Constructions Secure Against Receiver Selective Opening and Chosen Ciphertext Attacks

Dingding Jia[1,2,3(✉)], Xianhui Lu[1,2,3], and Bao Li[1,2,3]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, CAS, Beijing, China
{ddjia,xhlu,lb}@is.ac.cn
[2] Data Assurance and Communication Security Research Center,
CAS, Beijing, China
[3] University of Chinese Academy of Sciences, Beijing, China

Abstract. In this paper we study public key encryption schemes of indistinguishability security against receiver selective opening (IND-RSO) attacks, where the attacker can corrupt some receivers and get the corresponding secret keys in the multi-party setting. Concretely:

- We present a general construction of RSO security against chosen ciphertext attacks (RSO-CCA) by combining any RSO secure scheme against chosen plaintext attacks (RSO-CPA) with any regular CCA secure scheme, along with an appropriate non-interactive zero-knowledge proof.
- We show that the leakage-resistant construction given by Hazay *et al.* in Eurocrypt 2013 from weak hash proof system (wHPS) is RSO-CPA secure.
- We further show that the CCA secure construction given by Cramer and Shoup in Eurocrypt 2002 based on the universal HPS is RSO-CCA secure, hence obtain a more efficient paradigm for RSO-CCA security.

Keywords: Receiver selective opening · Chosen ciphertext security · Hash proof system

1 Introduction

Indistinguishability against chosen plaintext and chosen ciphertext attacks (IND-CPA, IND-CCA) are widely accepted security notions for public key encryption (PKE). However, in the multi-party situation, when attacks such as selective opening [7,11] are possible, the above security requirements are not enough.

Generally, in selective opening attacks the adversary may corrupt a fraction of parties and get the plaintext messages together with internal randomness for

This work is Supported by the National Basic Research Program of China (973 project) (No. 2013CB338002), the National Nature Science Foundation of China (No. 61502484, No. 61379137, No. 61572495).

H. Handschuh (Ed.): CT-RSA 2017, LNCS 10159, pp. 417–431, 2017.
DOI: 10.1007/978-3-319-52153-4_24

encryption or decryption, while it is hoped that messages for uncorrupted parties remain protected. The notion of selective opening attacks is considered in two settings: sender selective opening (SSO), where part of senders are corrupted and messages together with randomness for encryption are revealed; and receiver selective opening (RSO), where part of receivers are corrupted and messages together with secret keys for decryption are revealed [8].

Formal study of selective opening in PKE scenario was initiated by Bellare, Hofheinz and Yilek [4,5] in 2009. They gave rigorous definitions with two styles: indistinguishability-based (IND) and simulation-based (SIM). Considering that in the selective opening scenario, part of random coins or secret keys are opened, whether the ciphertext is consistant with the plaintext can be checked. In security proof this restricts the way how the target ciphertext generated, thus whether the ordinary IND security implies SO security and relations of SO security of different styles attracts much attention [1,3,12,21–23,31].

Earlier constructions of SO security either depended on erasures, updating secret keys, with long secret keys or were in the random oracle model [7,8,30]. As to the result in the random oracle model, Heuer *et al.* [17] proved that the practical schemes RSA-OAEP and DHIES were SIM-SSO-CCA secure. Next we review constructions that are stateless, non-interactive and without erasures in the standard model.

For constructions secure in the SSO setting a lot of works have been done in recent years [4,13,17–19,27–29]. Up to now constructions secure in the RSO setting [8,23] are relatively less, and these constructions are only RSO-CPA secure. In this paper we will focus on the constructions that are secure against RSO of the indistinguishability style and CCA attacks simultaneously.

1.1 Our Contribution

In this paper we show the existence of IND-RSO-CCA secure schemes by giving a construction from a variant of the Noar-Yung paradigm [6]. The construction is a combination of any IND-RSO-CPA secure scheme, any IND-CCA secure scheme and an appropriate non-interactive zero-knowledge proof (NIZK). And we prove that the leakage-resistant construction from weak hash proof systems (wHPS) in [20] is actually IND-RSO-CPA secure. For more efficient constructions, we prove that the Cramer-Shoup paradigm [9,10] from universal HPS is IND-RSO-CCA secure. In the following we outline the main idea of the construction.

To modify an IND-RSO-CPA secure scheme to be IND-RSO-CCA secure, one should handle decryption queries appropriately. We observe that when applying the Noar-Yung paradigm (or its variant), it is possible to keep secret keys unchanged by taking only the first copy of the secret key of the IND-RSO-CPA secure scheme as the secret key for the whole encryption scheme. Our first construction, which is constructed from an IND-RSO-CPA secure scheme, an IND-CCA secure scheme, an appropriate NIZK and a one-time signature, is inspired by the paradigm to achieving key-dependent message security against chosen ciphertext attacks (KDM-CCA) [6]. The proof sketch is shown in Fig. 5.

Besides, we prove the IND-RSO-CPA security for the leakage-resistant construction from wHPS given by Hazay *et al.* [20]. Since wHPS can be constructed from any CPA secure scheme, our result shows that IND-RSO-CPA secure PKE can be built from any IND-CPA secure PKE. Considering that IND-CCA secure PKE can be get from any IND-CPA secure PKE and an appropriate NIZK, we get that IND-RSO-CCA security can be built from any IND-CPA, an appropriate NIZK and a one-time signature. Generally speaking, a wHPS is a key encapsulation mechanism (KEM) along with a fake encapsulation algorithm. The fake encapsulation algorithm can generate a fake ciphertext, which is indistinguishable from the real ciphertext even given the secret key and is non-committing to any message when given the public key. In fact, the construction from wHPS, which adds to the encryption and decryption algorithm a bitwise XOR with the message, is IND-RSO-CPA secure. The security proof is straightforward, since when the adversary gets fake ciphertexts, messages are completely hidden, while fake ciphertexts are indistinguishable from real ciphertexts.

Although the framework we give above implies the existence of IND-RSO-CCA secure PKE, the use of NIZK makes it less efficient. In the final part, we prove that the construction from universal hash proof system (HPS) [9], which is more efficient, is IND-RSO-CCA secure. Here we give a general explaination. Hazay *et al.* demonstrated that smooth HPS implies tNCER, which leads to IND-RSO-CPA security [21]. Although the CCA construction from universal HPS adds elements in secret key for ciphertext verification compared with construction for CPA security, this does not affect the non-committing property, for the simulator is able to open messages along with secret keys which it holds.

