Formal Security Treatments for IBE-to-Signature Transformation: Relations among Security Notions*

Yang Cui[1], Eiichiro Fujisaki[2], Goichiro Hanaoka[1], Hideki Imai[1,3] and Rui Zhang[1]

[1] National Institute of Advanced Industrial Science and Technology (AIST), Japan.
{y-cui,hanaoka-goichiro,h-imai,r-zhang}@aist.go.jp
[2] NTT Information Sharing Platform Laboratories, Japan.
fujisaki@isl.ntt.co.jp
[3] Chuo University, Japan.

Abstract

In a seminal paper of identity based encryption (IBE), Boneh and Franklin [BF01] mentioned an interesting transform from an IBE scheme to a signature scheme, which was observed by Moni Naor. In this paper, we give formal security treatments for this transform and discover several implications and separations among security notions of IBE and transformed signature. For example, we show for such a successful transform, one-wayness of IBE is an essential condition. Additionally, we give a sufficient and necessary condition for converting a semantically secure IBE scheme into an existentially unforgeable signature scheme. Our results help establish strategies on design and automatic security proof of signature schemes from (possibly weak) IBE schemes. We also show some separation results which strongly support that one-wayness, rather than semantic security, of IBE captures an essential condition to achieve secure signature.
keywords: identity based encryption, digital signature, security notions

1 Introduction

Identity-based encryption (IBE) [Sh84, BF01] is a public key encryption scheme where a user's public key can be any bit string, such as an email address. Although IBE was originally advocated by Shamir [Sh84] to simplify public key and certificate management, it has now been shown a powerful tool in constructing various cryptographic applications: key-insulated encryption [DKXY02, BP02], forward secure encryption [An97, CHK03] and public key encryption with keyword search [BDOP04], etc. In this paper, we investigate an interesting application of IBE, whose observation was attributed to Naor, saying that "*an IBE scheme can immediately be converted into a public key signature scheme*" [BF01].

Let us briefly recall Naor's observation. In IBE, a *private key generator* (PKG) uses his master key msk to issue a decryption key d which corresponds to an arbitrary bit string "ID". Here, msk can also be seen as a signing key of the PKG, and by letting ID $= M$, d becomes the PKG's signature for M where M is a message to be signed. The signature verification can be done by checking if d functions properly as a correct IBE decryption key for identity "M" by encrypting a random plaintext and checking if the ciphertext is decrypted to the original plaintext. We hereafter call such a transformation, the *Naor Transform* (NT), and $NT(\Pi)$ denotes a signature scheme derived from an IBE scheme Π via NT (Refer Sec. 3 for a full description).

*An extended abstract of this paper appeared in ProvSec 2007 [CFH+07].

We investigate implications and separations among the notions of IBE and signature in detail. Our results provide generic security proofs for a wide range of Naor-transformed signatures. For example, we show that secure signatures can be generally derived from considerably weak IBE schemes.

1.1 IBE and Naor-Transformed Signatures

IBE. Boneh and Franklin [BF01] defined the security model and proposed the first full-fledged IBE, using bilinear maps and assuming random oracles. Independently, Cocks [Co01] also presented an IBE scheme based on the decisional quadratic residue assumption. Horwitz and Lynn [HL02] and Gentry and Silverberg [GS02] generalized the model of IBE with a hierarchical structure, and proposed hierarchical IBE (HIBE) schemes. Canetti, Halevi, and Katz [CHK04] proposed an IBE whose security can be proven without random oracles but in a weaker security notion, called the selective-ID (sID) model, where an adversary has to declare its target before the setup phase. Boneh and Boyen [BB04a] proposed two more practical IBE schemes in the sID model and they further presented the first fully secure (adaptively chosen ID secure) IBE system without random oracles [BB04b]. Waters [Wat05] subsequently simplified the scheme from [BB04b], substantially improving its efficiency. Recently, Gentry [Ge06] presented a more efficient fully secure IBE scheme with tight security reduction, relying on a stronger assumption. All schemes in [BB04a, BB04b, Wat05] used a technique proposed by Canetti, Halevi and Katz [CHK04] to have chosen ciphertext security [NY90, RS91].

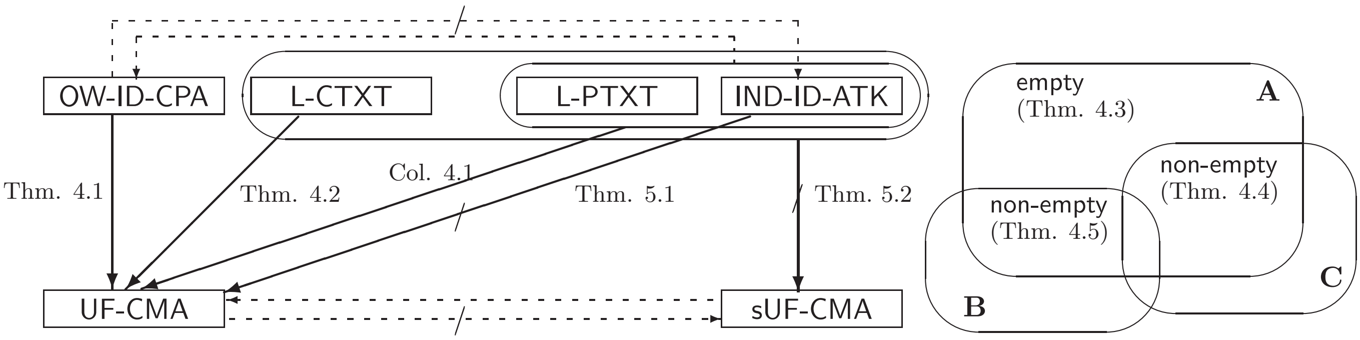
Naor-Transformed Signatures. Boneh, Lynn, and Shacham applied NT to the Boneh-Franklin IBE [BF01], resulting in a short signature [BLS01]. Gentry and Silverberg proposed a hierarchical identity-based signature (HIBS) scheme from their HIBE scheme via NT [GS02]. Furthermore, Waters [Wat05] presented the first (efficient) signature scheme whose security can be reduced to hardness of the computational Diffie-Hellman (CDH) problem. A subsequent paper [BSW06] strengthened the Waters signature to have strong existential unforgeability.

