCS 3650, pp. 203-217, Springer Verlag 2005.
5. A.W. Dent. Hybrid Signcryption Schemes with Insider Security. In Information Security and Privacy-ACISP 2005, LNCS 3574, pp. 253-266, Springer Verlag 2005.
6. D. Chiba, T. Matsuda, J.C.N. Schuldt and K. Matsuura. Efficient Generic Constructions of Signcryption with Insider Security in the Multi-user Setting In Applied Cryptography and Network Security-ACNS 2011, LNCS 6715, pp. 220-237, Springer Verlag 2011.
7. C.K. Li, G. Yang, D.S. Wong, X. Deng and S.S.M. Chow. An Efficient Signcryption Scheme with Key Privacy. In Public Key Infrastructure-EuroPKI 2007, LNCS 4582, pp. 78-93, Springer Verlag 2007.
8. B. Libert and J. Quisquater. Improved Signcryption from q-Diffie-Hellman Problems. In Security in Communication Networks-SCN 2004, LNCS 3352, pp. 220-234, Springer Verlag 2004.
9. B. Libert and J. Quisquater. Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups. In Public Key Cryptography-PKC 2004, LNCS 2947, pp. 187-200, Springer Verlag 2004.
10. T. Matsuda, K. Matsuura and J.C.N. Schuldt. Efficient Constructions of Signcryption Schemes and Signcryption Composability. In Progress in Cryptology-INDOCRYPT 2009, LNCS 5922, pp. 321-342, Springer Verlag 2009.
11. C.H. Tan. Signcryption Scheme in Multi-user Setting without Random Oracles. In Advances in Information and Computer Security-IWSEC 2008, LNCS 5312, pp. 64-82, Springer Verlag 2008.
12. Y. Zheng. Digital Signcryption or how to achieve Cost(Signature & Encryption) << Cost(Signature)+Cost(Encryption). In Advances in Cryptology-CRYPTO 1997, LNCS 1294, pp. 165-179, Springer-Verlag 1997.

A Appendix

A.1 Proof of Theorem 4.1

Proof. We shall show how to construct an OWE adversary $\mathcal{B}$ that uses $\mathcal{A}$ to gain a non-negligible advantage against ENC.

Suppose Algorithm $\mathcal{B}$ receives the public key PK_{ENC}. Then $\mathcal{B}$ chooses a Signature scheme SIG whose public key PK_{SIG} are generated independently from the public parameters of ENC. Without loss of generality, assume that $PK_{ENC} \cap PK_{SIG} = \phi$. $\mathcal{B}$ maintains two lists L_1, and L_2 for queries on the hash functions

H_1 and H_2. Besides these, $\mathcal{B}$ maintains a list L_{Dec} which keeps the list of ciphertexts queried to the Designcryption Oracle.

We now explain how requests from $\mathcal{A}$ are treated by $\mathcal{B}$ who plays the role of a challenger to $\mathcal{A}$. For the proof we need to make the following assumption.
Assumption: Adversary does not query a ciphertext $\mathcal{C} \equiv (c, c', h_1, \sigma)$ to the Designcryption Oracle, where $\mathcal{C}$ is obtained by applying the encryption algorithm on a message m *and* r *chosen by the adversary.*

In other words,we assume that the adversary has no advantage by getting the message m of its choice from the Designcryption Oracle.

1. Find Stage
   - H_1 query: Input (m_i, r_i)
     $\rightarrow$ Search (m_i, r_i, h_{1i}) in L_1
     $\rightarrow$ If exists
     $\ldots \rightarrow$ Return h_{1i}
     $\rightarrow$ Else
     $\ldots \rightarrow$ For each $(r_i, c'_{i_j}, h_{1i_j}, \sigma_{i_j}, h_{2i_j})$ in L_2
     $\ldots \ldots \rightarrow$ For each $(c_{i_{j_k}}, c'_{i_j}, h_{1i_j}, \sigma_{i_{j_k}})$ in L_{Dec}
     $\ldots \ldots \ldots \rightarrow$ Calculate $m_{i_{j_k}} = c_{i_{j_k}} \oplus h_{2i_j}$
     $\ldots \ldots \ldots \rightarrow$ If $m_{i_{j_k}} = m_i$
     $\ldots \ldots \ldots \ldots \rightarrow$ Put h_{1i_j} in H
     $\ldots \rightarrow$ Choose h_{1i} randomly such that $h_{1i} \notin H$
     $\ldots \rightarrow$ Put (m_i, r_i, h_{1i}) in the list L_1
     $\ldots \rightarrow$ Return h_{1i}

