Hedged Nonce-Based Public-Key Encryption: Adaptive Security under Randomness Failures

Zhengan Huang[1], Junzuo Lai[2,3,⋆], Wenbin Chen[1], Man Ho Au[4], Zhen Peng[5], and Jin Li[1,⋆]

1. School of Computer Science, Guangzhou University, Guangzhou, China
`zhahuang.sjtu@gmail.com, cwb2011@gzhu.edu.cn, jinli71@gmail.com`
2. College of Information Science and Technology, Jinan University, Guangzhou, China
3. State Key Laboratory of Cryptology, Beijing, China
`laijunzuo@gmail.com`
4. Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
`csallen@comp.polyu.edu.hk`
5. Westone Cryptologic Research Center, Beijing, China
`peng.zhen@westone.com.cn`

Abstract. Nowadays it is well known that randomness may fail due to bugs or deliberate randomness subversion. As a result, the security of traditional public-key encryption (PKE) cannot be guaranteed any more. Currently there are mainly three approaches dealing with the problem of randomness failures: deterministic PKE, hedged PKE, and nonce-based PKE. However, these three approaches only apply to different application scenarios respectively. Since the situations in practice are dynamic and very complex, it's almost impossible to predict the situation in which a scheme is deployed, and determine which approach should be used beforehand.

In this paper, we initiate the study of hedged security for nonce-based PKE, which adaptively applies to the situations whenever randomness fails, and achieves the best-possible security. Specifically, we lift the hedged security to the setting of nonce-based PKE, and formalize the notion of chosen-ciphertext security against chosen-distribution attacks (IND-CDA2) for nonce-based PKE. By presenting two counterexamples, we show a separation between our IND-CDA2 security for nonce-based PKE and the original NBP1/NBP2 security defined by Bellare and Tackmann (EUROCRYPT 2016). We show two nonce-based PKE constructions meeting IND-CDA2, NBP1 and NBP2 security simultaneously. The first one is a concrete construction in the random oracle model, and the second one is a generic construction based on a nonce-based PKE scheme and a deterministic PKE scheme.

Keywords: hedged security, nonce-based public-key encryption, deterministic public-key encryption, randomness failures

[⋆] Corresponding author.

1 Introduction

Background. It is well known that randomness plays a key role in cryptography. For most cryptographic constructions, their security is guaranteed on condition that the random coins employed are uniformly and independently chosen. For example, IND-CCA security [19], one universally accepted security notion for PKE, requires that the randomness employed during the encryption is uniformly chosen and independent of any other elements. However, randomness may fail because of bugs or randomness subversion. Recently, it is well-known that the randomness failures are actual threats, and bring new challenges to cryptographic constructions and information security products.

As far as we know, there are mainly three kinds of PKE which have been proposed to provide good privacy under randomness failures. The first one is *deterministic PKE* (D-PKE) [1, 4, 9], where the encryption algorithm does not need to use any randomness for encryption, and its security is guaranteed on condition that the messages have high min-entropy. D-PKE was proposed to provide fast search on encrypted data at first. Since the encryption does not use randomness, D-PKE is an important class of PKE dealing with the subsequently revealed problem of randomness subversion. The second one is *hedged PKE* (H-PKE) [2, 5], which can be seen as an extension of D-PKE. For hedged PKE, the encryption algorithm is randomized, and its security is guaranteed only if the messages and the randomness *jointly* have high min-entropy. The third one is *nonce-based PKE* (N-PKE) [8], the encryption algorithm of which is randomized, and the messages can be arbitrarily chosen. For each encryption, instead of taking fresh randomness, the encryption algorithm takes a uniform seed, which can be used repeatedly, and a nonce as input. A significant benefit brought by N-PKE is that it's not necessary for the senders to generate fresh, uniform and independent randomness at every encryption. The security of N-PKE is guaranteed as long as either the seed is confidential and the message-nonce pairs do not repeat, or the seed is exposed but the nonces are unpredictable.

The above three approaches focus on different scenarios. D-PKE is only suitable for the situations that the messages have sufficient min-entropy. H-PKE applies to the situations that the messages and the randomness have jointly sufficient min-entropy. Generally speaking, both of these two approaches require that the messages are independent of the public keys. N-PKE just applies to the case that either the seed or the nonces can provide sufficient randomness. Besides these three kinds of P-

KE schemes, currently the most commonly used ones in practice are the traditional PKE schemes (i.e., the security is guaranteed assuming that the randomness is good, and the messages can be arbitrarily chosen), such as RSA [22, 18].

However, unfortunately none of the aforementioned approaches is able to provide good privacy in all application scenarios. The messages we want to encrypt regularly do not have sufficient min-entropy [12] and sometimes may depend on the public key, and the randomness may fail because of bugs or deliberate randomness subversion [15, 13]. These facts limit the application of D-PKE and H-PKE. On the other hand, N-PKE can provide good privacy only if either the seed or the nonces have sufficient min-entropy from the adversaries' point of view. If one uses N-PKE, when both the seed and the nonces do not have sufficient min-entropy, the security of the scheme cannot be guaranteed. These facts limit the application of N-PKE. More importantly, it's almost unrealistic to determine beforehand which kinds of PKE should be used because the situations in which the scheme is deployed are dynamic.

Hedged security for nonce-based PKE. In this paper, we formalize the notions of hedged security for nonce-based PKE, and provide some constructions. N-PKE schemes achieving our hedged security are able to adaptively apply to the situations whenever randomness fails, and achieve the best-possible security. Specifically, we formalize the notion of chosen-ciphertext security against chosen-distribution attacks (IND-CDA2) for N-PKE, which can be seen as the CCA-and-N-PKE version of the original IND-CDA security for PKE formalized in [2][1]. This security is guaranteed on condition that the seeds, the messages and the nonces have jointly sufficient min-entropy.

We separate our IND-CDA2 security notion and the security notion proposed in [8] for N-PKE (i.e., NBP1 and NBP2 security), by presenting two counterexamples. Our counterexamples actually show that even extending the original IND-CDA security (for H-PKE) to the nonce-based setting, IND-CDA security is still separated from NBP1/NBP2 security.

Since the original NBP1/NBP2 security and IND-CDA2 security do not imply each other, when we consider the security of N-PKE, we have to require that the N-PKE schemes achieve NBP1, NBP2 and IND-CDA2 security simultaneously. For simplicity, we call it HN-IND security.

[1] Very recently, Boldyreva, Patton and Shrimpton [10] formalized one CCA version of IND-CDA security for traditional PKE. There are some differences between their formalizations and ours. See Remark 2 for details.

In order to handle the potential problem of randomness failures, we recommend that one use HN-IND secure N-PKE if possible, and, especially, *employ a combination of a variety of things which do not repeat (e.g., the current time), and fresh, uniform and independent chosen randomness as nonce at every encryption* (and the seed can be reused). The reasons are as follows. If there are no randomness failures, the N-PKE schemes meet the universally accepted IND-CCA security. If some randomness failures present, the security which is as good as possible can be guaranteed. More specifically, if the randomness of the nonces is compromised, as long as the seed is uniformly chosen and confidential and the message-nonce pairs do not repeat, then NBP1 security guarantees that the schemes still achieve IND-CCA security. If the seed is exposed, but if the nonces are still unpredictable, then NBP2 security guarantees IND-CCA security. For the case that neither the seeds nor the nonces have sufficient min-entropy, as long as the seed-message-nonce tuples have sufficient min-entropy, and the messages are independent of the public key, then the N-PKE schemes achieve IND-CDA2 security, which is defined under chosen-ciphertext attacks and strictly stronger than IND-CDA security. We also note that for an extreme situation that both the seed and the nonces are arbitrarily determined by the adversaries, but the messages still have sufficient min-entropy, then the schemes are actually D-PKE schemes achieving adaptive IND security (i.e., the adversary is allowed to access to the encryption oracle adaptively multiple times) in the CCA setting.

We note that the HN-IND secure N-PKE is able to adaptively handle the above cases, and achieves IND-CCA security even if there are some randomness failures. It's not necessary to decide which kind of PKE (i.e., traditional PKE, H-PKE, N-PKE or D-PKE) should be used according to the specific cases beforehand.

Besides, in the setting of D-PKE, there is another kind of adaptive security notion proposed by Raghunathan, Segev and Vadhan (RSV) in [20], where the messages are allowed to depend on the public key, but an upper bound on the number of the message distributions is required. For completeness, we also formalize a similar version of IND-CDA2 security *for N-PKE*, and call it the RSV version of HN-IND security.

HN-IND secure constructions. In this paper we provide an N-PKE scheme achieving HN-IND security in the random oracle model (ROM). Our approach is from the ROM construction of N-PKE in [8]. We notice that in [8], the nonce-based PKE schemes were constructed with a building block called *hedged extractor*. There are two constructions of hedged extractor proposed in [8], where the first one is in the ROM, and the second one is in the standard model. We emphasize that *under the security of hedged extractor*, both of the N-PKE schemes based on these two hedged extractors respectively are *not* HN-IND secure. The reason is that the security of hedged extractor is guaranteed only if either the seed or the nonce has enough min-entropy. Therefore, it seems that all the *generic constructions* of N-PKE based on hedged extractors do not achieve HN-IND security.

We also provide a generic construction of HN-IND secure N-PKE. The main idea of our scheme is from [16], which is a combination of an N-PKE scheme and a D-PKE scheme. Our conclusion shows that if the underlying N-PKE scheme is NBP1 and NBP2 secure, and the D-PKE scheme is adaptively IND secure in the CCA setting and unique-ciphertext secure, then the construction is HN-IND secure. If both the underlying constructions are built in the standard model, then our construction achieves HN-IND security in the standard model.

Moreover, we show that both of the constructions achieve the RSV version of HN-IND security.

Related work. Deterministic PKE was formally introduced by Bellare, Boldyreva and O'Neill [1] in CRYPTO 2007. A security notion called PRIV for D-PKE was defined, and some PRIV secure ROM constructions were proposed in [1]. Later, several equivalent security notions were formalized in [4], including the IND security used in this paper. Some variants of PRIV/IND security or D-PKE also appeared [9, 11, 17, 20, 5], and more D-PKE constructions were proposed [14, 6, 5]. Wichs [23] pointed out that the fully IND security of D-PKE in the standard model can not be achieved under any single-stage assumption. Later with the help of UCE [6], Bellare and Hoang [5] gave the first fully IND secure D-PKE scheme in the standard model. Selective opening security for D-PKE was also formalized and achieved in the ROM [3, 16]. We note that the most commonly used security for D-PKE (i.e., PRIV or IND security) is a *non-adaptive* security notion. In other words, in the game defining the security, the adversary is allowed to make the challenge query only once.

Hedged PKE was introduced by Bellare et al. [2]. In [2], an *adaptive* security notion called IND-CDA, which is an extension of IND, is formalized, and a PKE scheme is called H-IND secure if it achieves IND-CPA and IND-CDA security simultaneously. Very recently, Boldyreva, Patton and Shrimpton [10] formalized the CCA version of IND-CDA security (which they named MMR-CCA security) for PKE with associated data. Both ROM constructions and standard-model constructions achieving fully H-IND security (i.e., the message-randomness pairs may be arbitrarily correlated) have been proposed [2, 5, 10]. The use of H-PKE in practice was explored in [21, 10].

Nonce-based PKE was introduced by Bellare and Tackmann in [8]. They formalized two security notions called NBP1 and NBP2, and showed ROM and standard-model constructions achieving both of the two security. Their constructions are based on a new primitive called hedged extractor. Nonce-based signatures was also defined and built in [8]. Recently, Hoang, Katz, O'Neill and Zaheri [16] formalized SOA security for N-PKE, and lifted the security notion to H-PKE. To the best of our knowledge, it's the first security notion for hedged N-PKE. But their security is defined in the SOA setting, and more importantly, it is a *non-adaptive* security notion. Furthermore, we note that their security notion is a *comparison*-based security (see [4]), and our IND-CDA2 security is an *indistinguishability*-based one. Informally, denote by *COM-CDA2 security* the HN-SO-CCA security formalized in [16] with the restriction that I is *empty* (i.e., the adversaries do not perform corruptions. We refer the readers to [16] for the details). Exploring the relations among COM-CDA2 security and the *non-adaptive version* of our IND-CDA2 security is an interesting topic for future research.

2 Preliminaries

Notations and conventions. Vectors are written in boldface, e.g., $\mathbf{x}$. For a vector $\mathbf{x}$, let $|\mathbf{x}|$ denote its length and $\mathbf{x}[i]$ denote its i^{th} component for $i \in [|\mathbf{x}|]$. For a finite set X (resp. a string x), let $|X|$ (resp. $|x|$) denote its size (resp. length). We extend the set membership notations to vectors. For any game $\mathbf{G}$ presented in this paper, denote by $\Pr[\mathbf{G}]$ the probability that the final output of $\mathbf{G}$ is 1.