Boneh and Franklin [BF01], and Waters [Wat05] remarked (in an informal way) the security of Naor-transformed signatures: "*If IBE is semantically secure against adaptive chosen identity and adaptive chosen ciphertext attacks (*IND-ID-CCA*) [BF01], then the signature scheme is existentially unforgeable against adaptive chosen message attacks (*UF-CMA*) [GMR88]*". Posed a deeper consideration, the statement is *true*, yet with some subtle aspects that we later clarify. More importantly, since we are interested in "generic" applications of NT, we further wonder whether this statement admits of a broader interpretation. Namely, we would like to ask, for example, the following question: *What are sufficient and/or necessary conditions for underlying IBE to achieve* UF-CMA *signature*? Previous rich body of research on IBE seems not to have ready answers for such kind of "general questions". In particular, it should be noted that the security of signatures from [BLS01, GS02, Wat05, BSW06] was analyzed individually and was very specific to their schemes.

1.2 Our Contributions

The main theoretical results are relations among security notions for IBE and signature, which are depicted in Figure 1. Our results help understand both primitive better, especially on the nature of a signature scheme with a randomized verification algorithm, which was rarely studied before. Throughout this paper, we limit our scope within only basic NT with a *single* encrypt-then-decrypt verification for some reasons (See Sec. 3). As an important remark, some of our separation results may not hold if one considers other verification procedures. Especially, IND-ID-CPA implies UF-CMA if iterative encrypt-then-decrypt verification is introduced.

Let "$X \rightarrow_{NT} Y$" denote "a signature scheme $NT(\Pi)$ always satisfies condition Y if an IBE scheme Π satisfies condition X", "$X \not\rightarrow_{NT} Y$" denote "there exists Π such that $NT(\Pi)$ may not satisfy Y even if Π



Solid arrows denote implication and separation with respect to the NT with a single varication, where the symbol "$_{NT}$" is omitted in the above figure for simplicity, and ATK $\in$ {CPA, CCA}. Dotted arrows denote trivial implications or separations. **A**, **B**, and **C** denote $\{\Pi|\Pi$ is IND-ID-CPA $\wedge$ $NT(\Pi)$ is UF-CMA$\}$, $\{\Pi|\Pi$ is L-PTXT$\}$, and $\{\Pi|\Pi$ is L-CTXT$\}$, respectively.

Figure 1: Relations among Security notions for IBE and Signature.

satisfies X", and OW-ID-CPA (resp. IND-ID-CPA) [BF01] denotes one-wayness (resp. semantic security) against adaptive chosen identity and adaptive chosen plaintext attacks.

Implications. We show implications among notions for IBE and signature. We notice that most of the time, even very weak IBE implies strong digital signature. These supports the belief that IBE is a significantly stronger cryptographic primitive than signature.

1. OW-ID-CPA $\rightarrow_{NT}$ UF-CMA (Theorem 4.1). This is, existentially unforgeable secure signatures [GMR88] can be derived from considerably weak IBE schemes. An immediate corollary states that IND-ID-CPA $\wedge$ L-PTXT $\rightarrow_{NT}$ UF-CMA (Corollary 4.1), where we say Π satisfies largeness of plaintext space (L-PTXT, Definition 2.3) if $1/|\mathcal{M}|$ is negligible ($\mathcal{M}$ and $|\mathcal{M}|$ are the message space of Π and the cardinality of $\mathcal{M}$, respectively).

2. L-CTXT $\rightarrow_{NT}$ UF-CMA (Theorem 4.2). Roughly speaking, we say Π satisfies condition, largeness of ciphertext space (L-CTXT, Definition 2.4) if it is even hard to generate a "fake key" (without using PKG's master key) which maps a randomly chosen valid ciphertext onto $\mathcal{M}$. See Definition 2.4 for details. It is not difficult to determine whether an IBE scheme satisfies L-CTXT or not.

3. If Π is GOAL-ID-ATK and $NT(\Pi)$ is UF-CMA, then Π satisfies L-PTXT $\vee$ L-CTXT (Theorem 4.3), where GOAL $\in$ {OW, IND} and ATK $\in$ {CPA, CCA}. This implies L-PTXT $\vee$ L-CTXT is necessary and sufficient condition to achieve UF-CMA from IND-ID-CPA. It should be also noted that Π is not required to have a large message space if it satisfies L-CTXT. We give an example for such an IBE scheme, namely,

4. There exists Π such that Π and $NT(\Pi)$ satisfy IND-ID-CPA $\wedge$ $\neg$L-PTXT and UF-CMA, respectively (Theorem 4.4). On the other hand, there exists Π such that Π and $NT(\Pi)$ satisfy IND-ID-CPA $\wedge$ $\neg$L-CTXT and UF-CMA, respectively (Theorem 4.5).

Separations. We also show separations among security notions, which as usual, are demonstrated by counterexamples. However, these counterexamples are quite natural and non-trivial, which we believe form good guidance in building practical signature schemes from IBE.