One may notice that constructions in this paper can only achieve single-message security, while a more reliable requirement for practice is security for multi-message. In the full version [24] we give a reduction from multi-message security to single-message case through a hybrid argument. The reduction leads to a security loss related to the number of messages. We leave constructions that are secure for multi-messages with a tight reduction as an open problem.

Organization. The rest of our paper is organized as follows: in Sect. 2 we give definitions and preliminaries; in Sect. 3 we give a variant of the Noar-Yung paradigm to build IND-RSO-CCA secure encryption and prove that the leakage-resistant construction given by Hazay *et al.* from wHPS is IND-RSO-CPA secure; in Sect. 4 we prove that the construction in [9] is IND-RSO-CCA secure.

2 Preliminaries and Definitions

2.1 Preliminaries

Notations. In this paper we use PPT to represent probabilistic polynomial time for short. Let $[n]$ be the set of $\{1, 2, ..., n\}$. $a \leftarrow A$ is to denote choosing a random element from A when A is a set, and to denote picking a uniformly distributed randomness, running A with the randomness and assigning the output to a when A is a PPT algorithm. we use the lower case boldface to denote vectors. $Enc(\boldsymbol{pk}, \boldsymbol{m}) := (Enc(pk_1, m_1), ..., Enc(pk_n, m_n))$ when $\boldsymbol{pk}, \boldsymbol{m}$ are vectors of dimension n. The statistical distance of two distributions $\mathcal{X}, \mathcal{Y}$ is defined as $SD(\mathcal{X}, \mathcal{Y}) := \frac{1}{2}\Sigma_x|\Pr[\mathcal{X} = x] - \Pr[\mathcal{Y} = x]|$.

Besides efficiently samplable, the message space is required to be efficiently conditional resamplable to accompany the security definition we will give later.

Definition 1 (Efficiently Conditional Resamplable [4]). *Let dist be a joint distribution over $\mathbb{M}^n$, where $\mathbb{M}$ is the message space, then dist is efficiently conditional resamplable if there is a PPT algorithm Redist such that for any $I \subset [n]$ and any $\mathbf{m}_I := (m_i)_{i\in I}$, where $\mathbf{m} = (m_i)_{i\in[n]}$ is sampled from dist, the output $\mathbf{m}' \leftarrow Redist(\mathbf{m}_I)$ satisfies that $\mathbf{m}'$ is distributed according to dist and $m'_i = m_i$ for $i \in I$.*

2.2 Security Definitions

Public Key Encryption (PKE). A PKE scheme supported ciphertexts with labels consists of three algorithms: $Keygen(1^\lambda) \rightarrow (pk, sk)$, $Enc(pk, m, l) \rightarrow c$, $Dec(sk, c, l) \rightarrow m$ or $\perp$, where $Keygen$ is the key generation algorithm, Enc is the encryption algorithm with label l and Dec is the decryption algorithm.
Correctness. A PKE scheme satisfies correctness, if for all $(pk, sk) \leftarrow Keygen(1^\lambda)$, $m \in \mathbb{M}$, $Dec(sk, Enc(pk, m, l), l) = m$.

Clearly, an ordinary PKE scheme can be seen as a PKE scheme with empty label spaces.

Security. Here we give the definition of indistinguishability based security against receiver selective opening chosen ciphertext attacks (IND-RSO-CCA) as in [21] and IND-CCA security definition for ciphertexts with labels in Fig. 1. As in [4,19], we require the message space be efficiently conditional resamplable. The security experiment proceeds as follows:

Note that in $Exp^{\text{ind-rso-cca}}(\mathcal{A})$, the decryption query is of the form (c, j) satisfying that $c \neq c^*_j$, and is answered by $Dec(sk_j, c)$. And after the adversary gets $\boldsymbol{sk_I}$, it is required that $j \notin I$. The advantage is defined as $Adv_{\mathcal{A}}^{\text{IND-RSO-CCA}} =$

```
Experiment. $Exp^{\text{ind-rso-cca}}(\mathcal{A})$:
$b \leftarrow \{0,1\}$
$(\boldsymbol{pk}, \boldsymbol{sk}) := (pk_i, sk_i)_{i\in[n]} \leftarrow Setup(1^\lambda)$
$(dist, Redist, state_1) \leftarrow \mathcal{A}^{Dec(\cdot,\cdot)}(\boldsymbol{pk})$
$\boldsymbol{m_0} \leftarrow dist$
$\boldsymbol{c^*} \leftarrow Enc(\boldsymbol{pk}, \boldsymbol{m_0})$
$(I, state_2) \leftarrow \mathcal{A}^{Dec(\cdot,\cdot)}(\boldsymbol{c^*}, state_1)$
$\boldsymbol{m_1} \leftarrow Redist(\boldsymbol{m_{0I}})$
$b' \leftarrow \mathcal{A}^{Dec(\cdot,\cdot)}(\boldsymbol{sk_I}, \boldsymbol{m_b}, state_2)$
Return 1 if $b' = b$ and 0 else.
```

```
Experiment. $Exp^{\text{ind-cca}}(\mathcal{A})$:
$b \leftarrow \{0,1\}$
$(pk, sk) \leftarrow Setup(1^\lambda)$
$(m_0, m_1, l^*, state_1) \leftarrow \mathcal{A}^{Dec(\cdot,\cdot)}(pk)$
$c^* \leftarrow Enc(pk, m_b, l^*)$
$b' \leftarrow \mathcal{A}^{Dec(\cdot,\cdot)}(c^*, state_1)$
Return 1 if $b' = b$ and 0 else .
```

Fig. 1. The IND-RSO-CCA and IND-CCA experiment

$\left|2\Pr[Exp^{\text{ind-rso-cca}}(\mathcal{A}) = 1] - 1\right|$. In $Exp^{\text{ind-cca}}(\mathcal{A})$, the decryption query is of the form (c, l) such that $(c, l) \neq (c^*, l^*)$, where l is a label, and the query is answered by $Dec(sk, c, l)$. The advantage is defined as $Adv_{\mathcal{A}}^{\text{IND-CCA}} = \left|2\Pr[Exp^{\text{ind-cca}}(\mathcal{A}) = 1] - 1\right|$. When omitting the decryption oracle, the above experiment gives a definition of IND-RSO-CPA and IND-CPA security respectively.