   - H_2 query: Input $(r_i, c'_i, h_{1i}, \sigma_i)$
     $\rightarrow$ Search $(r_i, c'_i, h_{1i}, \sigma_i, h_{2i})$ in L_2
     $\rightarrow$ If exists
     $\ldots \rightarrow$ Return h_{2i}
     $\rightarrow$ Else
     $\ldots \rightarrow$ For each $(c_{i_j}, c'_i, h_{1i}, \sigma_i)$ in L_{Dec}
     $\ldots \ldots \rightarrow$ For each (m_{i_k}, r_i, h_{1i}) in L_1
     $\ldots \ldots \ldots \rightarrow$ Calculate $h_{2i_{j_k}} = m_{i_k} \oplus c_{i_j}$
     $\ldots \ldots \ldots \ldots \rightarrow$ Put $h_{2i_{j_k}}$ in H
     $\ldots \rightarrow$ Choose h_{2i} randomly such that $h_{2i} \notin H$
     $\ldots \rightarrow$ Put $(r_i, c'_i, h_{1i}, \sigma_i, h_{2i})$ in list L_2
     $\ldots \rightarrow$ Return h_{2i}

   - Designcryption query: Input$(c_i, c'_i, h_{1i}, \sigma_i)$
     $\rightarrow$ Put $(c_i, c'_i, h_{1i}, \sigma_i)$ in the list L_{Dec}
     $\rightarrow$ Return $\perp$
2. Challenge Phase
   The adversary $\mathcal{A}$ selects two equal length messages m_0 and m_1 and gives them to $\mathcal{B}$. $\mathcal{B}$ then requests ENC (the Challenger) for the challenge ciphertext. Let c' be the challenge ciphertext given by ENC to $\mathcal{B}$. $\mathcal{B}$ then selects

randomly two strings c and $h_1 \in \{0,1\}^{l_1}$ such that $(c, c', h_1, *)$ should not be in L_{Dec}. $\mathcal{B}$ then computes the signature, say σ, on h_1 and sends (c, c', h_1, σ) to $\mathcal{A}$.

3. Guess stage
   Same as in Find stage

After the end of the Guess stage, $\mathcal{A}$ guesses the message m_v, where $v \in \{0,1\}$. $\mathcal{B}$ ignores the bit v. $\mathcal{B}$ then follows the following algorithm to guess the decryption of c'.

– Algorithm
  → For each (m_0, r_j) in L_1
  ... → Put r_j in R
  → For each (m_1, r_k) in L_1
  ... → Put r_k in R
  → For each $(r_l, c', h_1, \sigma, *)$ in L_2
  ... → Put r_l in R
  → Select r randomly from R
  → Return r