Public-key encryption. A (general) public-key encryption (PKE) scheme is a tuple of PPT algorithms $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$. The key generation algorithm Kg, taking 1^k as input, generates a public/secret key pair (pk, sk). The encryption algorithm Enc, taking pk and message $m \in \{0,1\}^*$ as input, outputs a ciphertext c. The deterministic decryption algorithm Dec, taking sk and c as input, returns a value in $\{0,1\}^* \cup \{\perp\}$. Standard correctness is required, which means that for any valid message $m \in \{0,1\}^*$, $(pk, sk) \leftarrow \mathsf{Kg}(1^k)$ and $c \leftarrow \mathsf{Enc}(pk, m)$, $\mathsf{Dec}(sk, c) = m$ with overwhelming probability. For vectors $\mathbf{m}$, $\mathbf{r}$ with $|\mathbf{m}| = |\mathbf{r}|$, we denote by $\mathsf{Enc}(pk, \mathbf{m}; \mathbf{r}) := (\mathsf{Enc}(pk, \mathbf{m}[1]; \mathbf{r}[1]), \mathsf{Enc}(pk, \mathbf{m}[2]; \mathbf{r}[2]), \cdots, \mathsf{Enc}(pk, \mathbf{m}[|\mathbf{m}|]; \mathbf{r}[|\mathbf{m}|]))$.

```
Game $\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},A}(k)$
$(pk, sk) \leftarrow \mathsf{Kg}(1^k)$
$b \leftarrow \{0,1\}; C \leftarrow \emptyset$
$b' \leftarrow A^{\text{ENC},\text{DEC}}(pk)$
Return $(b' = b)$
```

```
ENC$(\mathbf{m}_0, \mathbf{m}_1)$
$\mathbf{c} \leftarrow \mathsf{Enc}(pk, \mathbf{m}_b)$
$C \leftarrow C \cup \mathbf{c}$
Return $\mathbf{c}$
```

```
DEC$(c)$
If $c \in C$, then
    Return $\perp$
$m \leftarrow \mathsf{Dec}(sk, c)$
Return $m$
```

```
Game $\mathbf{G}^{\text{de-ind}}_{\mathsf{DE},A}(k)$
$(pk, sk) \leftarrow \mathsf{DKg}(1^k)$; $b \leftarrow \{0,1\}$
$\mathcal{M} \leftarrow A_1(1^k)$
$(\mathbf{m}_0, \mathbf{m}_1) \leftarrow \mathcal{M}$; $\mathbf{c} \leftarrow \mathsf{DEnc}(pk, \mathbf{m}_b)$
$b' \leftarrow A_2(pk, \mathbf{c})$
Return $(b' = b)$
```

```
Game $\mathbf{G}^{\text{de-cca}}_{\mathsf{DE},A}(k)$
$(pk, sk) \leftarrow \mathsf{DKg}(1^k)$
$b \leftarrow \{0,1\}; C \leftarrow \emptyset$
$St \leftarrow A_1^{\text{ENC}}(1^k)$
$b' \leftarrow A_2^{\text{DEC}}(pk, St)$
Return $(b' = b)$
```

```
ENC$(\mathcal{M})$
$(\mathbf{m}_0, \mathbf{m}_1) \leftarrow \mathcal{M}$
$\mathbf{c} \leftarrow \mathsf{DEnc}(pk, \mathbf{m}_b)$
$C \leftarrow C \cup \mathbf{c}$
Return $\mathbf{c}$
```

```
DEC$(c)$
If $c \in C$, then
    Return $\perp$
$m \leftarrow \mathsf{DDec}(sk, c)$
Return $m$
```

Fig. 1. Games for defining IND-CCA security of a standard PKE scheme PKE, IND security and adaptively CCA security of a D-PKE scheme DE.

IND-CCA security for PKE is defined by game $\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},A}$ in Fig. 1. For any $(\mathbf{m}_0, \mathbf{m}_1)$ submitted to the encryption oracle ENC$(\cdot)$ in $\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},A}$, we require that $|\mathbf{m}_0| = |\mathbf{m}_1|$, and for every $i \in [|\mathbf{m}_0|]$, $|\mathbf{m}_0[i]| = |\mathbf{m}_1[i]|$. PKE is called *IND-CCA secure* if $\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},A}(k) = 2\Pr[\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},A}(k)] - 1$ is negligible for any PPT adversary A, and called *IND-CPA secure* if A is not allowed to access to the decryption oracle DEC$(\cdot)$.

Following [1], the maximum public-key collision probability of PKE is defined by $\mathsf{maxpk}_{\mathsf{PKE}}(k) = \max_{\omega \in \{0,1\}^*} \Pr[pk = \omega : (pk, sk) \leftarrow \mathsf{Kg}(1^k)]$.

PKE secure under randomness failures. Currently, there are mainly three approaches to deal with the problems of randomness failures for PKE: deterministic PKE, hedged PKE, and nonce-based PKE. We recall their definitions and security notions as follows.

Deterministic PKE. A PKE scheme is called *deterministic* if the encryption algorithm is deterministic. This notion was formally introduced by Bellare, Boldyreva, and O'Neill [1]. For a D-PKE scheme $\mathsf{DE} = (\mathsf{DKg}, \mathsf{DEnc}, \mathsf{DDec})$, IND security [4] is defined by game $\mathbf{G}^{\text{de-ind}}_{\mathsf{DE},A}$ in Fig. 1. An IND adversary $A = (A_1, A_2)$ in game $\mathbf{G}^{\text{de-ind}}_{\mathsf{DE},A}$ is called *legitimate*, if for any $(\mathbf{m}_0, \mathbf{m}_1)$ sampled by $\mathcal{M}$, associated with some polynomial $\mathsf{p}(\cdot)$, the following two conditions hold: (i) $|\mathbf{m}_0| = |\mathbf{m}_1| = \mathsf{p}(k)$, and for every $i \in [\mathsf{p}(k)]$, $|\mathbf{m}_0[i]| = |\mathbf{m}_1[i]|$; (ii) for any $b \in \{0,1\}$, $\mathbf{m}_b[1], \cdots, \mathbf{m}_b[\mathsf{p}(k)]$ are distinct. The guessing probability of A is denoted by $\text{Guess}_A(k)$, which returns the maximum of $\Pr[\mathbf{m}_b[i] = m]$ over all $b \in \{0,1\}$, all $i \in [\mathsf{p}(k)]$, all $m \in \{0,1\}^*$, and all $\mathcal{M}$ submitted by A_1, where the probability is taken over $(\mathbf{m}_0, \mathbf{m}_1) \leftarrow \mathcal{M}(1^k)$. The block-source guessing probability of A is denoted by $\text{Guess}^{\text{b-s}}_A(k)$, which returns the maximum of $\Pr[\mathbf{m}_b[i] = m_i \mid \mathbf{m}_b[j] = m_j,\ \forall j \in [i-1]]$ over all $b \in \{0,1\}$, all $i \in [\mathsf{p}(k)]$, all $m_1, \cdots, m_i \in \{0,1\}^*$, and all $\mathcal{M}$ submitted by A_1, where the probability is taken over $(\mathbf{m}_0, \mathbf{m}_1) \leftarrow \mathcal{M}(1^k)$. We say that A has *high min-entropy* (resp. *high block-source min-entropy* [9]) if $\text{Guess}_A(k)$

(resp. $\mathrm{Guess}_A^{\text{b-s}}(k)$) is negligible. Scheme DE is *fully IND secure* (resp. *block-source IND secure*) if $\mathbf{Adv}_{\mathsf{DE},A}^{\text{de-ind}}(k) = 2\Pr[\mathbf{G}_{\mathsf{DE},A}^{\text{de-ind}}(k)] - 1$ is negligible for any legitimate PPT adversary A of high min-entropy (resp. high block-source min-entropy).

We say that a PPT adversary is *adaptive* if it is allowed to query the challenge oracle multiple times, and each query may depend on the replies to the previous queries. IND is a non-adaptive security notion. A stronger adaptive security notion for D-PKE, *adaptively CCA security*, is defined by game $\mathbf{G}_{\mathsf{DE},A}^{\text{de-cca}}$ in Fig. 1. We similarly define adaptively CCA adversary that is *legitimate* and *has high min-entropy*. Scheme DE is *fully adaptively CCA secure* if $\mathbf{Adv}_{\mathsf{DE},A}^{\text{de-cca}}(k) = 2\Pr[\mathbf{G}_{\mathsf{DE},A}^{\text{de-cca}}(k)] - 1$ is negligible for any legitimate PPT adversary A of high min-entropy. Block-source adaptively CCA security for D-PKE is similarly defined.

DE is called *unique-ciphertext* [5], if for any k, any (pk, sk) generated by DKg, and any message $m \in \{0,1\}^*$, there is at most one $c \in \{0,1\}^*$ such that $\mathsf{DDec}(sk, c) = m$. Each D-PKE scheme can be efficiently transformed to a unique-ciphertext one [5].

Hedged PKE. In ASIACRYPT 2009, Bellare, et al. [2] introduced the notion of IND-CDA security, which formalized the security for PKE when the messages and the randomness jointly have high entropy. A PKE scheme is called *hedged* if it achieves both IND-CPA security and IND-CDA security, which means that it achieves IND-CPA security when the random coins employed during the encryption are truly random, and achieves IND-CDA security when bad random coins are employed but the messages and the random coins jointly have high min-entropy.

For a hedged PKE (H-PKE) scheme $\mathsf{HE} = (\mathsf{HKg}, \mathsf{HEnc}, \mathsf{HDec})$, IND-CDA security is defined by game $\mathbf{G}_{\mathsf{HE},A}^{\text{ind-cda}}$ in Fig. 2. An IND-CDA adversary $A = (A_1, A_2)$ in game $\mathbf{G}_{\mathsf{HE},A}^{\text{ind-cda}}$ is called *legitimate*, if for any $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r})$ sampled by $\mathcal{M}$, associated with some polynomial $\mathsf{p}(\cdot)$, which is the message sampler submitted to oracle $\mathrm{LR}(\cdot)$ by A_1, the following two conditions hold: (i) $|\mathbf{m}_0| = |\mathbf{m}_1| = |\mathbf{r}| = \mathsf{p}(k)$, and for every $i \in [\mathsf{p}(k)]$, $|\mathbf{m}_0[i]| = |\mathbf{m}_1[i]|$; (ii) for any $b \in \{0,1\}$, $(\mathbf{m}_b[1], \mathbf{r}[1]), \cdots, (\mathbf{m}_b[\mathsf{p}(k)], \mathbf{r}[\mathsf{p}(k)])$ are distinct. The guessing probability of A is denoted by $\mathrm{Guess}_A(k)$, which returns the maximum of $\Pr[(\mathbf{m}_b[i], \mathbf{r}[i]) = (m, r)]$ over all $b \in \{0,1\}$, all $i \in [\mathsf{p}(k)]$, all $m \in \{0,1\}^*$, all $r \in \{0,1\}^*$, and all $\mathcal{M}$ submitted by A_1, where the probability is taken over $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}) \leftarrow \mathcal{M}(1^k)$. We say that A has *high min-entropy* if $\mathrm{Guess}_A(k)$ is negligible. Scheme HE is *IND-CDA secure* if $\mathbf{Adv}_{\mathsf{HE},A}^{\text{ind-cda}}(k) = 2\Pr[\mathbf{G}_{\mathsf{HE},A}^{\text{ind-cda}}(k)] - 1$ is negligible for any legitimate PPT adversary A of high min-entropy. The notion of *block-source* IND-CDA security is similarly defined [2].

```
Game $\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NE},\mathsf{NG},A}(k)$
$(pk, sk) \leftarrow \mathsf{NKg}(1^k)$
$xk \leftarrow \mathsf{NSKg}(1^k)$
$b \leftarrow \{0,1\}; St \leftarrow \epsilon$
$C, Q_0, Q_1 \leftarrow \emptyset$
$b' \leftarrow A^{\mathrm{ENC},\mathrm{DEC}}(pk)$
Return $(b' = b)$

$\mathrm{ENC}(m_0, m_1, \eta)$
If $(|m_0| \neq |m_1|)$, then return $\perp$
If $((m_0, n) \in Q_0)$ or $((m_1, n) \in Q_1)$, then return $\perp$
$(n, St) \leftarrow \mathsf{NG}(1^k, \eta, St)$;  $c \leftarrow \mathsf{NEnc}(pk, xk, m_b, n)$
$Q_0 \leftarrow Q_0 \cup \{(m_0, n)\}$; $Q_1 \leftarrow Q_1 \cup \{(m_1, n)\}$
$C \leftarrow C \cup \{c\}$
Return $c$

$\mathrm{DEC}(c)$
If $c \in C$, then return $\perp$
$m \leftarrow \mathsf{NDec}(sk, c)$
Return $m$
```

```
Game $\mathbf{G}^{\mathrm{nbp2}}_{\mathsf{NE},\mathsf{NG},A}(k)$
$(pk, sk) \leftarrow \mathsf{NKg}(1^k)$
$xk \leftarrow \mathsf{NSKg}(1^k)$
$b \leftarrow \{0,1\}; St \leftarrow \epsilon$
$C \leftarrow \emptyset$
$b' \leftarrow A^{\mathrm{ENC},\mathrm{DEC}}(pk, xk)$
Return $(b' = b)$

$\mathrm{ENC}(m_0, m_1, \eta)$
If $(|m_0| \neq |m_1|)$, then
  return $\perp$
$(n, St) \leftarrow \mathsf{NG}(1^k, \eta, St)$
$c \leftarrow \mathsf{NEnc}(pk, xk, m_b, n)$
$C \leftarrow C \cup \{c\}$
Return $c$

$\mathrm{DEC}(c)$
If $c \in C$, then return $\perp$
$m \leftarrow \mathsf{NDec}(sk, c)$
Return $m$
```

```
Game $\mathbf{G}^{\mathrm{ind\text{-}cda}}_{\mathsf{HE},A}(k)$
$(pk, sk) \leftarrow \mathsf{HKg}(1^k)$
$b \leftarrow \{0,1\}$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$
$b' \leftarrow A_2(pk, St)$
Return $(b' = b)$

$\mathrm{LR}(\mathcal{M})$
$(\mathbf{m}_0, \mathbf{m}_1, \mathbf{r}) \leftarrow \mathcal{M}(1^k)$
$\mathbf{c} \leftarrow \mathsf{HEnc}(pk, \mathbf{m}_b; \mathbf{r})$
Return $\mathbf{c}$
```

Fig. 2. Games for defining NBP1, NBP2 security of a N-PKE scheme NE, and IND-CDA security for a H-PKE scheme HE.