Definition 2 (IND-RSO-CCA/CPA Security). *A PKE scheme is IND-RSO-CCA secure if for any PPT adversary $\mathcal{A}$, $Adv_{\mathcal{A}}^{\text{IND-RSO-CCA}}$ is negligible in λ. And it is IND-RSO-CPA secure if for any PPT adversary $\mathcal{A}$, $Adv_{\mathcal{A}}^{\text{IND-RSO-CPA}}$ is negligible in λ. IND-CCA/CPA security are defined similarly.*

One-Time Signature. A signature scheme consists of three PPT algorithms satisfying that for all: $Sig.Kg(1^\lambda) \to (vk, sigk), m \in \mathbb{M}, Ver(vk, m, Sign(sigk, m)) = 1$, where $Sig.Kg$ is the key generation algorithm, $Sign$ is the signature algorithm and Ver is the verification algorithm.

Security. Here we give the security notion of strong existential unforgeability under one-time chosen message attack in the following experiment between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$ (Fig. 2):

Definition 3 (One-time Unforgeable Security). *A signature scheme is strongly existential unforgeable under one-time chosen message attack if for any PPT adversary $\mathcal{A}$, $Adv_{\mathcal{A}}^{ots} := \Pr[Exp_{sig}^{uf\text{-}ot}(\mathcal{A}) = 1]$ is negligible in λ.*

2.3 Non-interactive Zero-Knowledge Proofs

Let R be a binary relation that is efficiently computable. Let $\mathcal{L} := \{x : \exists w,\ s.t.\ (x, w) \in R\}$. A non-interactive zero-knowledge (NIZK) proof system for R consists of three PPT algorithms $(CRSGen, P, V)$ satisfying the completeness property such that: for all $\mathfrak{C} \leftarrow CRSGen$, all $(x, w) \in R$, and $\mathfrak{p} \leftarrow P(\mathfrak{C}, x, w)$, $V(\mathfrak{C}, x, \mathfrak{p}) = 1$ where $CRSGen$ generates a common reference string (CRS), P is the proof algorithm and V is the verification algorithm.

```
Experiment. $Exp_{\text{sig}}^{\text{uf-ot}}(\mathcal{A})$:
$(vk, sigk) \leftarrow Sig.kg(1^\lambda)$
$(m, st) \leftarrow \mathcal{A}(vk)$
$\sigma \leftarrow Sign(sigk, m)$
$(m', \sigma') \leftarrow \mathcal{A}(st, \sigma)$
if $(m', \sigma') \neq (m, \sigma)$ and $Ver(vk, m', \sigma') = 1$, outputs 1, and 0 else
```

Fig. 2. One-time unforgeable for signatures

Definition 4 (NIZK [2,14]). *$(CRSGen, P, V)$ is an NIZK proof system for R if it satisfies the following properties:*

Computational Soundness: *For any PPT $\mathcal{A}$, $Adv^{cs}_{nizk,\mathcal{A}} = \Pr[\mathcal{A}(\mathfrak{C}) \rightarrow (x, \mathfrak{p}) \wedge x \notin \mathcal{L} \wedge V(\mathfrak{C}, x, \mathfrak{p}) = 1]$ is negligible, where $\mathfrak{C} \leftarrow CRSGen$ is given to $\mathcal{A}$.*

Computational Zero-knowledge: *There exists a simulator $\mathcal{S}$ such that for any PPT adversary $\mathcal{A}$, $Adv^{czk}_{nizk,\mathcal{A}} = |\Pr[Exp^{real}(\mathcal{A}) = 1] - \Pr[Exp^{sim}(\mathcal{A}) = 1]|$ is negligible, where $Exp^{real}(\mathcal{A})$ and $Exp^{sim}(\mathcal{A})$ are defined in Fig. 3, in which ϵ denotes an empty string and $\mathcal{E}$ denotes an empty set.*

```
Experiment. $Exp^{\mathrm{real}}(\mathcal{A})$:
$\mathfrak{C} \leftarrow CRSGen,\ st = \epsilon,\ \mathfrak{P} = \mathcal{E}$
for $i = 1, ..., n$
$\mathcal{A}(\mathfrak{C}, st, \mathfrak{P}) \rightarrow (x_i, w_i, st_i)$
$P(\mathfrak{C}, x_i, w_i) \rightarrow \mathfrak{p}_i$
$st \leftarrow st_i,\ \mathfrak{P} \leftarrow \mathfrak{P} \cup \mathfrak{p}_i$
end for
$b \leftarrow \mathcal{A}(st, \mathfrak{P})$
outputs $b$
```

```
Experiment. $Exp^{\mathrm{sim}}(\mathcal{A})$:
$(\mathfrak{C}, t) \leftarrow \mathcal{S},\ st = \epsilon,\ \mathfrak{P} = \mathcal{E}$
for $i = 1, ..., n$
$\mathcal{A}(\mathfrak{C}, st, \mathfrak{P}) \rightarrow (x_i, w_i, st_i)$
$\mathcal{S}(t, x_i) \rightarrow \mathfrak{p}_i$
$st \leftarrow st_i,\ \mathfrak{P} \leftarrow \mathfrak{P} \cup \mathfrak{p}_i$
end for
$b \leftarrow \mathcal{A}(st, \mathfrak{P})$
outputs $b$
```

Fig. 3. Computational zero-knowledge

Loosely speaking, CZK means that with the help of the secret information t generated with $\mathfrak{C}$, the simulator $\mathcal{S}$ can produce a proof that is indistinguishable from the real proof without the witness for $x \in \mathcal{L}$. For the construction in this paper, although only one message is encrypted for each public key, there are multi public keys, the one-time definition of computational zero-knowledge given by Blum *et al.* [2] is not enough.

3 An IND-RSO-CCA Secure Construction

In this section, we give an IND-RSO-CCA secure construction analogous to that in [6] with the following building blocks: a PKE $\mathbf{E}_1$ with IND-RSO-CPA security, a regular CCA secure PKE $\mathbf{E}_2$ that supports ciphertexts with labels, an NIZK proof system for the language consisting of the set of all pairs that encrypt the same message using $\mathbf{E}_1$ and $\mathbf{E}_2$, and a strong existential unforgeable one-time signature scheme. Then we prove that the construction from wHPS [20] is IND-RSO-CPA secure.