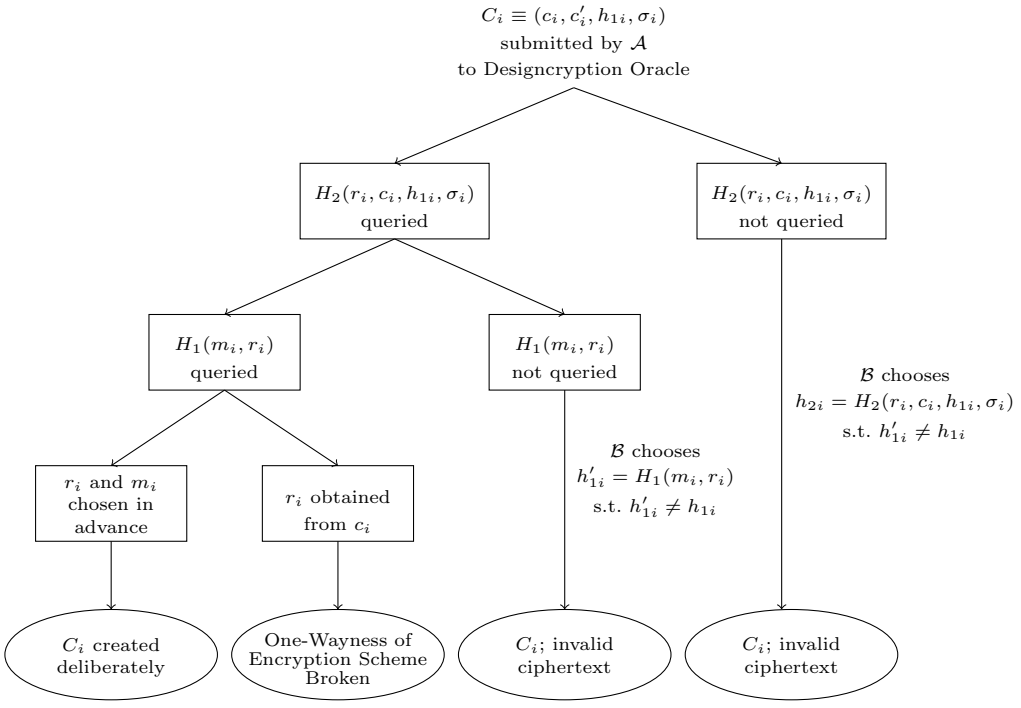

Fig. 1. Diagramattic Sketch of proof of Claim

Claim : Let q_{Dec} be the number of queries to the Designcryption Oracle. Then the Designcryption Oracle in the above game simulates the real game with the probability at least $(1-\epsilon)^{q_{Dec}}$, where ϵ is the advantage of breaking the OWE security of the Encryption Scheme.
Proof of Claim: We analyse the validity of the ciphertext $C_i \equiv (c_i, c_i', h_{1i}, \sigma_i)$ that was submitted by adversary $\mathcal{A}$. According to the simulation of the game, Designcryption oracle returns "*invalid ciphertext*" for each of the query submitted to it. Figure 1 gives a rough sketch of the proof. Let r_i be the decryption of c_i. We now consider all the cases:

1. $H_2(r_i, c_i', h_{1i}, \sigma_i)$ *has been queried*. Let h_{2i} be the output given by H_2 oracle. Then $m_i = c_i' \oplus h_{2i}$. If C_i is a valid ciphertext, then $H_1(m_i, r_i)$ should be h_{1i}. Now, consider the two cases:
   - $H_1(m_i, r_i)$ has not been queried. $\mathcal{B}$ then chooses a string h_{1i}' uniformly at random such that $h_{1i}' \neq h_{1i}$ and set $H_1(m_i, r_i) = h_{1i}'$ Such choice makes C_i to be an invalid ciphertext.
   - $H_1(m_i, r_i)$ has been queried. Let h_{1i}' be the output given by H_1 oracle. If $h_{1i}' \neq h_{1i}$, then C_i will not be a valid ciphertext. If $h_{1i} = h_{1i}'$, we consider two cases:
     - Adversary $\mathcal{A}$ has chosen some random number r_i and then created the ciphertext c_i'. In this case, $\mathcal{A}$ has deliberately created the ciphertext by fixing r_i and m_i in advance. According to our assumption, such a case is not going to arise.
     - Adversary $\mathcal{A}$ has obtained r_i from c_i', i.e., c_i' was chosen first and then r_i was obtained. According to our simulation of the game, designcryption oracle always treats C_j as an invalid ciphertext for $j = 1, \ldots, i-1$. So, $\mathcal{A}$ does not get any information about the decryption of C_i from the previous queries. Hence, obtaining r_i from c_i', in this case, amounts to breaking the one-wayness of the encryption scheme.
2. $H_2(r_i, c_i, h_{1i}, \sigma_i)$ has not been queried. In this case, $\mathcal{B}$ can choose a string h_{2i} uniformly at random such that if $m_i = h_{2i} \oplus c_i$, then $H_1(m_i, r_i) \neq h_{1i}$. Such a choice makes C_i to be an invalid ciphertext.
   Clearly, to every query C_i, the Decryption Oracle gives an incorrect response whenever $\mathcal{A}$ is able to decrypt c_i'. Thus, the above game is a simulation of the real game with probability $(1-\epsilon)^{q_{Dec}}$, where ϵ is the advantage of breaking the OWE security of the Encryption Scheme. □