Nonce-based PKE. A nonce-based public-key encryption (N-PKE) scheme with nonce space $\mathsf{NE.NS}$ is a tuple of PPT algorithms $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$. The key generation algorithm NKg, taking 1^k as input, generates a public/secret key pair (pk, sk). The seed generation algorithm NSKg taking 1^k returns a sender seed xk. Let $\mathsf{NE.SD}$ denote the seed space. We say that NSKg is *trivial*, if it returns a uniformly chosen xk from $\mathsf{NE.SD} = \{0,1\}^k$. The *deterministic* encryption algorithm NEnc, taking pk, xk, message $m \in \{0,1\}^*$, and nonce $n \in \mathsf{NE.NS}$ as input, outputs a ciphertext c. The deterministic decryption algorithm NDec is the same as that of the traditional PKE schemes, on input sk and c, returns a value in $\{0,1\}^* \cup \{\perp\}$. The nonce is not necessary for decryption. Standard correctness is required, which means that for any valid message $m \in \{0,1\}^*$, $(pk, sk) \leftarrow \mathsf{NKg}(1^k)$, $xk \leftarrow \mathsf{NSKg}(1^k)$, $n \in \mathsf{NE.NS}$ and $c \leftarrow \mathsf{NEnc}(pk, xk, m, n)$, $\mathsf{Dec}(sk, c) = m$ with overwhelming probability.

The notion of N-PKE was introduced by Bellare and Tackmann [8]. In their N-PKE constructions, the nonces are generated by a building block called *nonce generator* NG with nonce space $\mathsf{NE.NS}$. A nonce generator NG is a PPT algorithm taking 1^k, a current state St, and a *nonce selector* η as input, returns a nonce $n \in \mathsf{NE.NS}$ and a new state St, i.e., $(n, St) \leftarrow \mathsf{NG}(1^k, \eta, St)$. Standard security of NG requires that the generated nonces should be unpredictable and never repeat. We refer the readers to [8, 16] for the formal definition.

Two kinds of security notions for N-PKE were introduced in [8], which we recall in Fig. 2. An N-PKE scheme NE, with respect to NG, is NBP1 (resp. NBP2) secure if $\mathbf{Adv}^{\mathrm{nbp1}}_{\mathsf{NE},\mathsf{NG},A}(k) = 2\Pr[\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NE},\mathsf{NG},A}(k)] - 1$

(resp. $\mathbf{Adv}^{\text{nbp2}}_{\mathsf{NE},\mathsf{NG},A}(k) = 2\Pr[\mathbf{G}^{\text{nbp2}}_{\mathsf{NE},\mathsf{NG},A}(k)] - 1$) is negligible for any PPT adversary A, where game $\mathbf{G}^{\text{nbp1}}_{\mathsf{NE},\mathsf{NG},A}$ (resp. $\mathbf{G}^{\text{nbp2}}_{\mathsf{NE},\mathsf{NG},A}$) is defined in Fig. 2. According to [8], NBP1 security is achieved for any nonce generator (even for predictable nonce generator), as long as the message-nonce pairs do not repeat; NBP2 security is achieved for any unpredictable nonce generators.

3 Hedged security for nonce-based public-key encryption

In this section, we introduce hedged security for nonce-based public-key encryption. We first formalize chosen-ciphertext security against chosen-distribution attacks (IND-CDA2 security) for N-PKE. Then, we explore the relations among the security notions of N-PKE. Lastly, we formalize a special version (the Raghunathan-Segev-Vadhan [20] version) of IND-CDA2 security for N-PKE.

3.1 Chosen-ciphertext security against chosen-distribution attacks

Notice that the original message samplers were defined for the general PKE schemes, which do not sample the seeds and the nonces. Therefore, we firstly formalize the notion of message samplers for N-PKE as follows.

Definition 1 (Message sampler for N-PKE). *A message sampler $\mathcal{M}$ for N-PKE is a PPT algorithm taking 1^k as input, and returning $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$.*

For any N-PKE scheme $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$ w.r.t. nonce generator NG, consider game $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}$ as shown in Fig. 3.

We say that the adversary $A = (A_1, A_2)$ in game $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}$ is *legitimate*, if for any $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n})$ sampled by $\mathcal{M}$ which is associated with some polynomial $\mathsf{p}(\cdot)$, the following two conditions hold: (i) $|\mathbf{m}_0| = |\mathbf{m}_1| = |\mathbf{xk}| = |\mathbf{n}| = \mathsf{p}(k)$, and for every $i \in [\mathsf{p}(k)]$, $|\mathbf{m}_0[i]| = |\mathbf{m}_1[i]|$; (ii) for any $b \in \{0,1\}$, $(\mathbf{xk}[1], \mathbf{m}_b[1], \mathbf{n}[1]), \cdots, (\mathbf{xk}[\mathsf{p}(k)], \mathbf{m}_b[\mathsf{p}(k)], \mathbf{n}[\mathsf{p}(k)])$ are distinct.

Similarly, the guessing probability of A is denoted by $\text{Guess}_A(k)$, which returns the maximum of $\Pr[(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk, m, n)]$ over all $b \in \{0,1\}$, all $i \in [\mathsf{p}(k)]$, all $xk \in \{0,1\}^*$, all $m \in \{0,1\}^*$, all $n \in \{0,1\}^*$, and all $\mathcal{M}$ submitted by A_1, where the probability is taken over $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$. The block-source guessing probability of A is denoted by $\text{Guess}^{\text{b-s}}_A(k)$, which returns the maximum of

```
Game $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}(k)$
$(pk, sk) \leftarrow \mathsf{NKg}(1^k)$
$b \leftarrow \{0,1\}; C \leftarrow \emptyset$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$
$b' \leftarrow A_2^{\mathrm{DEC}}(pk, St)$
Return $(b' = b)$
```

```
$\mathrm{LR}(\mathcal{M})$
$(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
$\mathbf{c} \leftarrow \mathsf{NEnc}(pk, \mathbf{xk}, \mathbf{m}_b, \mathbf{n})$
$C \leftarrow C \cup \mathbf{c}$
Return $\mathbf{c}$
```

```
$\mathrm{DEC}(c)$
If $c \in C$, then return $\perp$
$m \leftarrow \mathsf{NDec}(sk, c)$
Return $m$
```

Fig. 3. Game for defining IND-CDA2 security of a N-PKE scheme NE

.

$\Pr[(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk, m, n) \mid (\mathbf{xk}[j], \mathbf{m}_b[j], \mathbf{n}[j]) = (xk_j, m_j, n_j), \forall j \in [i-1]]$ over all $b \in \{0,1\}$, all $i \in [\mathsf{p}(k)]$, all $xk_1, \cdots, xk_i \in \{0,1\}^*$, all $m_1, \cdots, m_i \in \{0,1\}^*$, all $n_1, \cdots, n_i \in \{0,1\}^*$, and all $\mathcal{M}$ submitted by A_1, where the probability is taken over $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$. We say that the IND-CDA2 adversary A has *high min-entropy* (resp. *high block-source min-entropy*) if $\mathrm{Guess}_A(k)$ (resp. $\mathrm{Guess}_A^{\text{b-s}}(k)$) is negligible.

Definition 2 (IND-CDA2). *An N-PKE scheme* $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$*, with respect to nonce generator* NG*, is IND-CDA2 secure (resp. block-source IND-CDA2 secure), if for any legitimate PPT adversary* $A = (A_1, A_2)$ *having high min-entropy (resp. high block-source min-entropy), its advantage* $\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{NE},A}(k) = 2\Pr[\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}(k)] - 1$ *is negligible, where game* $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}$ *is defined in Fig. 3.*

Remark 1 Note that if the adversary A is not allowed to access to the decryption oralce $\mathrm{DEC}(\cdot)$, then we call the defining security notion "IND-CDA security in the nonce-based setting". Note that in [2] the notion of "IND-CDA security" was defined for the general PKE schemes, not for N-PKE. For simplicity, in this paper we abuse the notation, still using "IND-CDA security" when we refer to "IND-CDA security in the nonce-based setting".

Remark 2 Recently, Boldyreva et al. [10] formalized the CCA version of IND-CDA security for PKE, and called it MMR-CCA security. The notion of MMR-CCA security is defined for PKE with associated data, and in the experiment defining MMR-CCA security, the adversary is allowed to access to the decryption oracle *before* seeing the public key. Our IND-CDA2 security is formalized for N-PKE (without associated data), and the adversary is not allowed to access to the decryption oracle until it receives the public key. If the lengths of the seed and the nonce are both restricted to be 0, our security will naturally become adaptive CCA security for D-PKE.

$\mathsf{NKg}'(1^k)$ $(pk, sk) \leftarrow \mathsf{NKg}(1^k)$ Return (pk, sk)	$\mathsf{NSKg}'(1^k)$ $xk \leftarrow \mathsf{NSKg}(1^k)$ Return xk	$\mathsf{NEnc}'(pk, xk, m, n)$ If $xk = 0^k$, then $c \leftarrow m$, $c' \leftarrow (c\|\|0)$ Else, $c \leftarrow \mathsf{NEnc}(pk, xk, m, n)$ $c' \leftarrow (c\|\|1)$ Return c'	$\mathsf{NDec}'(sk, c')$ Parse $c' = (c\|\|b)$ If $b = 0$, then $m \leftarrow c$ Else, $m \leftarrow \mathsf{NDec}(sk, c)$ Return m
$\mathsf{NKg}''(1^k)$ $(pk, sk) \leftarrow \mathsf{NKg}(1^k)$ Return (pk, sk)	$\mathsf{NSKg}''(1^k)$ $xk \leftarrow \mathsf{NSKg}(1^k)$ Return xk	$\mathsf{NEnc}''(pk, xk, m, n)$ If $m = pk$, then $c \leftarrow m$, $c'' \leftarrow (c\|\|0)$ Else, $c \leftarrow \mathsf{NEnc}(pk, xk, m, n)$ $c'' \leftarrow (c\|\|1)$ Return c''	$\mathsf{NDec}''(sk, c'')$ Parse $c'' = (c\|\|b)$ If $b = 0$, then $m \leftarrow c$ Else, $m \leftarrow \mathsf{NDec}(sk, c)$ Return m

Fig. 4. Counterexamples $\mathsf{NE}' = (\mathsf{NKg}', \mathsf{NSKg}', \mathsf{NEnc}', \mathsf{NDec}')$ and $\mathsf{NE}'' = (\mathsf{NKg}'', \mathsf{NSKg}'', \mathsf{NEnc}'', \mathsf{NDec}'')$.

3.2 Separations between NBP1/NBP2 security and IND-CDA2 security

We now show that NBP1/NBP2 security and IND-CDA2 security do not imply each other. Our separation results are based on the following observations. In the game defining IND-CDA2 security, (i) the sender seed xk is specified by the adversary through the generated message sampler $\mathcal{M}$, instead of being generated by NSKg in the game defining NBP1/NBP2 security; (ii) the challenge messages are independent of the public key, instead of being chosen by the adversary after seeing the public key in the game defining NBP1/NBP2 security.

NBP1/NBP2 $\not\Rightarrow$ IND-CDA2. Actually, we provide a stronger conclusion here "NBP1/NBP2 $\not\Rightarrow$ IND-CDA". For an NBP1/NBP2 secure N-PKE scheme $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$ w.r.t. a nonce generator NG, where NSKg is trivial, we construct a new N-PKE scheme $\mathsf{NE}' = (\mathsf{NKg}', \mathsf{NSKg}', \mathsf{NEnc}', \mathsf{NDec}')$, w.r.t. the same NG, as shown in Fig. 4.

Since NSKg is trivial, we have that $xk \leftarrow \{0,1\}^k$. As a result, the probability that $xk = 0^k$ is negligible. Therefore, NBP1/NBP2 security of NE' is guaranteed by NBP1/NBP2 security of NE.

Now we show an adversary $A = (A_1, A_2)$ attacking NE' in the sense of IND-CDA. For simplicity, we assume that the message space is $\{0,1\}^k$. A_1 makes an LR$(\cdot)$ query by submitting a message sampler $\mathcal{M}$ (with $\mathsf{p}(k) = 1$), which is defined as follows:

1. Set $xk = 0^k$.
2. For any $b \in \{0,1\}$, choose m_b uniformly random from $\{0,1\}^k$, conditioned on that the last bit of m_b is b.

3. Choose n uniformly random from nonce space $\mathsf{NE.NS}$.

Note that n is uniformly chosen from $\mathsf{NE.NS}$, and m_0, m_1 are both uniformly chosen from $\{0,1\}^{k-1}$. So adversary A is legitimate and has high min-entropy. After receiving the ciphertext $c' = (c||0)$ from LR$(\cdot)$, A returns the last bit of c as its final output. The advantage of A is obviously 1.

IND-CDA2 $\nRightarrow$ NBP1/NBP2. Assuming that there is an N-PKE scheme $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$, w.r.t. a nonce generator NG, achieving IND-CDA2 security and having negligible maximum public-key collision probability $\mathsf{maxpk}_{\mathsf{NE}}$. Note that the requirement that $\mathsf{maxpk}_{\mathsf{NE}}$ is negligible is very mild, since any IND-CPA secure PKE has negligible $\mathsf{maxpk}_{\mathsf{NE}}$ [1]. Based on NE, we present a new N-PKE scheme $\mathsf{NE}'' = (\mathsf{NKg}'', \mathsf{NSKg}'', \mathsf{NEnc}'', \mathsf{NDec}'')$, w.r.t. the same NG, as shown in Fig. 4.