3.1 Preliminaries for Section 3

Tweaked Non-committing Encryption for Receivers (tNCER). In [21], Hazay *et al.* defined tNCER and proved that a tNCER is IND-RSO-CPA secure. A tweaked PKE (tPKE) consists of five algorithms $(tKeygen, tEnc, tEnc^*, tDec, tOpen)$, where $(tKeygen, tEnc, tDec)$ form a regular PKE and the tweaked encryption algorithm $tEnc^*$ outputs a fake ciphertext $c^* \leftarrow tEnc^*(pk, sk, m)$ and the (possibly inefficient)open algorithm $tOpen$ outputs a secret key $sk^* \leftarrow tOpen(pk, c^*, m)$, satisfying that $tDec(sk^*, c^*) = m$.

```
Experiment. $Exp_{\text{tpke}}^{\text{ind-tcipher}}(\mathcal{A})$:
$b \leftarrow \{0,1\}$
$(pk, sk) \leftarrow tKeygen(1^\lambda)$
$(m, st) \leftarrow \mathcal{A}(pk)$
$c_0 \leftarrow tEnc(pk, m)$
$c_1 \leftarrow tEnc^*(pk, sk, m)$
$b' \leftarrow \mathcal{A}(sk, c_b, st)$
if $b = b'$, outputs 1, else outputs 0
```

```
Experiment. $Exp_{\text{tpke}}^{\text{ind-tncer}}(\mathcal{A})$:
$b \leftarrow \{0,1\}$
$(pk, sk_0) \leftarrow tKeygen(1^\lambda)$
$(m, st) \leftarrow \mathcal{A}(pk)$
$c_0 \leftarrow tEnc^*(pk, sk_0, m)$
$m' \leftarrow \mathbb{M}$
$c_1 \leftarrow tEnc^*(pk, sk_0, m')$
$sk_1 \leftarrow tOpen(pk, c_1, m)$
$b' \leftarrow \mathcal{A}(sk_b, c_b, st)$
if $b = b'$, outputs 1, else outputs 0
```

Fig. 4. Tweaked NCER

Definition 5 *(tNCER). A tPKE is a tweaked NCER (Fig. 4) if:*

- *for any PPT adversary $\mathcal{A}$, $Adv_{tpke,\mathcal{A}}^{ind\text{-}tcipher} := |2\Pr[Exp_{tpke}^{ind\text{-}tcipher}(\mathcal{A}) = 1] - 1|$ is negligible.*
- *for any unbounded adversary $\mathcal{A}$, $Adv_{tpke,\mathcal{A}}^{ind\text{-}tncer} := |2\Pr[Exp_{tpke}^{ind\text{-}tncer}(\mathcal{A}) = 1] - 1|$ is negligible.*

Weak Hash Proof System (wHPS). Weak hash proof system, which can be seen as a generalization of HPS, was proposed by Hazay *et al.* to provide leakage resistant security from CPA secure schemes [20]. Here we give a brief review. A wHPS is an ordinary KEM in addition with a fake encryption algorithm Enc^* that takes as input pk, outputs an invalid ciphertext. $c^* \leftarrow Enc^*(pk)$.

It should satisfy indistinguishability and smoothness properties.

Indistinguishability. Given $(pk, sk) \leftarrow Keygen(1^\lambda)$, any PPT adversary $\mathcal{A}$ cannot distinguish a valid ciphertext from an invalid ciphertext. That is, for any PPT adversary $\mathcal{A}$, $Adv_{\mathcal{A},\text{wHPS}}^{\text{CI}}$ is negligible, where

$$\begin{aligned} Adv_{\mathcal{A},\text{wHPS}}^{\text{CI}} = |\Pr[&\mathcal{A}(pk, sk, c|(c, K) \leftarrow Enc(pk)) = 1] \\ &- \Pr[\mathcal{A}(pk, sk, c^*|c^* \leftarrow Enc^*(pk)) = 1]|. \end{aligned}$$

Smoothness. For any invalid ciphertext c^*, the distribution of (pk, c^*, K^*) and (pk, c^*, K) are identical, where $K^* = Dec(sk, c^*)$ and K is chosen randomly from the session key space.

3.2 Construction

Let $\mathbf{E}_1 := (Keygen_1, Enc_1, Dec_1)$ be IND-RSO-CPA secure, and $\mathbf{E}_2 := (Keygen_2, Enc_2, Dec_2)$ be IND-CCA secure and supports ciphertext with labels, $\mathbf{S} := (Sig.Kg, Sign, Ver)$ be strong existential unforgeable under one-time chosen message attack, $\mathcal{L}_{eq} := \{(c_1, c_2, l) | \exists m, r_1, r_2, s.t. c_1 = Enc_1(pk_1, m; r_1), c_2 = Enc_2(pk_2, m, l; r_2)\}$. Let $\mathbf{P} := (CRSGen, P, V)$ be an NIZK proof for $\mathcal{L}_{eq}$. The scheme is described as follows:

Keygen: Generate $(pk_i, sk_i) \leftarrow Keygen_i(1^\lambda)$ for $i = 1, 2$, run $CRSGen$ to get the CRS $\mathfrak{C}$ of the NIZK $\mathbf{P}$. Set $pk := (pk_1, pk_2, \mathfrak{C}), sk := sk_1$.

Enc: Generate $(vk, sigk) \leftarrow Sig.Kg(1^\lambda)$, randomly choose r_1, r_2 and compute $c_1 = Enc_1(pk_1, m; r_1), c_2 = Enc_2(pk_2, m, vk; r_2), \mathfrak{p} \leftarrow P(\mathfrak{C}, (c_1, c_2, vk), (m, r_1, r_2)), \sigma = Sign(Sigk, c_1 \| c_2 \| \mathfrak{p})$. The ciphertext $c = (vk, c_1, c_2, \mathfrak{p}, \sigma)$.

Dec: Verifies whether $V(\mathfrak{C}, c_1 \| c_2 \| vk, \mathfrak{p}) = 1$ and $Ver(vk, c_1 \| c_2 \| \mathfrak{p}, \sigma) = 1$, if both equations hold, output $m = Dec_1(sk, c_1)$, otherwise reject.

Correctness of the decryption algorithm is trivially follows from the completeness of NIZK, correctness of the signature scheme and correctness of the IND-RSO-CPA scheme.

Theorem 1. *Let $\mathbf{E}_1$ be IND-RSO-CPA secure, $\mathbf{E}_2$ be IND-CCA secure that supports ciphertext with labels, $\mathbf{S}$ be existential unforgeable under one-time chosen message attack, $\mathbf{P}$ be an NIZK proof for $\mathcal{L}_{eq}$, then the scheme constructed above is IND-RSO-CCA secure. Concretely,*

$$Adv_{pke}^{\text{IND-RSO-CCA}} \leq 2q(Adv_{nizk}^{cs} + nAdv_{sig}^{\text{uf-ot}}) + 2nAdv_{pke}^{cca} + 2Adv_{nizk}^{czk} + Adv_{pke}^{\text{IND-RSO-CPA}}$$

Proof. The proof is through a sequence of games depicted in Fig. 5, where the boxed item is the change from the former game.