5. IND-ID-CCA $\not\rightarrow_{NT}$ UF-CMA (Theorem 5.1). This implies that $NT(\Pi)$ is not always secure even if Π satisfies the strongest security (i.e. IND-ID-CCA) for IBE. Actually, the separation is demonstrated by constructing various IND-ID-CCA secure IBE schemes that satisfy $\neg$L-PTXT $\wedge$ $\neg$L-CTXT. We show examples via various examples: a variant of Boneh-Franklin IBE [BF01], secure with random oracles, and a variant of Waters IBE [Wat05], secure without random oracles. It should be noticed that it is easy to achieve $\mathsf{L\text{-}PTXT}$ from $\mathsf{IND\text{-}ID\text{-}CCA}$ IBE by a simple modification: just enlarge the input plaintext domain by encrypting in parallel. However, this modification is considered as a method to acquire one-wayness from semantic security, and this fact supports our first result "$\mathsf{OW\text{-}ID\text{-}CPA} \rightarrow_{NT} \mathsf{UF\text{-}CMA}$", which establishes an essential relation between IBE and signatures.

6. $\mathsf{IND\text{-}ID\text{-}CCA} \wedge \mathsf{L\text{-}PTXT} \wedge \mathsf{L\text{-}CTXT} \not\rightarrow_{NT} \mathsf{sUF\text{-}CMA}$ (Theorem 5.2). Interestingly, this shows even the most secure IBE does not imply $\mathsf{sUF\text{-}CMA}$ secure Naor-transformed signature. This immediately implies that $\mathsf{OW\text{-}ID\text{-}CPA} \not\rightarrow_{NT} \mathsf{sUF\text{-}CMA}$. Here, roughly speaking, $\mathsf{sUF\text{-}CMA}$ [ADR02] means inability of adversaries to forge any signature even for any message signed before.

Applications. The first application is, needless to say, to provide security proof for signature schemes derived from IBE via NT. For example, by straightforwardly applying our results, we can automatically prove security of Waters signature under the computational bilinear Diffie-Hellman (CBDH) assumption (weaker than that claimed in [Wat05] via known automatic proof technique). However, we note that our automatic security proof affords the price of a possibly stronger assumption than that in the specific proof in [Wat05], i.e. the CDH assumption. Also, in the future, if a new IBE scheme is designed, a signature scheme corresponding to this IBE scheme will automatically be constructed with its security proof.

As another important application, we can relax requirements for a secure channel between a user and PKG. In an IBE system, each user's decryption key has to be securely transferred from PKG, and therefore, a secure channel is needed. However, a user's decryption key can be also considered as PKG's signature based on NT, and consequently, only a channel with confidentiality is required when PKG sends a decryption key to each user. Authentication from the PKG's side is not needed for this channel.

2 Definitions

Throughout this paper, we use the following notations. Define $x \stackrel{R}{\leftarrow} X$ as x being generated randomly and uniformly from a finite set X. If A is an algorithm, $x \leftarrow A$ means that the output of A is x. When y is not a finite set nor an algorithm, $x \leftarrow y$ is an assignment operation. $|\cdot|$ is defined as the bit length if "$\cdot$" is an element of a finite set (respectively, the cardinality of the set if "$\cdot$" is a finite set). Let "$||$" denote string concatenation. When we say that $\epsilon(k)$ is negligible, it means that for any constant c there exists $k_0 \in \mathbb{N}$, such that $\epsilon < (1/k)^c$ for any $k > k_0$.

First we review the definitions and desired security notions of both identity-based encryption and digital signature. We also define some other related security notions with respect to sizes of a plaintext and a ciphertext. Finally we review bilinear map and related assumptions.

2.1 Identity-Based Encryption

IBE. An identity-based encryption (IBE) scheme Π consists of four probabilistic polynomial time (PPT) algorithms: $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$. The setup algorithm Setup takes as inputs 1^k, and generates public system parameter PK and master key msk, where k is a security parameter. The key extraction algorithm Ext takes as inputs msk, $\mathsf{ID} \in \{0,1\}^*$ and PK, and returns the corresponding decryption key $\mathsf{SK_{ID}}$. The encryption algorithm Enc takes as inputs ID, $M \in \mathcal{M}$, PK, and outputs ciphertext $C \in \mathcal{C}$, where $\mathcal{M}$ and $\mathcal{C}$ are the plaintext and ciphertext spaces, respectively. The decryption algorithm Dec takes as inputs $\mathsf{SK_{ID}}$, C and PK, and outputs M or $\perp$, where $\perp$ is a distinguished symbol. We require that for all $(\mathsf{msk}, \mathsf{PK})(= \mathsf{Setup}(1^k))$, all ID, all $\mathsf{SK_{ID}}(= \mathsf{Ext}(\mathsf{msk}, \mathsf{ID}, \mathsf{PK}))$, all M, and $C(= \mathsf{Enc}(\mathsf{ID}, M, \mathsf{PK}))$, $\mathsf{Dec}(\mathsf{SK_{ID}}, C, \mathsf{PK}) = M$.