For any IND-CDA2 adversary $A = (A_1, A_2)$, A does not receive pk until it finishes the process of LR$(\cdot)$ query. The negligible $\mathsf{maxpk}_{\mathsf{NE}}$ guarantees that

$$\max_{i \in [|\mathbf{m}_0|]} \Pr[(\mathbf{m}_0[i] = pk) \vee (\mathbf{m}_1[i] = pk) : \mathcal{M} \text{ is generated by} A_1^{\mathrm{LR}},$$
$$(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)]$$

is negligible, where the probability is taken over A_1^{LR} and $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$. Therefore, NE'' is IND-CDA2 secure.

Note that in the game defining NBP1/NBP2 security, the adversary generates the challenge messages (m_0, m_1) *after* seeing the public key. So we construct a NBP1/NBP2 adversary A as follows. Upon receiving pk, A sets $m_0 = pk$, and chooses an arbitrary distinct m_1 from the message space such that $|m_1| = |m_0|$, and an arbitrary valid nonce selector η. Then A submits the generated (m_0, m_1, η) to the encryption oracle ENC$(\cdot)$. After receiving the ciphertext $c'' = (c||b)$, A returns b as its final output. The advantage of A is obviously 1.

Formally, we have the following theorem.

Theorem 1. *NBP1/NBP2 security and IND-CDA2 security do not imply each other.*

Remark 3 The aforementioned NBP1/NBP2 adversary attacking NE'' does not make any decryption query. So we actually proved that IND-CDA2 security does not imply the CPA version of NBP1/NBP2 security. Therefore, our results also show the separations between NBP1/NBP2 security and IND-CDA security.

3.3 The RSV version of IND-CDA2 security

In EUROCRYPT 2013, Raghunathan, Segev and Vadhan [20] formalized another security notion for D-PKE, ACD-CPA/CCA security, which allows the adversaries to adaptively choose message distributions *after* seeing the public key, with the following two restrictions: (1) the adversaries have high min-entropy; (2) for each adversary, there is an upper bound on the number of the message distributions from which the adversary is allowed to adaptively choose. The upper bound is $2^{p(k)}$ where $p(\cdot)$ is any a-priori fixed polynomial. Raghunathan et al. [20] proposed a D-PKE scheme achieving ACD-CCA security in the standard model, based on a primitive called $\mathcal{R}$-lossy trapdoor function.

Considering that this is an important optional security notion for D-PKE, and as far as we know, ACD-CCA is neither weaker nor stronger than adaptive CCA security, we formalize a similar version of IND-CDA2 security here, which we call the RSV version of IND-CDA2 security (RIND-CDA2).

Definition 3 (RSV message sampler for N-PKE). *An* RSV message sampler $\mathcal{M}$ *for N-PKE is a PPT algorithm taking* 1^k *as input, and returning* $(\mathbf{m}, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$.

Definition 4 (Uniform message sampler with respect to $\mathcal{M}$). *For an RSV message sampler* $\mathcal{M}$ *for N-PKE, a PPT algorithm* $\mathcal{U}$ *is a* uniform message sampler with respect to $\mathcal{M}$ *if for any message vector sampled by* $\mathcal{M}$ *(i.e.,* $(\mathbf{m}, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$*),* $\mathbf{m}_u \leftarrow \mathcal{U}(\mathcal{M}, \mathbf{m})$ *is uniformly distributed over the same message space specified by* $\mathcal{M}$*, such that* $|\mathbf{m}_u| = |\mathbf{m}|$ *and* $|\mathbf{m}_u[i]| = |\mathbf{m}[i]|$ *for any* $i \in [|\mathbf{m}|]$.

For any N-PKE scheme $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$ w.r.t. nonce generator NG, consider game $\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}$ as shown in Fig. 5.

The adversary A in game $\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}$ is *legitimate*, if for any $(\mathbf{m}, \mathbf{xk}, \mathbf{n})$ sampled by $\mathcal{M}$ which is associated with some polynomial $\mathsf{p}(\cdot)$, the following two conditions hold: (i) $|\mathbf{m}| = |\mathbf{xk}| = |\mathbf{n}| = \mathsf{p}(k)$; (ii) $(\mathbf{m}[1], \mathbf{xk}[1], \mathbf{n}[1]), \cdots, (\mathbf{m}[\mathsf{p}(k)], \mathbf{xk}[\mathsf{p}(k)], \mathbf{n}[\mathsf{p}(k)])$ are distinct.

Similar to that of Section 3.1, we have the guessing probabilities $\text{Guess}_A(k)$ and $\text{Guess}^{\text{b-s}}_A(k)$. We say that the RIND-CDA2 adversary A has *high min-entropy* (resp. *high block-source min-entropy*) if $\text{Guess}_A(k)$ (resp. $\text{Guess}^{\text{b-s}}_A(k)$) is negligible.

For any given polynomial $p(\cdot)$, we have the following definition.

Definition 5 ($2^{p(k)}$-bounded adversary). *For any PPT legitimate adversary A having high min-entropy (resp. high block-source min-entropy)*

```
Game $\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}(k)$
    $(pk, sk) \leftarrow \mathsf{NKg}(1^k)$
    $b \leftarrow \{0,1\}$; $C \leftarrow \emptyset$
    $b' \leftarrow A^{\text{RoR},\text{DEC}}(pk)$
    Return $(b' = b)$

RoR($\mathcal{M}$)
    $(\mathbf{m}, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{m}_1 \leftarrow \mathbf{m}$; $\mathbf{m}_0 \leftarrow \mathcal{U}(\mathcal{M}, \mathbf{m})$
    $\mathbf{c} \leftarrow \mathsf{NEnc}(pk, \mathbf{xk}, \mathbf{m}_b, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

DEC($c$)
    If $c \in C$, then return $\perp$
    $m \leftarrow \mathsf{NDec}(sk, c)$
    Return $m$
```

Fig. 5. Game for defining RIND-CDA2 security of a N-PKE scheme NE, where $\mathcal{U}$ is defined in Definition 4.

in game $\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}$*, let* $\mathcal{S}_{mg}$ *be the set of message samplers which* A *may submit to the RoR oracle as a query with non-zero probability.* A *is a* $2^{p(k)}$-bounded *(resp.* $2^{p(k)}$-bounded block-source*) adversary if for every* $k \in \mathbb{N}$*,* $|\mathcal{S}_{mg}| \leq 2^{p(k)}$*.*

Definition 6 (RIND-CDA2). *An N-PKE scheme* NE*, w.r.t. nonce generator* NG*, is* RIND-CDA2 secure *(resp.* block-source RIND-CDA2 secure*), if for any* $2^{p(k)}$*-bounded (resp.* $2^{p(k)}$*-bounded block-source) adversary* A*, its advantage* $\mathbf{Adv}^{\text{rind-cda2}}_{\mathsf{NE},A}(k) = 2\Pr[\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}(k)] - 1$ *is negligible, where game* $\mathbf{G}^{\text{rind-cda2}}_{\mathsf{NE},A}$ *is defined in Fig. 5.*

4 Construction of H-PKE in the random oracle model

In EUROCRYPT 2016, Bellare and Tackmann [8] proposed an NBP1/NBP2 secure N-PKE scheme in the random oracle model. Their construction is based on a building block which they introduced and called *hedged extractor.*

In this section, we show that the Bellare-Tackmann ROM construction actually achieves HN-IND security. But we note that this construction cannot be generalized to the schemes based on hedged extractors like [8, Figure 6].

Firstly, we recall the N-PKE scheme RtP [8], w.r.t. a nonce generator NG, as follows. Let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a traditional probabilistic PKE scheme with message space MSP and randomness space $\mathcal{R}_{\mathsf{Enc}}$, and $\mathsf{RO} : \{0,1\}^* \to \mathcal{R}_{\mathsf{Enc}}$ be a random oracle. The N-PKE scheme RtP is presented in Fig. 6.

Now we turn to the security. It has been proved in [8] that RtP is NBP1/NBP2 secure. So what remains is to prove its IND-CDA2 security. Formally, we have the following theorem.

Theorem 2. *If* PKE *is a traditional IND-CCA secure PKE scheme, then N-PKE scheme* RtP*, w.r.t. a nonce generator* NG*, is IND-CDA2 secure in the random oracle model.*

$\mathsf{RKg}(1^k)$	$\mathsf{RSKg}(1^k)$	$\mathsf{REnc}(pk, xk, m, n)$	$\mathsf{RDec}(sk, c)$
$(pk, sk) \leftarrow \mathsf{Kg}(1^k)$ Return (pk, sk)	$xk \leftarrow \mathsf{NE.SD}$ Return xk	$r \leftarrow \mathsf{RO}(xk, m, n)$ $c \leftarrow \mathsf{Enc}(pk, m; r)$ Return c	$m \leftarrow \mathsf{Dec}(sk, c)$ Return m

Fig. 6. N-PKE scheme $\mathsf{RtP} = (\mathsf{RKg}, \mathsf{RSKg}, \mathsf{REnc}, \mathsf{RDec})$.

Proof. For any legitimate PPT IND-CDA2 adversary A having high min-entropy, let $q_r(k)$ (resp. $q_l(k)$) denote the number of random-oracle queries (resp. LR queries) of A.

Consider a sequence of games $\mathbf{G}_0 - \mathbf{G}_6$ in Fig. 7 and Fig. 8. In each game, there is a random oracle RO which maintains a local array H as shown in Fig. 7. Denote by RO_A the random-oracle interface of A. Note that in games $\mathbf{G}_4$ and $\mathbf{G}_5$, the oracle answers of RO_A and the answers given to the LR oracle in reply to its RO queries are independent, so we introduce another local array H_A for RO_A. In game $\mathbf{G}_6$, the LR oracle does not access to RO, so we omit the procedure "**On query** RO" in Fig. 8. For convenience, the RO queries made by A through RO_A is called *RO_A queries* in this proof. Without loss of generality, we assume that in each game, A does not repeat any RO_A queries.

Now we explain the sequence of games.

Game $\mathbf{G}_0$ implements game $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{RtP},A}$. So we have

$$\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{RtP},A}(k) = 2\Pr[\mathbf{G}_0(k)] - 1. \tag{1}$$

In game $\mathbf{G}_1$, we introduces two sets T_1 and T_2. T_1 denotes the set of RO queries made by A (i.e., RO_A queries), and T_2 denotes the set of RO queries made by the LR oracle. The changes made in $\mathbf{G}_1$ does not affect the final output. Therefore,

$$\Pr[\mathbf{G}_1(k)] = \Pr[\mathbf{G}_0(k)]. \tag{2}$$

Games $\mathbf{G}_2$ and $\mathbf{G}_1$ are identical-until-bad_1. Denote by $\Pr[\mathsf{bad}_1]$ the probability that $\mathbf{G}_2$ sets bad_1. According to the fundamental lemma of game-playing [7], we have that $|\Pr[\mathbf{G}_2(k)] - \Pr[\mathbf{G}_1(k)]| \leq \Pr[\mathsf{bad}_1]$.

Let $\mathcal{M}'$, associated with some polynomial $\mathsf{p}(\cdot)$, denote the message sampler leading to bad_1. Game $\mathbf{G}_2$ sets bad_1 only if A has made some RO_A query (xk', m', n') beforehand, such that for the $\mathcal{M}'$ and $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}'$, there are some $b \in \{0,1\}$ and some $i \in [|\mathbf{n}|]$ satisfying $(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk', m', n')$. Since A has high min-entropy, for any RO_A query (xk', m', n'), we have that for any $\mathcal{M}'$, any $b \in \{0,1\}$, and any $i \in [|\mathsf{p}(k)|]$,

$$\Pr[(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk', m', n') : (\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}'] \leq \mathrm{Guess}_A(k).$$

```
Games $\mathbf{G}_0$, $\boxed{\mathbf{G}_1 - \mathbf{G}_3,}$ $\boxed{\boxed{\mathbf{G}_2 - \mathbf{G}_3,}}$ $\colorbox{lightgray}{$\mathbf{G}_3$}$
$(pk, sk) \leftarrow \mathsf{Kg}(1^k)$ ; $b \leftarrow \{0,1\}$; $C \leftarrow \emptyset$; $\boxed{T_1, T_2 \leftarrow \emptyset}$
$St \leftarrow A_1^{\mathrm{RO}_A, \mathrm{LR}}(1^k)$; $b' \leftarrow A_2^{\mathrm{RO}_A, \mathrm{DEC}}(pk, St)$
Return $(b' = b)$

On query $\mathrm{RO}_A(xk', m', n')$:
    $\boxed{T_1 \leftarrow T_1 \cup \{(xk', m', n')\}}$
    $\colorbox{lightgray}{If $(xk', m', n') \in T_2$, then}$
    $\colorbox{lightgray}{$\quad \mathsf{bad}_2 \leftarrow \mathsf{true}$; $H[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$}$
    Return $\mathrm{RO}(xk', m', n')$

On query $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    For $i \in [|\mathbf{n}|]$, then
        $\boxed{T_2 \leftarrow T_2 \cup \{(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i])\}}$
        $\boxed{\boxed{\text{If } (\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) \in T_1, \text{ then}}}$
        $\boxed{\boxed{\quad \mathsf{bad}_1 \leftarrow \mathsf{true};\ H[\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]] \leftarrow \mathcal{R}_{\mathsf{Enc}}}}$
        $\mathbf{r}[i] \leftarrow \mathrm{RO}(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i])$
        $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_b[i]; \mathbf{r}[i])$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{Dec}(sk, c')$
    Return $m'$

On query $\mathrm{RO}(xk', m', n')$:
    If $H[xk', m', n'] = \perp$, then $H[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H[xk', m', n']$
```

```
Games $\mathbf{G}_4$, $\boxed{\mathbf{G}_5}$
$(pk, sk) \leftarrow \mathsf{Kg}(1^k)$ ; $b \leftarrow \{0,1\}$; $C \leftarrow \emptyset$; $T_1, T_2 \leftarrow \emptyset$
$St \leftarrow A_1^{\mathrm{RO}_A, \mathrm{LR}}(1^k)$; $b' \leftarrow A_2^{\mathrm{RO}_A, \mathrm{DEC}}(pk, St)$
Return $(b' = b)$

On query $\mathrm{RO}_A(xk', m', n')$:
    $T_1 \leftarrow T_1 \cup \{(xk', m', n')\}$
    If $H_A[xk', m', n'] = \perp$, then
        $H_A[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H_A[xk', m', n']$

On query $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    For $i \in [|\mathbf{n}|]$, then
        $T_2 \leftarrow T_2 \cup \{(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i])\}$
        $\mathbf{r}[i] \leftarrow \mathrm{RO}(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i])$
        $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_b[i]; \mathbf{r}[i])$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{Dec}(sk, c')$
    Return $m'$

On query $\mathrm{RO}(xk', m', n')$:
    If $H[xk', m', n'] = \perp$, then
        $H[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    $\boxed{\text{If } H[xk', m', n'] \neq \perp, \text{ then}}$
    $\boxed{\quad \mathsf{bad}_3 \leftarrow \mathsf{true};\ H[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}}$
    Return $H[xk', m', n']$
```

Fig. 7. Games $\mathbf{G}_0 - \mathbf{G}_5$ in the proof of Theorem 2. Boxed code is only executed in the games specified by the game names in the same box style.