Next we give the formal description of the games. Let W_i denote the event that the adversary outputs 1 in Game$_i$.

Game$_\mathbf{0}$: the real security game when $b = 0$.

Game$_\mathbf{1}$: the same as Game$_0$, except that when responding to a decryption query (c, j), the challenger computes $m = Dec_2(sk_{2j}, c_2)$ instead of $m = Dec_1(sk_{1j}, c_1)$. From the soundness property of $\mathbf{P}$, one can get that $\Pr[W_1] - \Pr[W_0]$ is negligible.

Game$_\mathbf{2}$: the same as Game$_1$, except that $\mathfrak{C}$ is generated by a simulator $\mathcal{S}$ and when responding to the encryption query $dist$, the challenger produce simulated proofs $\mathfrak{p} \leftarrow \mathcal{S}(t, (c_1, c_2, vk))$ instead of a real $\mathfrak{p}$. From the zero-knowledge property of $\mathbf{P}$, one can get that $\Pr[W_2] - \Pr[W_1]$ is negligible.

Game$_3$: the same as Game$_2$, except that when responding to a decryption oracle (c, j), where $c = (vk, c_1, c_2, \mathfrak{p}, \sigma)$, the challenger checks whether $vk = vk_j^*$, if the equation holds, then it just rejects. From the existential unforgeable property of $\mathbf{S}$, one can get that $\Pr[W_3] - \Pr[W_2]$ is negligible.

Game$_4$: the same as Game$_3$ except that when responding to the encryption query *dist*, the challenger samples $\boldsymbol{m_0} \leftarrow dist$, and random $\boldsymbol{m_R}$ from the message space, generates $(\boldsymbol{vk}, \boldsymbol{sigk}) \leftarrow Sig.Kg^n(1^\lambda)$, computes $\boldsymbol{c_1^*} = Enc_1(\boldsymbol{pk_1}, \boldsymbol{m_0}), \boldsymbol{c_2^*} = Enc_2(\boldsymbol{pk_2}, \boldsymbol{m_R}, \boldsymbol{vk^*})$, and other parts of the ciphertext vector as in Game$_3$. From the CCA security of $\mathbf{E}_2$, by a hybrid argument one can get that $\Pr[W_4] - \Pr[W_3]$ is negligible.

Game$_5$: the same as Game$_4$, except that in the open phase, the adversary resamples $\boldsymbol{m_1} \leftarrow Redist(\boldsymbol{m_{0I}})$ and responds with $(\boldsymbol{sk_I}, \boldsymbol{m_1})$. From the RSO-CPA security of $\mathbf{E}_1$, one can get that $\Pr[W_5] - \Pr[W_4]$ is negligible.

Game$_6$: the same as Game$_5$, except that when responding to the encryption query *dist*, the challenger computes $\boldsymbol{c_2} = Enc_2(\boldsymbol{pk_2}, \boldsymbol{m_0}, \boldsymbol{vk^*})$, with the real sampled message vector instead of randomly chosen one. From the CCA security of $\mathbf{E}_2$, one can get that $\Pr[W_6] - \Pr[W_5]$ is negligible.

Game$_7$: the same as Game$_6$, except that when responding to a decryption query (c, j), the challenger no longer rejects when $vk = vk_j^*$. From the existential unforgeable property of $\mathbf{S}$, one can get that $\Pr[W_7] - \Pr[W_6]$ is negligible.

Game$_8$: the same as Game$_7$, except that $\mathfrak{C}$ is normally generated and when responding to the encryption query *dist*, the challenger produce real proofs $\mathfrak{p}$. From the zero-knowledge property of $\mathbf{P}$, one can get that $\Pr[W_8] - \Pr[W_7]$ is negligible.

Game$_9$: the real security game when $b = 1$. From the soundness property of $\mathbf{P}$, one can get that $\Pr[W_9] - \Pr[W_8]$ is negligible.

Combining the above game sequences, we get that $\Pr[W_9] - \Pr[W_0]$ is negligible. □

Game	Enc	Dec	Open	Remarks
0	$\boldsymbol{m_0}, \boldsymbol{m_0}$,real $\mathfrak{p}$	$\boldsymbol{sk_1}$	$\boldsymbol{m_0}, \boldsymbol{sk_I}$	
1	$\boldsymbol{m_0}, \boldsymbol{m_0}$,real $\mathfrak{p}$	$\boxed{\boldsymbol{sk_2}}$	$\boldsymbol{m_0}, \boldsymbol{sk_I}$	soundness of **P**
2	$\boldsymbol{m_0}, \boldsymbol{m_0}, \boxed{\text{fake } \mathfrak{p}}$	$\boldsymbol{sk_2}$	$\boldsymbol{m_0}, \boldsymbol{sk_I}$	NIZK of **P**
3	$\boldsymbol{m_0}, \boldsymbol{m_0}$,fake $\mathfrak{p}$	$\boldsymbol{sk_2}, \boxed{\text{reject } vk^*}$	$\boldsymbol{m_0}, \boldsymbol{sk_I}$	unforgeable Signature **S**
4	$\boldsymbol{m_0}, \boxed{\boldsymbol{m_R}}$,fake $\mathfrak{p}$	$\boldsymbol{sk_2}$,reject vk^*	$\boldsymbol{m_0}, \boldsymbol{sk_I}$	cca security of $\mathbf{E}_2$
5	$\boldsymbol{m_0}, \boldsymbol{m_R}$,fake $\mathfrak{p}$	$\boldsymbol{sk_2}$,reject vk^*	$\boxed{\boldsymbol{m_1}, \boldsymbol{sk_I}}$	rso-cpa security of $\mathbf{E}_1$
6	$\boldsymbol{m_0}, \boxed{\boldsymbol{m_0}}$,fake $\mathfrak{p}$	$\boldsymbol{sk_2}$,reject vk^*	$\boldsymbol{m_1}, \boldsymbol{sk_I}$	cca security of $\mathbf{E}_2$
7	$\boldsymbol{m_0}, \boldsymbol{m_0}$,fake $\mathfrak{p}$	$\boldsymbol{sk_2}, \boxed{\text{no reject } vk^*}$	$\boldsymbol{m_1}, \boldsymbol{sk_I}$	unforgeable Signature **S**
8	$\boldsymbol{m_0}, \boldsymbol{m_0}, \boxed{\text{real } \mathfrak{p}}$	$\boldsymbol{sk_2}$,	$\boldsymbol{m_1}, \boldsymbol{sk_I}$	NIZK of **P**
9	$\boldsymbol{m_0}, \boldsymbol{m_0}$,real $\mathfrak{p}$	$\boxed{\boldsymbol{sk_1}}$	$\boldsymbol{m_1}, \boldsymbol{sk_I}$	soundness of **P**