One-wayness. Here, we define one-wayness for IBE, i.e. OW-ID-CPA [BF01]. Let $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ and k be an adversary and the security parameter, respectively. s is some state information that $\mathcal{A}_1$ outputs, such as message domain and ID, etc. It will be further passed to $\mathcal{A}_2$. We next use it in the same way if without explanation. Now consider the following experiment:

$$\textbf{Experiment } \mathsf{Exp}^{\mathsf{ow\text{-}id\text{-}cpa}}_{\mathcal{A},\Pi}(k) : [(\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\mathsf{ID}^*, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_e}(\mathsf{PK}); M \xleftarrow{R} \mathcal{M};$$
$$C^* \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M, \mathsf{PK}); M' \leftarrow \mathcal{A}_2^{\mathcal{O}_e}(s, C^*); \text{return 1 if } M' = M, \text{ or 0 otherwise}],$$

where $\mathcal{O}_e$ is a key extraction oracle which for a given identity ID, returns $\mathsf{SK}_{\mathsf{ID}}(= \mathsf{Ext}(\mathsf{msk}, \mathsf{ID}, \mathsf{PK}))$. The only restriction is that ID^* is not allowed to submit to $\mathcal{O}_e$. We define $\epsilon_{owe,\mathcal{A}} = \Pr[\mathsf{Exp}^{\mathsf{ow\text{-}id\text{-}cpa}}_{\mathcal{A},\Pi}(k) = 1]$.

Definition 2.1 (OW-ID-CPA) *We say Π is (t, q_e, ϵ)-OW-ID-CPA secure if for any adversary $\mathcal{A}$ in time bound t with at most q_e queries to $\mathcal{O}_e$, $\epsilon_{owe,\mathcal{A}} \leq \epsilon$. As shorthand, we say that Π is OW-ID-CPA secure if ϵ is negligible.*

Indistinguishability. Semantic security [GM84] for IBE, i.e. IND-ID-ATK [BF01] where $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA}\}$, is defined as follows. Let $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ and k be an adversary and the security parameter, respectively. For $\mathsf{atk} \in \{\mathsf{cpa}, \mathsf{cca}\}$, consider the following experiment:

$$\textbf{Experiment } \mathsf{Exp}^{\mathsf{ind\text{-}id\text{-}atk}}_{\mathcal{A},\Pi}(k) : [(\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\mathsf{ID}^*, M_0, M_1, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_e,\mathcal{O}_d}(\mathsf{PK}); b \xleftarrow{R} \{0,1\};$$
$$C^* \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M_b, \mathsf{PK}); b' \leftarrow \mathcal{A}_2^{\mathcal{O}_e,\mathcal{O}_d}(s, C^*); \text{return 1 if } b' = b, \text{ or 0 otherwise}],$$

where $\mathcal{O}_e$ and its restriction are the same as the above, $\mathcal{O}_d$ is a decryption oracle which for given (ID, C), returns $M(\text{or } \perp)(= \mathsf{Dec}(\mathsf{SK}_{\mathsf{ID}}, C, \mathsf{PK}))$ if $\mathsf{atk} = \mathsf{cca}$, or a random bit string if $\mathsf{atk} = \mathsf{cpa}$. The only restriction is that (ID^*, C^*) is not allowed to submit to $\mathcal{O}_d$. We define $\epsilon_{ind\text{-}atk,\mathcal{A}} = |\Pr[\mathsf{Exp}^{\mathsf{ind\text{-}id\text{-}atk}}_{\mathcal{A},\Pi}(k) = 1] - 1/2|$.

Definition 2.2 (IND-ID-ATK) *We say Π is (t, q_e, q_d, ϵ)-IND-ID-CCA (resp. (t, q_e, ϵ)-IND-ID-CPA) secure, if for any $\mathcal{A}$ in time bound t with at most q_e queries to $\mathcal{O}_e$ and q_d queries to $\mathcal{O}_d$, $\epsilon_{ind\text{-}cca,\mathcal{A}} \leq \epsilon$ (resp. $\epsilon_{ind\text{-}cpa,\mathcal{A}} \leq \epsilon$). As shorthand, we say that Π is IND-ID-CCA (resp. IND-ID-CPA) secure if ϵ is negligible.*

The above security definitions have mainly considered adaptive chosen ID (ID) attack, however one can easily adjust the definitions to selective ID (sID) attack [CHK04]. The only difference between the two attack model is that for sID attack, the target identity ID^* must be selected by $\mathcal{A}$ before the key generation algorithm Setup is run.

Largeness of Plaintext and Ciphertext Spaces. Interestingly, security of Naor-transformed signatures is significantly influenced by sizes of the plaintext and the ciphertext spaces of the underlying IBE. Here, we define largeness of the plaintext space as follows.

Definition 2.3 (L-PTXT) *We say an IBE scheme Π is γ-L-PTXT if $1/|\mathcal{M}| \leq \gamma$. As shorthand, we say that Π is L-PTXT if γ is negligible.*

It is obvious that if an IBE scheme is IND-ID-CPA secure and L-PTXT, then it always satisfies OW-ID-CPA.[1]

[1] One might think that IND-ID-CPA immediately implies OW-ID-CPA without any condition. However, this is not true since if, for example, an IBE scheme Π is IND-ID-CPA and its plaintext length is only one-bit long, then by picking a random plaintext (which is a bit) we can easily break one-wayness of Π with probability at least 1/2.

Next, we define largeness of the ciphertext space. Here, it should be noticed that by adding harmless random bits, ciphertext-length can be generally (and meaninglessly) extended for any IBE schemes. In our definition, therefore, we introduce a new notion for a ciphertext which captures an essential requirement to achieve UF-CMA security. Sufficiently large ciphertext-length is a necessary condition for satisfying this notion, and consequently, an IBE scheme may not fulfill this notion if its ciphertext-length is not large enough. Let $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Without loss of generality, the information of domain and range is implicitly embedded in the algorithms. Let $\mathcal{A}$ and k be an adversary and the security parameter, respectively. Now, consider the following experiment:

$$\textbf{Experiment } \mathsf{Exp}^{\mathsf{l\text{-}ctxt}}_{\mathcal{A},\Pi}(k) : [(\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*}) \leftarrow \mathcal{A}^{\mathcal{O}_e}(\mathsf{PK}); M \xleftarrow{R} \mathcal{M};$$
$$C^* \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}^*}, C^*, \mathsf{PK}); \text{return } 1 \text{ if } M' \in \mathcal{M}, \text{ or } 0 \text{ otherwise}],$$

where $\mathcal{O}_e$ and its restriction are the same as the above. We define $\epsilon_{\ell\text{-}ctxt,\mathcal{A}} = \Pr[\mathsf{Exp}^{\mathsf{l\text{-}ctxt}}_{\mathcal{A},\Pi}(k) = 1]$.