In other words, for any RO_A query (xk', m', n'),

$$\max_{\mathcal{M}', b, i} \Pr[(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk', m', n') : (\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}'] \\ \leq \mathrm{Guess}_A(k).$$

Notice that A makes totally $q_r(k)$ random-oracle queries and $q_l(k)$ LR queries. So we have $\Pr[\mathsf{bad}_1] \leq 2q_r(k)q_l(k)\mathsf{p}(k)\mathrm{Guess}_A(k)$. Therefore,

$$|\Pr[\mathbf{G}_2(k)] - \Pr[\mathbf{G}_1(k)]| \leq \Pr[\mathsf{bad}_1] \leq 2q_r(k)q_l(k)\mathsf{p}(k)\mathrm{Guess}_A(k). \quad (3)$$

Games $\mathbf{G}_3$ and $\mathbf{G}_2$ are identical-until-bad_2. $\mathbf{G}_3$ sets bad_2 only if the current RO_A query (xk', m', n') has been queried by the LR oracle previously. In game $\mathbf{G}_3$, if bad_2 is set, then the $H[xk', m', n']$ is overwritten with a random element from $\mathcal{R}_{\mathsf{Enc}}$. Denote by $\Pr[\mathsf{bad}_2]$ the probability that $\mathbf{G}_3$ sets bad_2. Then, we have that $|\Pr[\mathbf{G}_3(k)] - \Pr[\mathbf{G}_2(k)]| \leq \Pr[\mathsf{bad}_2]$. In order to bound $\Pr[\mathsf{bad}_2]$, we present the following lemma and postpone its proof.

```
Game $\mathbf{G}_6$
$(pk, sk) \leftarrow \mathsf{Kg}(1^k)$ ; $b \leftarrow \{0,1\}$; $C \leftarrow \emptyset$
$St \leftarrow A_1^{\mathrm{RO}_A,\mathrm{LR}}(1^k)$; $b' \leftarrow A_2^{\mathrm{RO}_A,\mathrm{DEC}}(pk, St)$
Return $(b' = b)$

On query $\mathrm{RO}_A(xk', m', n')$:
    If $H_A[xk', m', n'] = \bot$, then
        $H_A[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H_A[xk', m', n']$

On query $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    For $i \in [|\mathbf{n}|]$, then
        $\mathbf{r}[i] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
        $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_b[i]; \mathbf{r}[i])$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\bot$
    $m' \leftarrow \mathsf{Dec}(sk, c')$
    Return $m'$
```

```
Adv $B^{\mathrm{ENC}_B,\mathrm{DEC}_B}(pk)$
$St \leftarrow A_1^{\mathrm{RO}_A,\mathrm{LR}}(1^k)$
$b' \leftarrow A_2^{\mathrm{RO}_A,\mathrm{DEC}}(pk, St)$
Return $b'$

On query $\mathrm{RO}_A(xk', m', n')$:
    If $H_A[xk', m', n'] = \bot$, then
        $H_A[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H_A[xk', m', n']$

On query $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{c} \leftarrow \mathrm{ENC}_B(\mathbf{m}_0, \mathbf{m}_1)$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    $m' \leftarrow \mathrm{DEC}_B(c')$
    Return $m'$
```

Fig. 8. Game $\mathbf{G}_6$ (left) and adversary B (right) in the proof of Theorem 2. Note that in this paper we extend the set membership notations to vectors, writing $X \cup \mathbf{x}$ to mean $X \cup \{\mathbf{x}[i] | i \in [|\mathbf{x}|]\}$.

Lemma 1. *There is an IND-CCA adversary B_{upr} attacking* PKE *with advantage $\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k)$, such that*

$$\Pr[\mathsf{bad}_2] \leq 2\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) + (q_r(k) + \frac{q_l(k)\mathsf{p}(k) - 1}{2}) q_l(k)\mathsf{p}(k)\mathrm{Guess}_A(k).$$

It follows that

$$\begin{aligned} &|\Pr[\mathbf{G}_3(k)] - \Pr[\mathbf{G}_2(k)]| \\ &\leq 2\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) + (q_r(k) + \frac{q_l(k)\mathsf{p}(k) - 1}{2}) q_l(k)\mathsf{p}(k)\mathrm{Guess}_A(k). \qquad (4) \end{aligned}$$

Note that in game $\mathbf{G}_3$, the oracle answers of RO_A and the answers given to the LR oracle in reply to its RO queries are independent. Therefore, game $\mathbf{G}_4$ is a simplified version of $\mathbf{G}_3$, which implies that

$$\Pr[\mathbf{G}_4(k)] = \Pr[\mathbf{G}_3(k)]. \qquad (5)$$

Games $\mathbf{G}_5$ and $\mathbf{G}_4$ are identical-until-bad_3. Similarly, denote by $\Pr[\mathsf{bad}_3]$ the probability that $\mathbf{G}_5$ sets bad_3. We have that $|\Pr[\mathbf{G}_5(k)] - \Pr[\mathbf{G}_4(k)]| \leq \Pr[\mathsf{bad}_3]$. $\mathbf{G}_5$ sets bad_3 only if there is some tuple (xk', m', n') which has been queried by the LR oracle at least twice. Since A has high min-entropy, for any $(xk', m', n') \in T_2$, any $\mathcal{M}$ queried by A, any $b \in \{0,1\}$, and any $i \in [\mathsf{p}(k)]$, $\Pr[(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) = (xk', m', n') : (\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n})$

$\leftarrow \mathcal{M}] \leq \mathrm{Guess}_A(k)$ is negligible. Notice that A makes totally $q_l(k)$ LR queries, and for each LR query $\mathcal{M}$, the LR oracle makes $\mathsf{p}(k)$ RO queries, so we derive that $\Pr[\mathsf{bad}_3] \leq \frac{q_l(k)\mathsf{p}(k)(q_l(k)\mathsf{p}(k)-1)}{2}\mathrm{Guess}_A(k)$. Therefore,

$$|\Pr[\mathbf{G}_5(k)] - \Pr[\mathbf{G}_4(k)]| \leq \frac{q_l(k)\mathsf{p}(k)(q_l(k)\mathsf{p}(k)-1)}{2}\mathrm{Guess}_A(k). \quad (6)$$

Note that in game $\mathbf{G}_5$, both T_1 and T_2 are useless, and the vector $\mathbf{r}$ generated by the LR oracle is truly random from A's point of view. Therefore, game $\mathbf{G}_6$ is a simplified version of $\mathbf{G}_5$, which implies that

$$\Pr[\mathbf{G}_6(k)] = \Pr[\mathbf{G}_5(k)]. \quad (7)$$

Next, we construt an IND-CCA adversary B attacking PKE as shown in Fig. 8. In order to distinguish B's own decryption oracle (in the sense of IND-CCA) and A's decryption oracle (in the sense of IND-CDA2), we denote by DEC_B (resp. ENC_B) B's decryption (resp. encryption) oracle. B uses ENC_B to answer A's LR queries, and uses DEC_B to answer A's decryption queries. B perfectly simulates game $\mathbf{G}_6$ for A, and that B wins game $\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},B}$ if and only if A wins game $\mathbf{G}_6$. Hence,

$$\Pr[\mathbf{G}^{\text{ind-cca}}_{\mathsf{PKE},B}(k)] = \Pr[\mathbf{G}_6(k)]. \quad (8)$$

Combining equations (1)-(8), we derive that

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{RtP},A}(k) \leq\ & \mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B}(k) + 4\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) \\ & + (6q_r(k) + 2q_l(k)\mathsf{p}(k) - 2)q_l(k)\mathsf{p}(k)\mathrm{Guess}_A(k).\end{aligned}$$

Now, we catch up with the proof of Lemma 1.

Proof (of Lemma 1). We say that "$\mathbf{G}_4$ sets bad_2" (resp. "$\mathbf{G}_5$ sets bad_2") if A submits an RO_A query (xk', m', n'), such that $(xk', m', n') \in T_2$, in $\mathbf{G}_4$ (resp. $\mathbf{G}_5$).

Since $\mathbf{G}_4$ is a simplified version of $\mathbf{G}_3$, and $\mathbf{G}_5$ and $\mathbf{G}_4$ are identical-until-bad_3,

$$\begin{aligned}\Pr[\mathsf{bad}_2] = \Pr[\mathbf{G}_4 \text{ sets } \mathsf{bad}_2] &\leq \Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] + \Pr[\mathsf{bad}_3] \\ &\leq \Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] + \frac{q_l(k)\mathsf{p}(k)(q_l(k)\mathsf{p}(k)-1)}{2}\mathrm{Guess}_A(k). \quad (9)\end{aligned}$$

To bound $\Pr[\mathbf{G}_5$ sets $\mathsf{bad}_2]$, we consider an IND-CCA adversary B_{upr} as shown in Fig. 9. Similarly, denote by $\mathrm{ENC}_{B_{upr}}$ (resp. $\mathrm{DEC}_{B_{upr}}$) B_{upr}'s encryption (resp. decryption) oracle in the sense of IND-CCA. Let $\widetilde{b}$ be the

```
**Adversary** $B_{upr}^{\mathrm{ENC}_{B_{upr}},\mathrm{DEC}_{B_{upr}}}(pk)$
$a, b^* \leftarrow \{0,1\}$;  $T_1, T_2 \leftarrow \emptyset$
$St \leftarrow A_1^{\mathrm{RO}_A,\mathrm{LR}}(1^k)$;  $b' \leftarrow A_2^{\mathrm{RO}_A,\mathrm{DEC}}(pk, St)$
Return $b^*$

**On query** $\mathrm{RO}_A(xk', m', n')$:
    $T_1 \leftarrow T_1 \cup \{(xk', m', n')\}$
    If $(xk', m', n') \in T_2$, then
        $b^* \leftarrow a$
    If $H_A[xk', m', n'] = \perp$, then
        $H_A[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H_A[xk', m', n']$

**On query** $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{m}_a^{\mathsf{ch}} \leftarrow \mathbf{m}_a$
    $\mathbf{m}_{1-a}^{\mathsf{ch}} \leftarrow \mathsf{MSP}^{|\mathbf{n}|}$
    For $i \in [|\mathbf{n}|]$,
        $T_2 \leftarrow T_2 \cup \{(\mathbf{xk}[i], \mathbf{m}_a[i], \mathbf{n}[i])\}$
    $\mathbf{c} \leftarrow \mathrm{ENC}_{B_{upr}}(\mathbf{m}_0^{\mathsf{ch}}, \mathbf{m}_1^{\mathsf{ch}})$
    Return $\mathbf{c}$

**On query** $\mathrm{DEC}(c')$:
    $m' \leftarrow \mathrm{DEC}_{B_{upr}}(c')$
    Return $m'$
```

```
**Game** $\mathbf{G}_{B_{upr},A}^{\mathrm{sim}}$
$a, b^* \leftarrow \{0,1\}$;  $C, T_1, T_2 \leftarrow \emptyset$;  $\widetilde{b} \leftarrow \{0,1\}$
$St \leftarrow A_1^{\mathrm{RO}_A,\mathrm{LR}}(1^k)$;  $b' \leftarrow A_2^{\mathrm{RO}_A,\mathrm{DEC}}(pk, St)$
Return $b^*$

**On query** $\mathrm{RO}_A(xk', m', n')$:
    $T_1 \leftarrow T_1 \cup \{(xk', m', n')\}$
    If $(xk', m', n') \in T_2$, then
        $\mathsf{bad}_2 \leftarrow \mathsf{true}$;  $b^* \leftarrow a$
    If $H_A[xk', m', n'] = \perp$, then
        $H_A[xk', m', n'] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
    Return $H_A[xk', m', n']$

**On query** $\mathrm{LR}(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{m}_a^{\mathsf{ch}} \leftarrow \mathbf{m}_a$
    $\mathbf{m}_{1-a}^{\mathsf{ch}} \leftarrow \mathsf{MSP}^{|\mathbf{n}|}$
    For $i \in [|\mathbf{n}|]$,
        $T_2 \leftarrow T_2 \cup \{(\mathbf{xk}[i], \mathbf{m}_a[i], \mathbf{n}[i])\}$
        $\mathbf{r}[i] \leftarrow \mathcal{R}_{\mathsf{Enc}}$
        $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_{\widetilde{b}}^{\mathsf{ch}}[i]; \mathbf{r}[i])$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

**On query** $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{Dec}(sk, c')$
    Return $m'$
```

Fig. 9. Adversary B_{upr} (left) and game $\mathbf{G}_{B_{upr},A}^{\mathrm{sim}}$ (right) in the proof of Lemma 1.

challenge bit in game $\mathbf{G}_{\mathsf{PKE},B_{upr}}^{\text{ind-cca}}$. Denote by $\mathbf{G}_{B_{upr},A}^{\mathrm{sim}}$ the game simulated by B_{upr} for A (as shown in Fig. 9). B_{upr}'s advantage is as follows.

$$\mathbf{Adv}_{\mathsf{PKE},B_{upr}}^{\text{ind-cca}}(k) = 2\Pr[\mathbf{G}_{\mathsf{PKE},B_{upr}}^{\text{ind-cca}}(k)] - 1 = 2\Pr[b^* = \widetilde{b}] - 1 \tag{10}$$

$$= 2(\Pr[b^* = \widetilde{b} \mid \widetilde{b} = a]\Pr[\widetilde{b} = a] + \Pr[b^* = \widetilde{b} \mid \widetilde{b} \neq a]\Pr[\widetilde{b} \neq a]) - 1 \tag{11}$$

$$= \Pr[b^* = \widetilde{b} \mid \widetilde{b} = a] + \Pr[b^* = \widetilde{b} \mid \widetilde{b} \neq a] - 1 \tag{12}$$

Equations (10)-(11) are trivial. Since a is uniformly random chosen from $\{0,1\}$, $\Pr[\widetilde{b} = a] = \Pr[\widetilde{b} \neq a] = \frac{1}{2}$. This justifies Equation (12).