Proof of the Theorem
Note that in the above simulated game, the Decryption Oracle gives an incorrect output when the adversary $\mathcal{A}$ gives a ciphertext $\mathcal{C} \equiv (c, c', h_1, \sigma)$ to the Decryption Oracle, where

- $\mathcal{A}$ knows $DEC(c') = r$ but she has not run the encryption algorithm on r to obtain c' and
- the message m is chosen apriori by $\mathcal{A}$.

Let

- E_C be the event of decrypting a given ciphertext C without running the algorithm $DEC(.,\ldots,.)$
- E_{Dec} be the event that each output of Decryption Oracle is correct i.e. as in the real game.
- q_{H_1} be the number of H_1 Oracle queries.
- q_{H_2} be the number of H_2 Oracle queries.
- q_{Dec} be the number of Decryption Oracle queries.

Then as explained above

- $\Pr(E_{Dec}) = (1 - \Pr(E_C))^{q_{Dec}}$.

Now observe that when the Decryption Oracle gives correct outputs the simulation is perfect.oreover, when $\mathcal{A}$ guesses the correct bit without a coin-toss, either the H_1-oracle or the H_2-oracle must have been querried and the correct r must occur in the list. By picking a random tuple from the $L_1 \bigcup L_2$, $\mathcal{B}$ wims with probability $\frac{1}{q_{H_1}+q_{H_2}}$.

Let
E_1 denote the event of picking a random tuple from the lists and output r.
E_2 denote the simulation of the real game ,
E_3 denote the event of guessing the correct bit without tossing a coin.
Then
$\Pr(\mathcal{B}wins) = \Pr(E_C) \geq \Pr(E_1 \bigwedge E_2 \bigwedge E_3) \geq \frac{1}{q_{H_1}+q_{H_2}} \Pr(E_{Dec}) \mathcal{A}dv(\mathcal{A}) = \frac{1}{q_{H_1}+q_{H_2}} (1 - \Pr(E_C))^{q_{Dec}} \mathcal{A}dv(\mathcal{A})$
Since $0 \leq \Pr(E_C) \leq 1$, $(1 - \Pr(E_C))^{q_{Dec}} \geq (1 - q_{Dec}\Pr(E_C))$
So,
$\Pr(E_C) \geq \frac{1}{q_{H_1}+q_{H_2}} (1 - q_{Dec}\Pr(E_C)) \mathcal{A}dv(\mathcal{A})$
Hence $\Pr(E_C) \geq \frac{1}{q_{Dec}} (\frac{\mathcal{A}dv(\mathcal{A})}{q_{H_1}+q_{H_2}+\mathcal{A}dv(\mathcal{A})}) \geq \frac{1}{2q_{Dec}} (\frac{\mathcal{A}dv(\mathcal{A})}{q_{H_1}+q_{H_2}})$.
This completes the proof.

A.2 Proof of Theorem 4.2

Proof. Let there be an adversary $\mathcal{A}$ that can forge our scheme. We will show how $\mathcal{B}$ can either find a collision on H_1 or forge the signature scheme S_{SIG}. $\mathcal{B}$ keeps a list L_{sig} to maintain the list of queries made by $\mathcal{A}$ to the signcryption oracle.

First, S_{SIG} gives the public parameters $Params_{Sig}$ to $\mathcal{B}$. $\mathcal{B}$ then chooses an encryption scheme and gives $Params = (Params_{Enc}, Params_{Sig})$ to $\mathcal{A}$.