Definition 2.4 (L-CTXT) *We say Π is (t, q_e, ϵ)-L-CTXT if for any $\mathcal{A}$ in time bound t with at most q_e queries to $\mathcal{O}_e$, $\epsilon_{\ell\text{-}ctxt,\mathcal{A}} \leq \epsilon$. As shorthand, we say that Π is L-CTXT if ϵ is negligible.*

We note that the mapped plaintext $M'(= \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}^*}, C^*, \mathsf{PK}))$ is not necessary to be the original M, and therefore it is not difficult to find a "fake" key $\mathsf{SK}'_{\mathsf{ID}^*}$ which maps C^* onto some element of $\mathcal{M}$ unless $|\mathcal{C}|$ is significantly larger than $|\mathcal{M}|$.

Here, we additionally explain how largeness of ciphertexts is captured by L-CTXT. It should be noticed that since for any encryption scheme we can extend its ciphertext length by meaninglessly adding harmless bits, naive evaluation based on ciphertext length cannot properly express essential largeness of ciphertexts. Therefore, we focus on implicit redundancy of ciphertexts instead, where implicit redundancy means redundancy that is essentially used for decryption. If a ciphertext has a sufficiently large amount of such redundancy, then we can expect that for any ciphertext its decryption result becomes "$\perp$" unless the correct decryption key is used. In fact, a necessary condition of L-CTXT is that a ciphertext is significantly longer than a plaintext. We have to also honestly mention that L-CTXT seems stronger than more intuitive notions for largeness of ciphertext.

2.2 Digital Signature

Signature. A signature scheme Σ consists of three PPT algorithms: $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. The key generation algorithm Gen takes as inputs 1^k, and generates signing key SigK and verification key VK. The signing algorithm Sig takes as inputs SigK, $m \in \{0,1\}^*$, and VK, and outputs (σ, m), where m is a message to be signed. The verification algorithm Ver takes as inputs VK, σ', and m', and outputs `accept` or `reject`. We require that for all $(\mathsf{SigK}, \mathsf{VK})(= \mathsf{Gen}(1^k))$, all m, all $(\sigma, m)(= \mathsf{Sig}(\mathsf{SigK}, m, \mathsf{VK}))$, we have $\mathsf{Ver}(\mathsf{VK}, \sigma, m) = \texttt{accept}$.

Unforgeability. Here, we define unforgeability for signatures, i.e. UF-CMA [GMR88], and a stronger notion, i.e. sUF-CMA [ADR02]. Let $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme. Let $\mathcal{A}$ and k be an adversary and the security parameter, respectively. For $\mathsf{goal} \in \{\mathsf{uf}, \mathsf{suf}\}$, consider the following experiment:

$$\textbf{Experiment } \mathsf{Exp}^{\mathsf{goal\text{-}cma}}_{\mathcal{A},\Sigma}(k) : [(\mathsf{SigK}, \mathsf{VK}) \leftarrow \mathsf{Gen}(1^k); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathcal{O}_s}(\mathsf{PK}); \text{return } \mathsf{Ver}(\mathsf{VK}, \sigma^*, m^*)],$$

where $\mathcal{O}_s$ is a signing oracle which for a given message m, returns (σ, m). The only restriction is that m^* is not allowed to submit to $\mathcal{O}_s$ if $\mathsf{goal} = \mathsf{uf}$, or that (σ^*, m^*) is not allowed to be one of responses from $\mathcal{O}_s$ if $\mathsf{goal} = \mathsf{suf}$. We define $\epsilon_{goal\text{-}cma,\mathcal{A}} = \Pr[\mathsf{Exp}^{\mathsf{goal\text{-}cma}}_{\mathcal{A},\Sigma}(k) = \texttt{accept}]$ for $\mathsf{goal} \in \{\mathsf{uf}, \mathsf{suf}\}$.

Definition 2.5 ((s)UF-CMA) *We say Σ is (t, q_s, ϵ)-UF-CMA (resp. sUF-CMA) if for any $\mathcal{A}$ in time bound t with at most q_s queries to $\mathcal{O}_s$, $\epsilon_{uf\text{-}cma,\mathcal{A}} \leq \epsilon$ (resp. $\epsilon_{suf\text{-}cma,\mathcal{A}} \leq \epsilon$). As shorthand, we say that Σ is UF-CMA (resp. sUF-CMA) secure if ϵ is negligible.*

Algorithm $\mathsf{Gen}(1^k)$	**Algorithm** $\mathsf{Sig}(\mathsf{SigK}, m, \mathsf{VK})$	**Algorithm** $\mathsf{Ver}(\mathsf{VK}, \sigma, m)$
$(\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k)$;	$\mathsf{ID} \leftarrow m$;	$\mathsf{ID} \leftarrow m$; $\mathsf{SK}'_{\mathsf{ID}} \leftarrow \sigma$; $M \stackrel{R}{\leftarrow} \mathcal{M}$;
$\mathsf{SigK} \leftarrow \mathsf{msk}$;	$\mathsf{SK}_{\mathsf{ID}} \leftarrow \mathsf{Ext}(\mathsf{SigK}, \mathsf{ID}, \mathsf{VK})$;	$C \leftarrow \mathsf{Enc}(\mathsf{ID}, M, \mathsf{VK})$;
$\mathsf{VK} \leftarrow \mathsf{PK}$;	$\sigma \leftarrow \mathsf{SK}_{\mathsf{ID}}$;	$M' \leftarrow \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}}, C, \mathsf{VK})$;
return $(\mathsf{SigK}, \mathsf{VK})$	return (σ, m)	if $M' = M$, return `accept`;
		else return `reject`

Table 1: Algorithms of $NT(\Pi)$.