For $\Pr[b^* = \widetilde{b} \mid \widetilde{b} = a]$, we have the following equations.

$$\begin{aligned}
&\Pr[b^* = \widetilde{b} \mid \widetilde{b} = a] \\
=&\Pr[b^* = \widetilde{b} \mid (\widetilde{b} = a) \wedge (\mathbf{G}_{B_{upr},A}^{\mathrm{sim}} \text{ sets } \mathsf{bad}_2)]\Pr[\mathbf{G}_{B_{upr},A}^{\mathrm{sim}} \text{ sets } \mathsf{bad}_2 \mid \widetilde{b} = a] \\
&\quad + \Pr[b^* = \widetilde{b} \mid (\widetilde{b} = a) \wedge \neg(\mathbf{G}_{B_{upr},A}^{\mathrm{sim}} \text{ sets } \mathsf{bad}_2)] \\
&\qquad\qquad \cdot \Pr[\neg(\mathbf{G}_{B_{upr},A}^{\mathrm{sim}} \text{ sets } \mathsf{bad}_2) \mid \widetilde{b} = a]
\end{aligned} \tag{13}$$

$$=\Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] + \frac{1}{2}\Pr[\neg(\mathbf{G}_5 \text{ sets } \mathsf{bad}_2)] \tag{14}$$

$$=\frac{1}{2}\Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] + \frac{1}{2}. \tag{15}$$

Equation (13) is trivial. We notice that when $\widetilde{b} = a$, the simulated game $\mathbf{G}^{\text{sim}}_{B_{upr},A}$ is the same as $\mathbf{G}_5$ from A's point of view, so we have $\Pr[\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2 \mid \widetilde{b} = a] = \Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2]$. We also note that if $\mathbf{G}^{\text{sim}}_{B_{upr},A}$ sets bad_2, then B_{upr} outputs $b^* = a$, otherwise B_{upr} outputs $b^* \leftarrow \{0,1\}$. Therefore, $\Pr[b^* = \widetilde{b} \mid (\widetilde{b} = a) \wedge (\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)] = 1$ and $\Pr[b^* = \widetilde{b} \mid (\widetilde{b} = a) \wedge \neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)] = \frac{1}{2}$. This justifies Equation (14). Equation (15) is because $\Pr[\neg(\mathbf{G}_5 \text{ sets } \mathsf{bad}_2)] = 1 - \Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2]$.

With similar analysis, for $\Pr[b^* = \widetilde{b} \mid \widetilde{b} \neq a]$, we have the following equations.

$$\begin{aligned}
&\Pr[b^* = \widetilde{b} \mid \widetilde{b} \neq a] \\
&= \Pr[b^* = \widetilde{b} \mid (\widetilde{b} \neq a) \wedge (\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)]\Pr[\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2 \mid \widetilde{b} \neq a] \\
&\quad + \Pr[b^* = \widetilde{b} \mid (\widetilde{b} \neq a) \wedge \neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)] \\
&\qquad \cdot \Pr[\neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2) \mid \widetilde{b} \neq a] \qquad (16) \\
&= 0 + \frac{1}{2}\Pr[\neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2) \mid \widetilde{b} \neq a] \qquad (17) \\
&= \frac{1}{2}(1 - \Pr[\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2 \mid \widetilde{b} \neq a]) \qquad (18) \\
&\geq \frac{1}{2}(1 - q_l(k)q_r(k)\mathsf{p}(k)\mathrm{Guess}_A(k)). \qquad (19)
\end{aligned}$$

Equation (16) is trivial. B_{upr} outputs $b^* = a$ when $\mathbf{G}^{\text{sim}}_{B_{upr},A}$ sets bad_2, so we have that $\Pr[b^* = \widetilde{b} \mid (\widetilde{b} \neq a) \wedge (\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)] = 0$. Considering that B_{upr} outputs $b^* \leftarrow \{0,1\}$ when $\mathbf{G}^{\text{sim}}_{B_{upr},A}$ does not set bad_2, so we have $\Pr[b^* = \widetilde{b} \mid (\widetilde{b} \neq a) \wedge \neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2)] = \frac{1}{2}$. We have justified Equation (17). Equation (18) is because $\Pr[\neg(\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2) \mid \widetilde{b} \neq a] = 1 - \Pr[\mathbf{G}^{\text{sim}}_{B_{upr},A} \text{ sets } \mathsf{bad}_2 \mid \widetilde{b} \neq a]$. Notice that $\widetilde{b} \neq a$ implies $\widetilde{b} = 1 - a$, i.e., the challenge ciphertext vectors A received are the encryption of some uniformly random chosen message vectors. Thus the challenge ciphertext vectors do not contain any information about any $\mathbf{m}_a$. Besides, in the simulated game $\mathbf{G}^{\text{sim}}_{B_{upr},A}$, the answers (of RO_A, the LR oracle, and the decryption oracle) given to A do not contain any information about the $\mathbf{xk}$ and $\mathbf{n}$ sampled by the LR oracle. Therefore, for any tuple $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}$ sampled by the LR oracle in game $\mathbf{G}^{\text{sim}}_{B_{upr},A}$, A

has no additional information about any element of $\{(\mathbf{xk}[i], \mathbf{m}_b[i], \mathbf{n}[i]) \mid i \in [\mathsf{p}(k)], b \in \{0,1\}\}$. Recall that $\mathbf{G}^{\mathrm{sim}}_{B_{upr},A}$ sets bad_2 only if A succeeds in guessing some element in $\{(\mathbf{xk}[i], \mathbf{m}_a[i], \mathbf{n}[i]) \mid i \in [\mathsf{p}(k)]\}$ for some $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}$ sampled by the LR oracle and the a sampled by B_{upr}. Notice that the total number of random-oracle (resp. LR-oracle) queries of A is $q_r(k)$ (resp. $q_l(k)$). So we derive that $\Pr[\mathbf{G}^{\mathrm{sim}}_{B_{upr},A}$ sets $\mathsf{bad}_2 \mid \widetilde{b} \neq a] \leq q_l(k) q_r(k) \mathsf{p}(k) \mathrm{Guess}_A(k)$. We have justified Equation (19).

Combining Equations (12), (15) and (19), we derive that

$$\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) \geq \frac{1}{2}(\Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] - q_l(k) q_r(k) \mathsf{p}(k) \mathrm{Guess}_A(k)). \quad (20)$$

Hence,

$$\Pr[\mathbf{G}_5 \text{ sets } \mathsf{bad}_2] \leq 2\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) + q_l(k) q_r(k) \mathsf{p}(k) \mathrm{Guess}_A(k). \quad (21)$$

Combining Equations (9) and (21), we obtain that

$$\Pr[\mathsf{bad}_2] \leq 2\mathbf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},B_{upr}}(k) + (q_r(k) + \frac{q_l(k)\mathsf{p}(k) - 1}{2}) q_l(k) \mathsf{p}(k) \mathrm{Guess}_A(k).$$

□

Remark 4 The N-PKE scheme RtP is a special case of the ROM scheme NPE in [8, Figure 6], but it seems that the original, generic ROM scheme NPE proposed in [8, Figure 6] does not achieve IND-CDA2 security. The reason is as follows. In [8], the security of NPE is guaranteed by the IND-CCA security of the traditional PKE scheme, and the prf security and the ror security (defined in [8]) of their proposed building block, hedged extractor. The prf security focuses on the case that the seeds are random and confidential, and the ror security focuses on the case that the nonces are unpredictable. In other words, the security of hedged extractor just considers the case that either the seeds or the nonces have high entropy. And the IND-CDA2 security of N-PKE should be guaranteed as long as the seeds, messages and nonces jointly have high min-entropy.

With respect to RIND-CDA2 security, with similar technique we have the following corollary.

Corollary 1. *If* PKE *is a traditional IND-CCA secure PKE scheme, then N-PKE scheme* RtP*, w.r.t. a nonce generator* NG*, is RIND-CDA2 secure in the random oracle model.*

$\mathsf{NDKg}(1^k)$	$\mathsf{NDSKg}(1^k)$	$\mathsf{NDEnc}(pk, xk, m, n)$	$\mathsf{NDDec}(sk, c)$
$(pk_n, sk_n) \leftarrow \mathsf{NKg}(1^k)$ $(pk_d, sk_d) \leftarrow \mathsf{DKg}(1^k)$ $pk \leftarrow (pk_n, pk_d)$ $sk \leftarrow (sk_n, sk_d)$ Return (pk, sk)	$xk \leftarrow \mathsf{NSKg}(1^k)$ Return xk	Parse $pk = (pk_n, pk_d)$ $y \leftarrow \mathsf{NEnc}(pk_n, xk, m, n)$ $c \leftarrow \mathsf{DEnc}(pk_d, y)$ Return c	Parse $sk = (sk_n, sk_d)$ $y \leftarrow \mathsf{DDec}(sk_d, c)$ $m \leftarrow \mathsf{NDec}(sk_n, y)$ Return m

Fig. 10. N-PKE scheme $\mathsf{NtD} = (\mathsf{NDKg}, \mathsf{NDSKg}, \mathsf{NDEnc}, \mathsf{NDDec})$.

5 Construction of H-PKE in the standard model

Generic construction. Let $\mathsf{NE} = (\mathsf{NKg}, \mathsf{NSKg}, \mathsf{NEnc}, \mathsf{NDec})$ be an N-PKE scheme, w.r.t. a nonce generator NG. Let $\mathsf{DE} = (\mathsf{DKg}, \mathsf{DEnc}, \mathsf{DDec})$ be a D-PKE scheme. Recall the transform Nonce-then-Deterministic NtD $= (\mathsf{NDKg}, \mathsf{NDSKg}, \mathsf{NDEnc}, \mathsf{NDDec})$ proposed in [16] as shown in Fig. 10.

In [16], Hoang et al. consider SOA security of NtD, showing that if NE is N-SO-CPA (resp. N-SO-CCA) secure, and DE is D-SO-CPA (resp. D-SO-CCA and unique-ciphertext) secure, then NtD is HN-SO-CPA (resp. HN-SO-CCA) secure. The HN-SOA security notions formalized in [16] are non-adaptive. Therefore, the HN-SO-CCA security formalized in [16] does not imply our HN-IND security.

In this section, we point out that NtD also applies to the HN-IND setting. Specifically, we assume NE is NBP1 and NBP2 secure, and DE is adaptively CCA secure and unique-ciphertext. Additionally, we require that NE is *entropy-preserving*, which is a property of N-PKE formalized by Hoang et al. [16].

Denote by $\mathsf{Entrp}_{\mathsf{NE}}(\theta(k))$ the conditional min-entropy of $\mathsf{NEnc}(pk_n, xk, m, n)$ given X, where X is a random variable such that the conditional min-entropy of (xk, m, n) is at least $\theta(k)$, and $(pk_n, sk_n) \leftarrow \mathsf{NKg}(1^k)$ is independent of (xk, m, n, X). NE is called *entropy-preserving*, if for any $\theta(k)$ satisfying that $2^{-\theta(k)}$ is negligible, then $2^{-\mathsf{Entrp}_{\mathsf{NE}}(\theta(k))}$ is also negligible.

Formally, we have the following theorem.