Fig. 5. Game transform for RSO-CCA security from RSO-CPA security

3.3 IND-RSO-CPA Secure PKE from wHPS

Up to now there are instantiations of RSO-CPA secure PKE [21], CCA secure scheme with labeled ciphertext [6], NIZK for equal message relations [6,16], one-time signatures [15]. Here we prove that the leakage-resistant construction from wHPS [20] is IND-RSO-CPA secure. Since in [20] Hazay *et al.* showed that wHPS can be realized from CPA secure PKE schemes, our result implies that IND-RSO-CPA secure PKE can be constructed from any IND-CPA secure PKE.

Lemma 1 **([21]).** *For any PPT adversary $\mathcal{A}$ attacking tPKE in the IND-RSO-CPA scheme, there exists a PPT adversary $\mathcal{B}$ and an unbounded adversary $\mathcal{C}$, such that $Adv_{tpke}^{ind\text{-}rso\text{-}cpa}(\mathcal{A}) \leq 2n(Adv_{tpke}^{ind\text{-}tcipher}(\mathcal{B}) + Adv_{tpke}^{ind\text{-}tncer}(\mathcal{C}))$.*

Construction. Next we show that the PKE constructed from wHPS [20] is a tNCER. The scheme is described as follows.

$tKeygen(1^\lambda)$: The key generation algorithm is the generation algorithm of wHPS. $(pk, sk) \leftarrow wHPS.Keygen(1^\lambda)$.

$tEnc(pk, m)$: $c = (c_1, c_2)$, where $(c_1, K) \leftarrow wHPS.Enc(pk), c_2 = K + m$, here we assume that the encrypted messages are in an additive group.

$tDec(sk, c)$: $K \leftarrow wHPS.Dec(sk, c_1), m \leftarrow c_2 - K$.

$tEnc^*(pk, sk, m)$: $c^* = (c_1^*, c_2^*), c_1^* \leftarrow wHPS.Enc^*(pk), K^* \leftarrow wHPS.Dec(sk, c_1^*)$,
$c_2^* = K^* + m$.

$tOpen(pk, c^*, m)$: Parse c^* as $c^* = (c_1^*, c_2^*)$, compute $K^* = c_2^* - m$, find an sk^* such that $wHPS.Dec(sk^*, c^*) = m$.

Correctness can be easily verified from the correctness property of wHPS. It is obvious that the decryption of a fake ciphertext c^* outputs the encrypted message m. Since c_1^* is an output of $wHPS.Enc^*(pk)$, from the smooth property of wHPS, $(pk, c_1^*, wHPS.Dec(sk, c_1^*))$ is distributed as (pk, c_1^*, K) for randomly chosen K. Hence for a given K^*, there exists a sk^* corresponding to pk such that $wHPS.Dec(sk^*, c_1^*) = K^*$, an unbounded algorithm can find it. The ciphertext indistinguishability of tPKE easily follows from the indistinguishability of wHPS. And the non-committing property for fake ciphertexts follows from the smoothness property of wHPS.

4 IND-RSO-CCA Secure PKE from Universal HPS

The construction of the above section implies the existence of IND-RSO-CCA secure scheme. However, due to the employment of NIZK (pairing), the construction is less efficient, and the ciphertext is not compact. In this section we prove that the compact and efficient CCA secure scheme in [9] based on HPS is IND-RSO-CCA secure.

4.1 Universal Hash Proof System

Projective Hash Family. Firstly we recall the concept of hash proof system (HPS) introduced by Cramer and Shoup [9]. A projective hash family consists of $(\varLambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$, where $\mathcal{X}, \mathcal{Y}, \mathcal{L}, \mathcal{W}, \mathcal{SK}, \mathcal{PK}$ are sets and $\mathcal{L} \subset \mathcal{X}$ is a language, Let $\varLambda$ be a family of hash functions indexed by $sk \in \mathcal{SK}$ mapping from $\mathcal{X}$ to $\mathcal{Y}$. Let μ be a polynomial time function mapping from $\mathcal{SK}$ to $\mathcal{PK}$. A hash family $\mathbf{H} = (\varLambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$ is projective if for all $sk \in \mathcal{SK}$, the action of $\varLambda_{sk}$ on $\mathcal{L}$ is determined by $\mu(sk)$.

Definition 6 (ϵ-smoothness [9]). *The projective hash family is ϵ-smooth if for randomly chosen $sk \leftarrow \mathcal{SK}$, $X \leftarrow \mathcal{X}\backslash\mathcal{L}, pk = \mu(sk)$, given pk, X, the distribution of $Y = \varLambda_{sk}(X)$ and randomly chosen $\tilde{Y} \in \mathcal{Y}$ are statistically indistinguishable,*

$$SD((pk, X, Y), (pk, X, \tilde{Y})) \leq \epsilon.$$

Definition 7 (ι-related ϵ-smoothness). *The projective hash family is ι-related ϵ-smooth if for ι randomly chosen $\boldsymbol{sk} = (sk_1, ..., sk_\iota) \leftarrow \mathcal{SK}^\iota$, $\boldsymbol{X} = (X_1, ..., X_\iota) \leftarrow (a\mathcal{L})^\iota, a \leftarrow \mathcal{X}\backslash\mathcal{L}$, compute $\boldsymbol{pk} = (\mu(sk_1), ..., \mu(sk_\iota))$, $\boldsymbol{Y} = (\varLambda_{sk_1}(X_1), ..., \varLambda_{sk_\iota}(X_\iota))$, for randomly chosen $\tilde{\boldsymbol{Y}} \in \mathcal{Y}^\iota$,*

$$SD((\boldsymbol{pk}, \boldsymbol{X}, \boldsymbol{Y}), (\boldsymbol{pk}, \boldsymbol{X}, \tilde{\boldsymbol{Y}})) \leq \epsilon.$$

ι-related ϵ-smoothness property can be easily deduced from the ordinary smoothness property of hash family with a hybrid proof argument.