We will now show how the signcryption queries made by $\mathcal{A}$ are treated by $\mathcal{B}$.

1. Signcryption query: Input(m_i)
   $\rightarrow$ Choose a random string $r_i \in \mathcal{R}$
   $\rightarrow$ Compute $H_1(m_i, r_i)$, say h_{1i}
   $\rightarrow$ Give h_{1i} as an input to signature scheme S_{SIG}. Let its output be σ_i
   $\rightarrow$ Compute $ENC(r_i, PK_{Rec}, Params_{Enc})$. Let its output be c_i'
   $\rightarrow$ Compute $H_2(r_i, c_i', h_{1i}, \sigma_i)$. Let its output be h_{2i}
   $\rightarrow$ Compute $c_i = h_{2i} \oplus m_i$
   $\rightarrow$ Put $(m_i, c_i, c_i', h_{1i}, \sigma_i)$ into the list L_{Sig}
   $\rightarrow$ Send $\mathcal{C} = (c_i, c_i', h_{1i}, \sigma_i)$

Once this stage is over, $\mathcal{A}$ gives a forged ciphertext $C = (c, c', h_1, \sigma)$. The following cases arise:

1. $C^* = (c^*, c'^*, h_1, \sigma^*)$ has not been returned from Signcryption oracle for any c^*, c'^* and σ^*. In this case, $\mathcal{B}$ will return (h_1, σ) to the challenger $\mathcal{C}$.
2. $C^* = (c^*, c'^*, h_1, \sigma^*)$ has been returned from Signcryption oracle for some c^*, c'^* and σ^* (c^*, c'^* and σ^* may be equal to c, c' and σ respectively). Let
   $m = \text{DSC}\ (C, SK_{Rec}, PK_{Sen}, Params)$,
   $m^* = \text{DSC}(C^*, SK_{Rec}, PK_{Sen}, Params)$,
   $r = \text{DEC}(c', SK_{Rec}, PK_{Rec})$ and
   $r^* = \text{DEC}(c'^*, SK_{Rec}, PK_{Rec})$.
   Now, the following two cases arise:
   (a) $m^* \neq m$. In this case, $h_1 = H_1(m^*, r^*) = H_1(m, r)$. Thus a collision obtained on H_1.
   (b) $m^* = m$. By definiton of fM-EUF-CMA, such case will not arise.

Formally, $\mathcal{B}$ runs the following algorithm to respond to the challenger $\mathcal{C}$.

– Algorithm:
  $\rightarrow$ Designcryption($\mathcal{C}, SK_{Rec}, PK_{Sen}, Param$). Let its output be m
  $\rightarrow$ Search $(m_j, c_j, c_j', h_1, \sigma_j)$ in L_{Sig}
  $\rightarrow$ If exists
  $\ldots \rightarrow$ Calculate $DEC(c_j', SK_{Rec}, Params_{ENC})$. Let its output be r_j
  $\ldots \rightarrow$ Calculate $DEC(c', SK_{Rec}, Params_{ENC})$. Let its output be r
  $\ldots \rightarrow$ Return (m, r) and (m_j, r_j)
  $\rightarrow$ Else
  $\ldots \rightarrow$ Return (h_1, σ)

Let

– E_{H_1} be the event of finding a collision for H_1
– E_{Sig} be the event of finding a valid message-signature pair in S_{SIG}

From case 1 and 2, it is clear that whenever $\mathcal{A}$ produces a forged ciphertext during the game of fM-EUF-CMA, $\mathcal{B}$ either finds a collision on H_1 or produces a forged message-signature pair on S_{SIG} during the game of EUF-CMA. Formally,

$\Pr(E_{H_1}) + \Pr(E_{Sig}) \geq \mathcal{A}dv(\mathcal{A})$
or,

$$\mathcal{A}dv(\mathcal{A}) \leq \Pr(\text{Collision on } H_1) + \Pr(\text{forging } S_{SIG})$$