2.3 Bilinear Groups and Related Assumptions

Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic groups of prime order p and g be a generator of $\mathbb{G}_1$. A bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ satisfies the following properties. For all $(a, b) \in \mathbb{Z}^2$, $e(g^a, g^b) = e(g, g)^{ab}$, and $e(g, g) \neq 1$. We briefly review the computational bilinear Diffie-Hellman (CBDH) [BF01], the decisional bilinear Diffie-Hellman (DBDH) [CHK03], and the gap bilinear Diffie-Hellman (GBDH) [OP01] assumptions.

Definition 2.6 (BDH assumptions) *Let g be a generator of $\mathbb{G}_1$ and $a, b, c, z \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$. The (t, ϵ)-*CBDH *assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if for given (g, g^a, g^b, g^c), no t-time algorithm finds $e(g, g)^{abc}$ with probability at least ϵ. The (t, ϵ)-*DBDH *assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has with at least ϵ advantage, where for an algorithm $\mathcal{A}$, $\mathcal{A}$'s advantage $\epsilon_{\mathcal{A}}$ is defined as $\epsilon_{\mathcal{A}} = \frac{1}{2}|\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^z) = 1]|$. The (t, q, ϵ)-*GBDH *assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if for given (g, g^a, g^b, g^c) and $\mathcal{O}$, no t-time algorithm finds $e(g, g)^{abc}$ with probability at least ϵ, where $\mathcal{O}$ is a decision oracle which for a given $(g, g^\alpha, g^\beta, g^\gamma, T) \in \mathbb{G}_1^4 \times \mathbb{G}_2$, returns 1 if $T = e(g, g)^{\alpha\beta\gamma}$ or 0 otherwise, assuming that an algorithm is allowed to submit at most q queries to $\mathcal{O}$.*

3 Naor-Transform and Its Variants

In this section, we give a detailed description of NT, which is based on the explanation by Boneh and Franklin [BF01] and Waters [Wat05]. We also discuss some variants of NT.

3.1 A Generic Conversion from IBE to Signature

Let $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Then, a Naor-transformed signature scheme $NT(\Pi) = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ consists of three algorithms, which are depicted in Table 1.

NT can be also extended to other types of IBE schemes. For example, applying NT to an $(\ell + 1)$-level HIBE scheme [HL02, GS02], one gains an ℓ-level HIBS scheme. Applying NT to an sID secure IBE scheme [CHK04, BB04a], a signature scheme with "selective unforgeability" is then acquired, where selective unforgeability [Sti05] is a weakened notion of UF-CMA, and in this notion an adversary has to commit the target message m^* for the forged signature before the setup phase. In the context of the NT the target identity ID^* in the IBE scheme Π corresponds to the target message m^* in the signature scheme $NT(\Pi)$, and therefore, sID security of Π implies selective unforgeability of $NT(\Pi)$.

3.2 Some Variants

In this paper, we regard the above transformation as Naor Transform (NT), since it is the most natural and basic formalization of the intuitive explanation of [BF01] and [Wat05]. However, besides the above basic construction of NT, there are some more variants with respect to signature verification mechanisms.

Iterative Verification. In the above basic NT, the verification algorithm is randomized, and there is possibility of verification error. To enhance security, it is possible to reduce error probability by running the verification algorithm for multiple times. This method is equivalent to the standard message expansion technique for encryption schemes with small message space. Namely, instead of iterative verification, we can also extend the message space of the underlying IBE scheme by individually encrypting each block of a message, and transform it to signature via the basic NT (with a single verification). Therefore, in the rest of this paper we consider only NT with a single verification, and this makes essential conditions for achieving UF-CMA clearer.

Non-Interactive Proof of Correctness of Decryption Key. Let $L = \{(m, \sigma, \mathsf{VK}) | \exists (R, \mathsf{SigK})$ s.t. $\sigma = \mathsf{Ext}(\mathsf{SigK}, m, \mathsf{VK}; R)\}$, where R denotes internal coin-flipping of Ext. Since L is an NP-language, it is also possible to prove validity of σ by adding *non-interactive zero-knowledge* (NIZK) proof [BFM88] for $(m, \sigma, \mathsf{VK}) \in L$. However, NIZK proof is generally expensive and/or requires additional assumptions, e.g. common reference string, random oracle, etc., and therefore, we do not consider this approach.

Specific Verification Function. Suppose that there exists an efficiently computable function f such that $f(\mathsf{SK}'_{\mathsf{ID}}, \mathsf{ID}, \mathsf{PK}) = 1$ if and only if $\mathsf{SK}'_{\mathsf{ID}}$ is a decryption key for identity "ID". Then, verification process becomes much simpler, and some IBE schemes, e.g. Boneh-Franklin [BF01] and Cocks [Co01], have such specific verification functions. In [BF01], one can test correctness of $\mathsf{SK}'_{\mathsf{ID}}$ by only one pairing computation, and its corresponding signature, i.e. Boneh-Lynn-Shacham signature [BLS01], is constructed by using this method. In [Co01], a decryption key for ID is square root of (hashed) ID or $-\mathsf{ID}$, and hence, this is also easily checkable. By using this relation, (a variant of) Rabin signature can be obtained from [Co01].