As in [9], we introduce a finite set $\mathcal{E}$ to extend the sets $\mathcal{X}$ and $\mathcal{L}$ to define a universal$_2$ extended projective hash family $\mathbf{H} = (\varLambda, \mathcal{SK}, \mathcal{X} \times \mathcal{E}, \mathcal{L} \times \mathcal{E}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$.

Definition 8 (universal$_2$ [9,25]). *The extended projective hash family is universal$_2$ if for all $pk \in \mathcal{PK}$, $X_1, X_2 \in \mathcal{X}\backslash\mathcal{L}, E_1, E_2 \in \mathcal{E}$, $(X_1, E_1) \neq (X_2, E_2)$, for all $Y_1, Y_2 \in \mathcal{Y}$,*

$$\Pr[\varLambda_{sk}(X_2, E_2) = Y_2 | \mu(sk) = pk, \varLambda_{sk}(X_1, E_1) = Y_1] = \frac{1}{|\mathcal{Y}|}.$$

Subset Membership Problem (SMP). An SMP specifies an instance ensembles $\{I_n\}_n$ such that for each n, I_n specifies a distribution over instance $\varGamma = (\mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{R})$, where $\mathcal{X}, \mathcal{L}, \mathcal{W}$ are non-empty sets and $\mathcal{L} \subset \mathcal{X}$ and $\mathcal{R} \subset \mathcal{X} \times \mathcal{W}$ is a binary relation such that $x \in \mathcal{L}$ iff there exists a w satisfying $(x, w) \in \mathcal{R}$.

We assume that there are efficient algorithms to sample instances from I_n, elements from $\mathcal{X}$, $\mathcal{X}\backslash\mathcal{L}$ and elements L from $\mathcal{L}$ together with its witness $w \in \mathcal{W}$. Also we require that $\mathcal{X}, \mathcal{Y}$ being abelian groups (with computational symbol "+") and $\mathcal{L}$ being subgroup of $\mathcal{X}$.

Definition 9 (Subset Membership (SM) Problem [9]). *The advantage of an adversary $\mathcal{A}$ in breaking SMP is defined as:*

$$Adv_{\mathcal{A}}^{SM} = |\Pr[\mathcal{A}(\varGamma, Z_0) = 1] - \Pr[\mathcal{A}(\varGamma, Z_1) = 1]|,$$

where the probability is taken over the randomness of choosing instance Γ and elements Z_0, Z_1, the internal randomness of $\mathcal{A}$. We say that the SM problem is hard if for every PPT $\mathcal{A}$, $Adv_{\mathcal{A}}^{SM}$ is negligible.

Hash Proof System (HPS). An HPS associates each SM instance Γ with a projective hash family $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$. In addition, it provides PPT algorithms to choose $sk \in \mathcal{SK}$ and $X \in \mathcal{X}$ uniformly at random, PPT algorithm to compute $\mu(sk)$, and PPT algorithms $(Priv, Pub)$ to compute $\Lambda_{sk}(L)$ for $L \in \mathcal{L}$ with witness w :

$$\Lambda_{sk}(L) = Priv(sk, L) = Pub(\mu(sk), L, w).$$

HPS with Trapdoor. Following [25,26], we also require that the SM problem can be efficiently solved with a master trapdoor, which will be used not in the actual scheme but in the security proof. In fact, all known hash proof systems have such a trapdoor.

4.2 Construction

Let $\mathbf{H}_1 = (\Lambda_1, \mathcal{SK}_1, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}_1, \mathcal{PK}_1, \mu_1)$ be a smooth projective hash proof system, $\mathbf{H}_2 = (\Lambda_2, \mathcal{SK}_2, \mathcal{X} \times \mathcal{Y}_1, \mathcal{L} \times \mathcal{Y}_1, \mathcal{W}, \mathcal{Y}_2, \mathcal{PK}_2, \mu_2)$ be an extended universal$_2$ projective hash proof system. Public parameters are set as $pp = (\mathbf{H}_1, \mathbf{H}_2)$.

$Keygen(pp)$: The key generation algorithm chooses random secret key $sk_1 \leftarrow \mathcal{SK}_1, sk_2 \leftarrow \mathcal{SK}_2$ and computes the public key as $pk = (pk_1 = \mu_1(sk_1), pk_2 = \mu_2(sk_2))$.

$Enc(pk, m)$: The encryption algorithm samples random $L \in \mathcal{L}$ with witness w, and computes the ciphertext $c = (c_0, c_1, c_2)$ as:

$$c_0 = L, Y_1 = Pub(pk_1, L, w), c_1 = Y_1 + m, c_2 = Pub(pk_2, L, c_1, w).$$

$Dec(sk, c)$: The decryption algorithm first verifies whether $c_2 = Priv(sk_2, c_0, c_1)$, if the equation does not hold, it just rejects, else it computes the message as:

$$Y_1 = Priv(sk_1, c_0), m = c_1 - Y_1.$$

Correctness can be easily verified from the projective property of the HPS.

4.3 Security Proof

Theorem 2. *If $\boldsymbol{H}_1$ is a ϵ_1-smooth projective HPS with the corresponding SM problem hard, $\boldsymbol{H}_2$ is an extended universal$_2$ projective hash proof system with the same corresponding SM problem hard, then our PKE scheme is IND-RSO-CCA secure. Concretely,*

$$Adv_{\mathcal{A}}^{IND\text{-}RSO\text{-}CCA} \leq Adv_{\mathcal{B}}^{SM,HPS} + q\left(\frac{1}{(|\mathcal{X}| - |\mathcal{L}|) \cdot |\mathcal{Y}_1|} + \frac{1}{|\mathcal{Y}_2|}\right) + n\epsilon_1.$$

where q is the number of decryption queries, n is the number of key pairs.

Proof. A ciphertext c is invalid if $c_0 \notin \mathcal{L}$. The master trapdoor mt is used to solve the SM problem.

To prove the security of our scheme, we define a sequence of games whereby any PPT adversary can not tell the difference between consecutive games.

$Game_0$**:** the real security game.

$Game_1$**:** the same as $Game_0$ except that the challenge ciphertexts are generated using the secret keys. That is $Y_{i1}^* = Priv_1(sk_{i1}, c_{i0}^*), c_{i2}^* = Priv_2(sk_{i2}, c_{i0}^*, c_{i1}^*)$.