Theorem 3. *For an NBP1, NBP2 secure and entropy-preserving N-PKE scheme* NE *and a D-PKE scheme* DE*, let* NtD *be an N-PKE scheme defined in Fig. 10.*

(i) If DE *is adaptively CCA secure and unique-ciphertext, then* NtD *is HN-IND secure.*
(ii) If DE *is ACD-CCA secure and unique-ciphertext, then* NtD *is RSV-version HN-IND secure.*

Proof. Firstly, we prove that NtD is NBP1 secure. The proof of NBP2 security is similar, which we will omit here.

```
Adv $B_{nbp1}^{\mathrm{ENC}_B,\mathrm{DEC}_B}(pk_n)$
$(pk_d, sk_d) \leftarrow \mathsf{DKg}(1^k)$
$pk \leftarrow (pk_n, pk_d)$
$b' \leftarrow A^{\mathrm{ENC},\mathrm{DEC}}(pk)$
Return $b'$
```

```
On query $\mathrm{ENC}(m_0, m_1, \eta)$:
    $y \leftarrow \mathrm{ENC}_B(m_0, m_1, \eta)$
    $c \leftarrow \mathsf{DEnc}(pk_d, y)$
    Return $c$
```

```
On query $\mathrm{DEC}(c')$:
    $y' \leftarrow \mathsf{DDec}(sk_d, c')$
    $m' \leftarrow \mathrm{DEC}_B(y')$
    Return $m'$
```

```
Adv $B_1^{\mathrm{ENC}_B}(1^k)$
$(pk_n, sk_n) \leftarrow \mathsf{NKg}(1^k)$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$
$St_B \leftarrow (pk_n, sk_n, St)$
Return $St_B$
```

```
On query $\mathrm{DEC}(c')$:
    $y' \leftarrow \mathrm{DEC}_B(c')$
    If $y' = \perp$, then return $\perp$
    $m' \leftarrow \mathsf{NDec}(sk_n, y')$
    Return $m'$
```

```
Adv $B_2^{\mathrm{DEC}_B}(pk_d, St_B)$
Parse $St_B = (pk_n, sk_n, St)$
$pk \leftarrow (pk_n, pk_d)$
$b' \leftarrow A_2^{\mathrm{DEC}}(pk, St)$
Return $b'$
```

```
Alg. $\mathsf{MST}_{\text{n-d}}(\mathcal{M}, pk_n)(1^k)$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{y}_0 \leftarrow \mathsf{NEnc}(pk_n, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})$
    $\mathbf{y}_1 \leftarrow \mathsf{NEnc}(pk_n, \mathbf{xk}, \mathbf{m}_1, \mathbf{n})$
    Return $(\mathbf{y}_0, \mathbf{y}_1)$
```

```
On query $\mathrm{LR}(\mathcal{M})$:
    $\mathbf{c} \leftarrow \mathrm{ENC}_B(\mathsf{MST}_{\text{n-d}}(\mathcal{M}, pk_n))$
    Return $\mathbf{c}$
```

Fig. 11. Adversary B_{nbp1} (up) and adversary B (down) in the proof of Theorem 3.

For any NBP1 adversary A attacking NtD, we present an NBP1 adversary B_{nbp1} attacking NE as shown in Fig. 11. Denote by ENC_B (resp. DEC_B) B_{nbp1}'s encryption (resp. decryption) oracle in the sense of NBP1. Note that DE is unique-ciphertext. As a result, for any decryption query c' of A, if $y' \leftarrow \mathsf{DDec}(sk_d, c')$ is one of the challenge ciphertext B_{nbp1} received, then c' is also one of the challenge ciphertext A received. Thus the DEC oracle simulated by B_{nbp1} is identical to the real DEC oracle in game $\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NtD},A}$. It's easy to see that the ENC oracle simulated by B_{nbp1} is identical to the real ENC oracle of A. Therefore, B_{nbp1} perfectly simulates game $\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NtD},A}$ for A, and B_{nbp1} wins game $\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NE},B_{nbp1}}$ if and only if A wins $\mathbf{G}^{\mathrm{nbp1}}_{\mathsf{NtD},A}$. So we derive that $\mathbf{Adv}^{\mathrm{nbp1}}_{\mathsf{NtD},A}(k) = \mathbf{Adv}^{\mathrm{nbp1}}_{\mathsf{NE},B_{nbp1}}(k)$.

Next, we show that NtD is IND-CDA2 secure. We call a PPT algorithm $\mathsf{MST}_{\text{n-d}}$ a *message sampler transformer from N-PKE to D-PKE*, if it takes a message sampler for N-PKE (and some state information) as input, and acts as a message sampler for D-PKE (see Fig. 11). For any legitimate PPT IND-CDA2 adversary A having high min-entropy, we construct a $\mathsf{MST}_{\text{n-d}}$ and an adaptively CCA adversary $B = (B_1, B_2)$ attacking DE as shown in Fig. 11. Similarly, denote by ENC_B (resp. DEC_B) B's encryption (resp. decryption) oracle in the sense of adaptive CCA. B perfectly simulates game $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NtD},A}$ for A. Since NE is entropy-preserving, the construction of $\mathsf{MST}_{\text{n-d}}$ guarantees that B is legitimate and has high min-entropy. Note that B wins game $\mathbf{G}^{\mathrm{cca}}_{\mathsf{DE},B}$ if and only if A wins $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NtD},A}$. So we derive that $\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{NtD},A}(k) = \mathbf{Adv}^{\mathrm{cca}}_{\mathsf{DE},B}(k)$.

With similar techniques, we can prove the RIND-CDA2 security of NtD. □

Remark 5 Theorem 3 applies to both the ROM constructions and the standard-model constructions.

Concrete constructions. According to Theorem 3, let NE be the NBP1 and NBP2 secure standard-model construction proposed in [8], and DE be the ACD-CCA secure standard-model construction proposed in [20], then we obtain an RSV-version HN-IND secure N-PKE scheme NtD in the standard model.

Now we turn to HN-IND security of NtD. According to Theorem 3, what remains is to construct a (unique-ciphertext) standard-model D-PKE scheme achieving adaptively CCA security. Considering IND-CDA2 security in the setting of H-PKE, instead of N-PKE, if the length of the randomness is zero (i.e., $|\mathbf{r}[i]| = 0$ for all $i \in [|\mathsf{p}(k)|]$), then IND-CDA2 security actually becomes adaptive CCA security for D-PKE. Therefore, the problem that construct an IND-CDA2 secure N-PKE scheme in the standard model is at least as hard as the one that construct a fully adaptively CCA secure D-PKE scheme in the standard model. To the best of our knowledge, the latter is still an open problem. On the other hand, Theorem 3 shows that if an adaptively CCA secure (and unique-ciphertext) standard-model D-PKE scheme is constructed, then we will have an N-PKE scheme achieving HN-IND security in the standard model.

Some notes on adaptively CCA secure D-PKE. Recall that Bellare et al. [2] presented an adaptively IND secure D-PKE scheme, by showing any PKE scheme, achieving a special anonymity (i.e., the ANON security in [2]) and non-adaptive IND-CDA security simultaneously, achieves (adaptively) IND-CDA security. Although the conclusion cannot be employed to show an adaptively CCA secure D-PKE scheme directly, we note that it can be transformed to the setting of N-PKE under CCA attacks. For completeness, we present the transform in Appendix A.

More specifically, in Appendix A, we formalize the notion of ANON-CCA security *for N-PKE*, and show that if an N-PKE scheme achieves non-adaptive IND-CDA *(not IND-CDA2)* and ANON-CCA security, then it achieves IND-CDA2 security. We stress that very recently, Boldyreva et al. [10] showed a similar conclusion (for general PKE). But their formalized ANON-CCA security is stronger than ours (i.e., informally, the adversary can make decryption queries under two secret keys). More importantly, their conclusion, informally with our notations in this paper, is that "non-adaptive IND-CDA2 + stronger ANON-CCA $\Rightarrow$ IND-CDA2". Our conclusion shows that the same result can be obtained under some weaker assumptions.

Acknowledgment. We thank the anonymous reviewers for their helpful comments. The first author was supported by National Natural Science Foundation of China (No. 61702125), and Scientific Research Foundation for Post-doctoral Researchers of Guangzhou (No. gdbsh2016020). The second author was National Natural Science Foundation of China (No. 61572235), Guangdong Natural Science Funds for Distinguished Y-oung Scholar (No. 2015A030306045), and Pearl River S&T Nova Program of Guangzhou. The third author was partly supported by the Program for Innovative Research Team in Education Department of Guangdong Province Under Grant No.2015KCXTD014. and No.2016KCXTD017. The sixth author was supported by National Natural Science Foundation of China (No. 61472091), National Natural Science Foundation for Outstanding Youth Foundation (No. 61722203), and the State Key Laboratory of Cryptology, Beijing, China.

References

1. Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. Advances in Cryptology-CRYPTO 2007, pp. 535-552. Springer (2007).
2. Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged public-key encryption: How to protect a-gainst bad randomness. Advances in Cryptology-ASIACRYPT 2009, pp. 232-249. Springer (2009).
3. Mihir Bellare, Rafael Dowsley, and Sriram Keelveedhi. How Secure is Deterministic Encryption? IACR International Workshop on Public Key Cryptography. Springer (2015).
4. Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart. Deterministic encryption: Definitional equivalences and constructions without random oracles. In Annual International Cryptology Conference-CRYPTO 2008, pp. 360-378. Springer (2008).
5. Mihir Bellare, and Viet Tung Hoang. Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model. In Advances in Cryptology-EUROCRYPT 2015, volume 9057 of LNCS, pp. 627-656. Springer (2015).
6. Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi. Instantiating random oracles via UCEs. Advances in Cryptology-CRYPTO 2013, pp. 398-415. Springer (2013).
7. Mihir Bellare, and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. In EUROCRYPT 2006. LNCS, vol. 4004, pp. 409-426. Springer (2006).
8. Mihir Bellare, and Bjorn Tackmann. Nonce-based cryptography: retaining security when randomness fails. Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 729-757. Springer (2016).
9. Alexandra Boldyreva, Serge Fehr, and Adam O'Neill. On notions of security for deterministic encryption, and efficient constructions without random oracles. Advances in Cryptology-CRYPTO 2008, pp. 335-359. Springer (2008).

10. Alexandra Boldyreva, Christopher Patton, and Thomas Shrimpton. Hedging public-key encryption in the real world. In Annual International Cryptology Conference-CRYPTO 2017, pp. 462-494. Springer (2017).
11. Zvika Brakerski, and Gil Segev. Better security for deterministic public-key encryption: The auxiliary-input setting. In CRYPTO 2011, volume 6841 of LNCS, pp. 543-560. Springer (2011).
12. David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. Leakage-abuse attacks against searchable encryption. In ACM CCS 2015, pp. 668-679. ACM Press (2015).
13. Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham. On the Practical Exploitability of Dual EC in TLS Implementations. In USENIX Security, volume 1 (2014).
14. Benjamin Fuller, Adam O'Neill, and Leonid Reyzin. A unified approach to deterministic encryption: New constructions and a connection to computational entropy. In TCC 2012, volume 7194 of LNCS, pp. 582-599. Springer (2012).
15. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In USENIX Security Symposium, pp. 205-220 (2012).
16. Viet Tung Hoang, Jonathan Katz, Adam O'Neill, and Mohammad Zaheri. Selective-Opening Security in the Presence of Randomness Failures. In Advances in Cryptology-ASIACRYPT 2016. Proceedings, Part II 22, pp. 278-306. Springer (2016).
17. Ilya Mironov, Omkant Pandey, Omer Reingold, and Gil Segev. Incremental deterministic public-key encryption. In EUROCRYPT 2012, volume 7237 of LNCS, pp. 628-644. Springer (2012).
18. B. Kaliski. Public-Key Cryptography Standards (PKCS) # 1: RSA Cryptography Specifications Version 2.1 2003. RFC 3447. https://tools.ietf.org/html/rfc3447
19. Charles Rackoff, and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. Annual International Cryptology Conference. Springer (1991).
20. Ananth Raghunathan, Gil Segev, and Salil Vadhan. Deterministic public-key encryption for adaptively chosen plaintext distributions. In: EUROCRYPT 2013, volume 7881 of LNCS, pp. 93-110. Springer (2013).
21. Thomas Ristenpart, and Scott Yilek. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. NDSS (2010).
22. Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-126 (1978).
23. Daniel Wichs. Barriers in cryptography with weak, correlated and leaky sources. Proceedings of the 4th conference on Innovations in Theoretical Computer Science. ACM (2013).

A. From non-adaptive IND-CDA to adaptive IND-CDA2

Firstly, we formalize the notion of anonymity for IND-CDA2 for N-PKE. Then we will present our theorem. Consider game $\mathbf{G}^{\text{anon-cca}}_{\mathsf{NE},A}$ as shown in Fig. 12. For the adversary A in game $\mathbf{G}^{\text{anon-cca}}_{\mathsf{NE},A}$, we can similarly define

```
Game $\mathbf{G}^{\text{anon-cca}}_{\mathsf{NE},A}(k)$
$(pk_0, sk_0) \leftarrow \mathsf{NKg}(1^k)$
$(pk_1, sk_1) \leftarrow \mathsf{NKg}(1^k)$
$b \leftarrow \{0,1\}$; $C \leftarrow \emptyset$
$\mathsf{kr} \leftarrow \mathsf{false}$
$b' \leftarrow A^{\text{ENC}_0,\text{LR},\text{DEC}_0}(1^k)$
Return $(b' = b)$
```

```
$\text{ENC}_0(\mathcal{M})$
If $\mathsf{kr} = \mathsf{true}$, then
  return $\perp$
$(\mathbf{m}, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
$\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}, \mathbf{n})$
$C \leftarrow C \cup \mathbf{c}$
Return $\mathbf{c}$
```

```
$\text{LR}(\mathcal{M})$
If $\mathsf{kr} = \mathsf{true}$, then
  return $\perp$
$\mathsf{kr} \leftarrow \mathsf{true}$
$(\mathbf{m}, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
$\mathbf{c} \leftarrow \mathsf{NEnc}(pk_b, \mathbf{xk}, \mathbf{m}, \mathbf{n})$
$C \leftarrow C \cup \mathbf{c}$
Return $(pk_0, pk_1, \mathbf{c})$
```

```
$\text{DEC}_0(c)$
If $\mathsf{kr} = \mathsf{false}$, then
  return $\perp$
If $c \in C$, then
  return $\perp$
$m \leftarrow \mathsf{NDec}(sk_0, c)$
Return $m$
```

Fig. 12. Game for defining ANON-CCA security of an N-PKE scheme NE.

legitimate adversary, and the adversary *having high min-entropy (resp. high block-source min-entropy).* We do not repeat the details here.