4 Implication Results

Denote the IBE scheme Π and a corresponding signature $NT(\Pi)$ as $\Pi = (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ and $NT(\Pi) = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. We present several theorems regarding implications among security definitions regarding Π and $NT(\Pi)$.

We first show an important and essential relation, which says a weak IBE with only one-wayness is sufficient to imply a UF-CMA secure Naor-transformed signature.

Theorem 4.1 (OW-ID-CPA $\to_{NT}$ UF-CMA) *If an IBE scheme Π is $(t + O(\tau), q, \epsilon)$-*OW-ID-CPA *secure, $NT(\Pi)$ is (t, q, ϵ)-*UF-CMA *secure. Here τ is the upper bound of time for one decryption operation.*

Proof of Theorem 4.1. We prove the theorem by contradiction. Namely, assuming that there exists a UF-CMA forger $\mathcal{A}$ against $NT(\Pi)$ with running time t, q signature queries, and succeeding probability $\epsilon_{\mathcal{A}} > \epsilon$, we construct a OW-ID-CPA adversary $\mathcal{B}$ against Π with running time $t + O(\tau)$, q key extraction queries, and succeeding probability $\epsilon_{\mathcal{B}} \geq \epsilon_{\mathcal{A}}$.

For a given public system parameter PK, $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ interacts $\mathcal{A}$ as follows:

Algorithm $\mathcal{B}_1^{\mathcal{O}_e}(\mathsf{PK})$ $\mathsf{VK} \leftarrow \mathsf{PK}$; $(\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{VK})$; $\mathsf{ID}^* \leftarrow m^*$; $s \leftarrow (\mathsf{ID}^*, \sigma^*, \mathsf{PK})$; return (ID^*, s)	**Algorithm** $\mathcal{B}_2^{\mathcal{O}_e}(s, C^*)$ $(\mathsf{ID}^*, \sigma^*, \mathsf{PK}) \leftarrow s$; $\mathsf{SK}'_{\mathsf{ID}^*} \leftarrow \sigma^*$; $M' \leftarrow \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}^*}, C^*, \mathsf{PK})$; return M'

When $\mathcal{A}$ asks a signing query on a message m_i for $1 \leq i \leq q$, $\mathcal{B}_1$ queries its own key extraction oracle $\mathcal{O}_e$ on "identity" m_i to get the corresponding decryption key, and delivers it to $\mathcal{A}$ as the signature σ_i for m_i. Note that σ_i is always valid signature on m_i. $\mathcal{S}$ denotes the simulated signing oracle by $\mathcal{B}$. Finally, $\mathcal{A}$ outputs a pair (σ^*, m^*), where m^* has not been asked as one of signature queries. $\mathcal{B}_1$ then sets m^* as its target identity ID^*, and relays σ^* to $\mathcal{B}_2$. $\mathcal{B}_2$ decrypts C^* by using it. One point to note here is that σ^* is not necessary to be a correct decryption key for ID^*. Now, we estimate $\mathcal{B}$'s succeeding probability $\epsilon_{\mathcal{B}}$, that is,

$$\begin{aligned}\epsilon_{\mathcal{B}} &= \Pr[M' = M | (\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\mathsf{ID}^*, s) \leftarrow \mathcal{B}_1^{\mathcal{O}_e}(\mathsf{PK}); \\ &\quad M \xleftarrow{R} \mathcal{M}; C^* \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M, \mathsf{PK}); M' \leftarrow \mathcal{B}_2^{\mathcal{O}_e}(s, C^*)] \\ &= \Pr[M' = M | (\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{PK}); \\ &\quad M \xleftarrow{R} \mathcal{M}; C^* \leftarrow \mathsf{Enc}(m^*, M, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\sigma^*, C^*, \mathsf{PK})]. \qquad (1)\end{aligned}$$

On the other hand, since the simulation of signing oracle is perfect, we have that

$$\epsilon_{\mathcal{A}} = \Pr[\mathsf{Ver}(\mathsf{VK}, \sigma^*, m^*) = \mathtt{accept} | (\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{PK})].$$

Now, recall that $\mathsf{Ver}(\mathsf{VK}, \sigma^*, m^*) = \mathtt{accept}$ if and only if $(M' = M | M \xleftarrow{R} \mathcal{M}; C \leftarrow \mathsf{Enc}(m^*, M, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\sigma^*, C, \mathsf{PK}))$. Then, we have

$$\begin{aligned}\epsilon_{\mathcal{A}} = \Pr[M' = M | (\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{PK}); \\ M \xleftarrow{R} \mathcal{M}; C \leftarrow \mathsf{Enc}(m^*, M, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\sigma^*, C, \mathsf{PK})]. \qquad (2)\end{aligned}$$

Since right-hand sides of Eqs. (1) and (2) are completely identical, we immediately have that $\epsilon_{\mathcal{B}} = \epsilon_{\mathcal{A}}$. The running time of $\mathcal{B}$ is $t + O(\tau)$, and $\mathcal{B}$ asks exactly q key extraction queries, which are easily verified from the description of $\mathcal{B}$. □

One-wayness Is Essential. It should be noticed that Eq. (1) is strikingly identical to Eq. (2) by accident, and this similarity functions significantly in the above proof. This implies that one-wayness captures an essential condition to derive a secure Naor-transformed signature. Note that the above strategy cannot help an IND-ID-CPA adversary $\mathcal{B}'$. In the IND-ID-CPA setting, for a given ciphertext C^* $\mathcal{B}'$ has to correctly guess M_b which is the corresponding plaintext of C^*. By introducing the above strategy, $\mathcal{B}'$ can recover M_b from C^* by using $\mathcal{A}$'s output. Therefore, one may (carelessly) conclude that IND-ID-CPA $\rightarrow_{NT}$ UF-CMA as well. However, this is not true. Namely, even if M_b is correctly recovered with non-negligible probability, this does not imply that M_{1-b} is incorrectly and accidentally recovered with only negligible probability. Hence, the above reasoning for IND-ID-CPA $\rightarrow_{NT}$ UF-CMA is invalidated.