$Game_2$**:** the same as $Game_1$ except that the challenge ciphertexts are invalid. Concretely, $\{c_{i0}^*\}_{i\in[n]}$ are chosen uniformly from a random coset of $\mathcal{L}$, that is $a\mathcal{L}, a \leftarrow \mathcal{X}\backslash\mathcal{L}$.

$Game_3$**:** the same as $Game_2$ except that the decryption oracle rejects all queries (c, j) that satisfy $c_0 \notin \mathcal{L}$. This can be achieved with the help of the master trapdoor mt.

Let $Adv_{\mathcal{A}}^i$ denote $\mathcal{A}$'s advantage in $Game_i$ for $i = 0, 1, 2, 3$.

It is clear to see $Adv_{\mathcal{A}}^0 = Adv_{\mathcal{A}}^1$ from the projective property of HPS.

Lemma 2. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^1 - Adv_{\mathcal{A}}^2 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with advantage ϵ in solving the SM problem.*

Lemma 3. *$Adv_{\mathcal{A}}^2 - Adv_{\mathcal{A}}^3 \leq \epsilon$ if the projective HPS $\boldsymbol{H}_2$ satisfies the universal$_2$ property, where $\epsilon = q(\frac{1}{(|\mathcal{X}|-|\mathcal{L}|)\cdot|\mathcal{Y}_1|} + \frac{1}{|\mathcal{Y}_2|})$.*

Lemma 4. *$Adv_{\mathcal{A}}^3 \leq n\epsilon_1$, if the underlying projective HPS $\boldsymbol{H}_1$ is ϵ_1-smooth.*

Concrete proofs for Lemmas 2, 3 and 4 are deferred to the full version. □

Instantiations. The instantiations are the same as that in [9] from the DDH, DCR and QR assumptions.

Acknowledgments. We are grateful to Yamin Liu and Haiyang Xue for helpful discussions and advice. We also thank the anonymous reviewers of CT-RSA 2017 for their useful comments.

References

1. Bellare, M., Dowsley, R., Waters, B., Yilek, S.: Standard security does not imply security against selective-opening. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 645–662. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_38
2. Blum, M., Feldman, P., Micali, S.: Non-interactive zero-knowledge and its applications (extended abstract). In: STOC 1988, pp. 103–112 (1988)

3. Böhl, F., Hofheinz, D., Kraschewski, D.: On definitions of selective opening security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 522–539. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30057-8_31
4. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_1
5. Bellare, M., Yilek, S.: Encryption schemes secure under selective opening attack. IACR Cryptology ePrint Archive 2009, 101 (2009)
6. Camenisch, J., Chandran, N., Shoup, V.: A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_20
7. Canetti, R., Feige, U., Goldreich, O., Naor, M.: Adaptively secure multi-party computation. In: Twenty-Eighth Annual ACM Symposium on Theory of Computing, Proceedings of STOC 1995, pp. 639–648. ACM Press (1996)
8. Canetti, R., Halevi, S., Katz, J.: Adaptively-secure, non-interactive public-key encryption. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 150–168. Springer, Berlin (2005). doi:10.1007/978-3-540-30576-7_9
9. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002). doi:10.1007/3-540-46035-7_4
10. Cramer, R., Shoup, V.: Design and analysis of practical public-Key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Compt. **33**(1), 167–226 (2003)
11. Dwork, C., Naor, M., Reingold, O., Stockmeyer, L.: Magic functions. J. ACM **50**(6), 852–921 (2003)
12. Fuchsbauer, G., Heuer, F., Kiltz, E., Pietrzak, K.: Standard security does imply security against selective opening for Markov distributions. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 282–305. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49096-9_12
13. Fehr, S., Hofheinz, D., Kiltz, E., Wee, H.: Encryption schemes secure against chosen-ciphertext selective opening attacks. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 381–402. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_20
14. Feige, U., Lapidot, D., Shamir, A.: Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In: FOCS 1990, pp. 308–317 (1990)
15. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006). doi:10.1007/11935230_29
16. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78967-3_24
17. Heuer, F., Jager, T., Kiltz, E., Schäge, S.: On the selective opening security of practical public-key encryption schemes. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 27–51. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_2
18. Huang, Z., Liu, S., Qin, B., Chen, K.: Fixing the sender-equivocable encryption scheme in Eurocrypt 2010. In: INCOS, pp. 366–372 (2013)

19. Hemenway, B., Libert, B., Ostrovsky, R., Vergnaud, D.: Lossy encryption: constructions from general assumptions and efficient selective opening chosen ciphertext security. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 70–88. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25385-0_4
20. Hazay, C., López-Alt, A., Wee, H., Wichs, D.: Leakage-resilient cryptography from minimal assumptions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 160–176. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38348-9_10
21. Hazay, C., Patra, A., Warinschi, B.: Selective opening security for receivers. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 443–469. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_19
22. Hofheinz, D., Rupp, A.: Standard versus selective opening security: separation and equivalence results. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 591–615. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54242-8_25
23. Hofheinz, D., Rao, V., Wichs, D.: Standard security does not imply indistinguishability under selective opening. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 121–145. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53644-5_5
24. Jia, D., Lu, X., Li, B.: Constructions secure against receiver selective opening and chosen ciphertext attacks. IACR Cryptology ePrint Archive 2016, 1083 (2016)
25. Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_26
26. Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A new randomness extraction paradigm for hybrid encryption. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 590–609. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_34
27. Lai, J., Deng, R.H., Liu, S., Weng, J., Zhao, Y.: Identity-based encryption secure against selective opening chosen-ciphertext attack. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 77–92. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_5
28. Liu, S., Paterson, K.G.: Simulation-based selective opening CCA security for PKE from key encapsulation mechanisms. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 3–26. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_1
29. Liu, S., Zhang, F., Chen, K.: Public-key encryption scheme with selective opening chosen-ciphertext security based on the Decisional Diffie-Hellman assumption. Concurrency Comput. Pract. Experience **26**(8), 1506–1519 (2014)
30. Nielsen, J.B.: Separating random oracle proofs from complexity theoretic proofs: the non-committing encryption case. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 111–126. Springer, Heidelberg (2002). doi:10.1007/3-540-45708-9_8
31. Ostrovsky, R., Rao, V., Visconti, I.: On selective-opening attacks against encryption schemes. In: Abdalla, M., Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 578–597. Springer, Heidelberg (2014). doi:10.1007/978-3-319-10879-7_33