Definition 7 (ANON-CCA). *An N-PKE scheme* NE *is ANON-CCA secure (resp. block-source ANON-CCA secure), if for any legitimate PP-T adversary A having high min-entropy (resp. high block-source min-entropy), its advantage* $\mathbf{Adv}^{\text{anon-cca}}_{\mathsf{NE},A}(k) = 2\Pr[\mathbf{G}^{\text{anon-cca}}_{\mathsf{NE},A}(k)] - 1$ *is negligible, where game* $\mathbf{G}^{\text{anon-cca}}_{\mathsf{NE},A}$ *is defined in Fig. 12.*

Theorem 4. *Let* NE *be an N-PKE scheme. If* NE *achieves non-adaptive IND-CDA security and ANON-CCA security simultaneously, then it also achieves adaptive IND-CDA2 security.*

Proof. The proof is based on the approach proposed in [2]. For any PPT legitimate IND-CDA2 adversary A having high min-entropy and making $q(k)$ LR queries, denote by $\mathbf{G}^{\text{ind-cda2-}b}_{\mathsf{NE},A}$ $(b \in \{0,1\})$ the game as follows: $\mathbf{G}^{\text{ind-cda2-}b}_{\mathsf{NE},A}$ is the same as $\mathbf{G}^{\text{ind-cda2}}_{\mathsf{NE},A}$, except that b is a fixed value in $\{0,1\}$, and the final output of this game is b'. A standard argument shows that the advantage of A can be written as $\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{NE},A}(k) = |\Pr[\mathbf{G}^{\text{ind-cda2-1}}_{\mathsf{NE},A}(k) - \Pr[\mathbf{G}^{\text{ind-cda2-0}}_{\mathsf{NE},A}(k)]|$. Games $\mathbf{G}^{\text{ind-cda-}b}_{\mathsf{NE},A}$, $\mathbf{G}^{\text{anon-cca-}b}_{\mathsf{NE},A}$ $(b \in \{0,1\})$ (resp. the corresponding advantages) can be defined (resp. written) similarly.

Consider the sequence of games in Fig. 13. Game $\mathbf{G}_{-1}$ is the same as game $\mathbf{G}^{\text{ind-cda2-0}}_{\mathsf{NE},A}$, i.e., $\Pr[\mathbf{G}_{-1}] = \Pr[\mathbf{G}^{\text{ind-cda2-0}}_{\mathsf{NE},A}]$. Game $\mathbf{G}_0$ introduces (pk_1, sk_1), which is useless in $\mathbf{G}_0$. So we have $\Pr[\mathbf{G}_0] = \Pr[\mathbf{G}_{-1}]$. For $0 \le i \le q(k)$, game $\mathbf{G}_i$ is the same as $\mathbf{G}_0$, except that for the j^{th} LR query of A, if $j \le i$, the challenge ciphertext vector $\mathbf{c}$ is an encryption of $\mathbf{m}_1$ (under the public key pk_0), instead of an encryption of $\mathbf{m}_0$. Therefore, $\mathbf{G}_{q(k)}$ is identical to $\mathbf{G}^{\text{ind-cda2-1}}_{\mathsf{NE},A}$. Hence, what remains is to show the indistinguishability between $\mathbf{G}_i$ and $\mathbf{G}_{i+1}$ for any $0 \le i \le q(k) - 1$.

As shown in Fig. 13, for $0 \le i \le q(k) - 1$, game $\mathbf{H}_i$ is the same as $\mathbf{G}_i$, except that for the i^{th} LR query of A, the challenge ciphertext vector $\mathbf{c}$ is an encryption of $\mathbf{m}_0$ under pk_1, instead of an encryption of $\mathbf{m}_1$ under pk_0.

```
Games $\mathbf{G}_{-1}$, $\boxed{\mathbf{G}_0}$
$(pk_0, sk_0) \leftarrow \mathsf{NKg}(1^k)$; $\boxed{(pk_1, sk_1) \leftarrow \mathsf{NKg}(1^k)}$
$C \leftarrow \emptyset$;  $j \leftarrow 0$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$;  $b' \leftarrow A_2^{\mathrm{DEC}}(pk_0, St)$
Return $b'$

On query LR($\mathcal{M}$):
    $j \leftarrow j + 1$;  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query DEC($c'$):
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{NDec}(c')$
    Return $m'$
```

```
Games $\mathbf{G}_i$, $\boxed{\mathbf{H}_i}$, $\colorbox{lightgray}{$\mathbf{H}'_i$}$
$(pk_0, sk_0) \leftarrow \mathsf{NKg}(1^k)$; $(pk_1, sk_1) \leftarrow \mathsf{NKg}(1^k)$
$C \leftarrow \emptyset$;  $j \leftarrow 0$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$;  $b' \leftarrow A_2^{\mathrm{DEC}}(pk_0, St)$
Return $b'$

On query LR($\mathcal{M}$):
    $j \leftarrow j + 1$;  $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    If $j < i$, then $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_1, \mathbf{n})$
    If $j = i$, then $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_1, \mathbf{n})$
    $\boxed{\text{If } j = i, \text{ then } \mathbf{c} \leftarrow \mathsf{NEnc}(pk_1, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})}$
    $\colorbox{lightgray}{If $j = i$, then $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_1, \mathbf{xk}, \mathbf{m}_1, \mathbf{n})$}$
    If $j > i$, then $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query DEC($c'$):
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{NDec}(c')$
    Return $m'$
```

Fig. 13. Games $\mathbf{G}_{-1} - \mathbf{G}_q$ and $\mathbf{H}_0 - \mathbf{H}_{q-1}$ in the proof of Theorem 4. Boxed code is only executed in the games specified by the game names in the same box style.

Game $\mathbf{H}'_i$ is the same as $\mathbf{H}_i$, except that for the i^{th} LR query of A, the challenge ciphertext vector $\mathbf{c}$ is an encryption of $\mathbf{m}_1$ under pk_1, instead of an encryption of $\mathbf{m}_0$ under pk_1. Formally, we have three claims below.

Claim 1 *For any $1 \leq i \leq q(k)$, there is an ANON-CCA adversary B_{an1} such that $\mathbf{Adv}^{\text{anon-cca}}_{\mathsf{NE},B_{an1}}(k) = |\Pr[\mathbf{G}_{i-1}] - \Pr[\mathbf{H}_i]|$.*

Claim 2 *For any $1 \leq i \leq q(k)$, there is a non-adaptively IND-CDA adversary B such that $\mathbf{Adv}^{\text{ind-cda}}_{\mathsf{NE},B}(k) = |\Pr[\mathbf{H}_i] - \Pr[\mathbf{H}'_i]|$.*

Claim 3 *For any $1 \leq i \leq q(k)$, there is an ANON-CCA adversary B_{an2} such that $\mathbf{Adv}^{\text{anon-cca}}_{\mathsf{NE},B_{an2}}(k) = |\Pr[\mathbf{H}'_i] - \Pr[\mathbf{G}_i]|$.*

Combining these three claims, we derive that

$$\begin{aligned}&\mathbf{Adv}^{\text{ind-cda2}}_{\mathsf{NE},A}(k) = |\Pr[\mathbf{G}_{q(k)}] - \Pr[\mathbf{G}_0]| \\ &= q(k)(\mathbf{Adv}^{\text{ind-cda}}_{\mathsf{NE},B}(k) + \mathbf{Adv}^{\text{anon-cca}}_{\mathsf{NE},B_{an1}}(k) + \mathbf{Adv}^{\text{anon-cca}}_{\mathsf{NE},B_{an2}}(k)).\end{aligned}$$

Therefore, what remains is to prove the above three claims. The proof of Claim 3 is similar to that of Claim 1. So we omit it here.

Proof (of Claim 1). Note that in game $\mathbf{G}_{i-1}$ $(1 \leq i \leq q(k))$, for the j^{th} LR query of A, if $j \leq i - 1$, the challenge ciphertext vector $\mathbf{c}$ is an encryption of $\mathbf{m}_1$ under pk_0, and if $j \geq i$, $\mathbf{c}$ is an encryption of $\mathbf{m}_0$ under pk_0. Therefore, $\mathbf{H}_i$ is identical to $\mathbf{G}_{i-1}$, except that the answer A received to its i^{th} LR query is an encryption of $\mathbf{m}_0$ under pk_1, instead of

```
Adv $B_{an1}^{\mathrm{ENC}_0,\mathrm{LR}_B,\mathrm{DEC}_0}(1^k)$
$C \leftarrow \emptyset$; $j \leftarrow 0$
$St \leftarrow A_1^{\mathrm{LR}}(1^k)$
$b' \leftarrow A_2^{\mathrm{DEC}}(pk_0, St)$
Return $b'$

On query $\mathrm{LR}(\mathcal{M})$:
    $j \leftarrow j+1$
    If $j \leq i-1$, then $\mathbf{c} \leftarrow \mathrm{ENC}_0(\mathcal{M}_1)$
    If $j = i$, then $(pk_0, pk_1, \mathbf{c}) \leftarrow \mathrm{LR}_B(\mathcal{M}_0)$
    If $j > i$, then
        $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
        $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathrm{DEC}_0(c')$
    Return $m'$
```

```
Adv $B_1^{\mathrm{LR}_B}(1^k)$
$(pk_0, sk_0) \leftarrow \mathsf{NKg}(1^k)$
$C \leftarrow \emptyset$; $j \leftarrow 0$
$(St', \mathcal{M}) \leftarrow A_{1.(I)}^{\mathrm{LR}_1}(1^k)$
$\mathbf{c}^* \leftarrow \mathrm{LR}_B(\mathcal{M})$
$St_B \leftarrow (C, j, St', \mathbf{c}^*)$
Return $St_B$

Adv $B_2(pk_1, St_B)$
Parse $St_B = (C, j, St', \mathbf{c}^*)$
$St \leftarrow A_{1.(II)}^{\mathrm{LR}_2}(St', \mathbf{c})$
$b' \leftarrow A_2^{\mathrm{DEC}}(pk_0, St)$
Return $b'$

On query $\mathrm{LR}_1(\mathcal{M})$:
    $j \leftarrow j+1$
    If $j \geq i$, then return $\perp$
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_1, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{LR}_2(\mathcal{M})$:
    $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$
    $\mathbf{c} \leftarrow \mathsf{NEnc}(pk_0, \mathbf{xk}, \mathbf{m}_0, \mathbf{n})$
    $C \leftarrow C \cup \mathbf{c}$
    Return $\mathbf{c}$

On query $\mathrm{DEC}(c')$:
    If $c' \in C$, then return $\perp$
    $m' \leftarrow \mathsf{NDec}(sk_0, c')$
    Return $m'$
```

Fig. 14. Adversary B_{an1} (up) in the proof of Claim 1, and adversary B (down) in the proof of Claim 2.

the encryption of $\mathbf{m}_0$ under pk_0. For any message sampler $\mathcal{M}$ output by A, and any $b \in \{0,1\}$, we define a new message sampler $\mathcal{M}_b$ as follows: run $(\mathbf{m}_0, \mathbf{m}_1, \mathbf{xk}, \mathbf{n}) \leftarrow \mathcal{M}(1^k)$, and return $(\mathbf{m}_b, \mathbf{xk}, \mathbf{n})$. We construct a PPT legitimate ANON-CCA adversary B_{an1} in Fig. 14. Denote by LR_B the LR oracle of B_{an1}, and b the challenge bit of $\mathbf{G}_{\mathsf{NE},B_{an1}}^{\text{anon-cca}}$. When $b=1$ (resp. $b=0$), B_{an1} perfectly simulates game $\mathbf{H}_i$ (resp. game $\mathbf{G}_{i-1}$) for A. So we conclude this proof.

Proof (of Claim 2). Since $\mathbf{H}_i'$ is identical to $\mathbf{H}_i$, except that the answer A received to its i^{th} LR query is an encryption of $\mathbf{m}_1$ under pk_1, instead of the encryption of $\mathbf{m}_0$ under the same public key. We note that without loss of generality, for any IND-CDA2 adversary $A=(A_1,A_2)$ making $q(k)$ LR queries, and any $i \in [q(k)]$, the procedure of A_1 can be trivially divided into two parts $(A_{1.(I)}, A_{1.(II)})$ as follows, where $A_{1.(I)}$ makes $i-1$ queries to LR_1 oracle, and $A_{1.(II)}$ makes $q(k)-i$ queries to LR_2 oracle. LR_1, LR_2 denote the LR-oracle interfaces of $A_{1.(I)}$, $A_{1.(II)}$, respectively.

```
Adversary $A_1^{\mathrm{LR}}(1^k)$:
    $(St', \mathcal{M}) \leftarrow A_{1.(I)}^{\mathrm{LR}_1}(1^k)$;  $\mathbf{c} \leftarrow \mathrm{LR}(\mathcal{M})$;  $St \leftarrow A_{1.(II)}^{\mathrm{LR}_2}(St', \mathbf{c})$
    Return $St$
```

We construct a PPT legitimate non-adaptively IND-CDA adversary B as shown in Fig. 14. Let b be the challenge bit of $\mathbf{G}_{\mathsf{NE},B}^{\text{ind-cda}}$. When $b=1$ (resp. $b=0$), B perfectly simulates game $\mathbf{H}_i'$ (resp. game $\mathbf{H}_i$) for A. Therefore, we conclude this proof. □