Certainly, if the plaintext space is large, i.e., $1/|\mathcal{M}|$ is negligible, indistinguishability always implies one-wayness, which leads to an immediate corollary. Note that the condition that $1/|\mathcal{M}|$ is negligible is exactly what we defined as L-PTXT.

Corollary 4.1 (IND-ID-CPA $\wedge$ L-PTXT $\rightarrow_{NT}$ UF-CMA) *If an IBE scheme* Π *is* $(t+O(\tau), q, \frac{\epsilon-\gamma}{2-2\gamma})$-IND-ID-CPA *secure and* γ-L-PTXT, *then* $NT(\Pi)$ *is* (t, q, ϵ)-UF-CMA *secure. Here,* τ *is the upper bound of time for one decryption operation.*

Up to now, the curious reader may wonder in order to build a secure signature $NT(\Pi)$ from semantically secure IBE Π that is not L-PTXT, whether one has to first enlarge the plaintext space, e.g., by adopting interactive verifications. However, this is sometimes unnecessary. We show if Π meets L-CTXT, $NT(\Pi)$ is always UF-CMA secure, namely,

Theorem 4.2 (L-CTXT $\rightarrow_{NT}$ UF-CMA) *If an IBE scheme* Π *is* (t, q, ϵ)-L-CTXT, *then* $NT(\Pi)$ *is* (t, q, ϵ)-UF-CMA *secure.*

The proof to Theorem 4.2 is given in Appendix B. We then show the following theorem, which implies L-CTXT is a "properly correct" condition for IBE schemes to derive secure signatures. More precisely, L-CTXT $\vee$ L-PTXT is a necessary and sufficient condition for extracting UF-CMA secure signature from IND-ID-CPA secure IBE.

Theorem 4.3 *If an IBE scheme Π is* GOAL-ID-ATK *secure (*GOAL$\in${OW,IND}, ATK$\in${CPA,CCA}*) and $NT(\Pi)$ is* UF-CMA *secure, then Π always satisfies* L-PTXT *or* L-CTXT.

Theorem 4.3 in fact overlaps some of the previous results, namely Theorem 4.1 and Corollary 4.1. However, we adopt this complicated statement because we believe it explains precisely our entire understanding on relations among security definitions of IBE and corresponding signature schemes. We want to demonstrate the following: Assuming Π is IND-ID-CPA secure but not OW-ID-CPA secure, to make $NT(\Pi)$ UF-CMA secure, Π should meet L-CTXT. Then combining the above claims with this new claim, we immediately get the statement of Theorem 4.3. The details are given below.

Proof of Theorem 4.3. From Theorem 4.1, it is easy to see that Π being OW-ID-ATK secure implies both $NT(\Pi)$ is UF-CMA secure and Π meets L-PTXT. Then it suffices to prove that when $NT(\Pi)$ is UF-CMA and Π is IND-ID-ATK secure, Π should also meet L-PTXT or L-CTXT. On the other hand, from Corollary 4.1, if Π is IND-ID-ATK secure and Π meets L-PTXT, $NT(\Pi)$ is UF-CMA secure. It remains to show that if Π is IND-ID-CPA secure (CCA implies CPA) but Π is not L-PTXT, Π must meet L-CTXT. Regarding the last point, we present the following lemma:

Lemma 4.1 *Suppose $NT(\Pi)$ is (t, q, ϵ_s)-*UF-CMA *secure and Π is not γ-*L-PTXT *(i.e. $1/|\mathcal{M}| > \gamma$). If Π is $(t + O(\tau), q, \frac{\gamma\epsilon-\epsilon_s}{2-2\gamma})$-*IND-ID-CPA *secure, it is also (t, q, ϵ)-*L-CTXT*. Here, τ is the upper bound of time for one decryption operation.*

The proof to Lemma 4.1 is given in Appendix C. In Lemma 4.1, we have that $\frac{\gamma\epsilon-\epsilon_s}{2-2\gamma}$ is non-negligible if ϵ and γ are non-negligible and ϵ_s is negligible, which proves Theorem 4.3. $\square$

We have demonstrated that L-CTXT, together with L-PTXT, is necessary and sufficient to derive secure signature from semantically secure IBE via NT. The following theorem shows L-CTXT is actually a natural and sufficiently weak notion. Many weak IBE schemes in fact meet L-CTXT.

Theorem 4.4 *There exists an IBE scheme Π such that Π and $NT(\Pi)$ satisfy* IND-ID-CPA $\wedge$ $\neg$L-PTXT *and* UF-CMA*, respectively.*

The proof of the above theorem is given in Appendix D. Basically, we present an example that is a simple modification of (chosen-plaintext secure version of) Waters IBE scheme. Another example can be found in Sec. 5.1. A similar modification as the one shown in the proof of Theorem 4.4 to Boneh-Franklin IBE [BF01], Boneh-Boyen (fully secure) IBE [BB04b], or Gentry IBE [Ge06] also reaches the same conclusion as Theorem 4.4. All these modified schemes meet $\neg$L-PTXT$\wedge$L-CTXT. On the other hand, we have,

Theorem 4.5 *There exists an IBE scheme Π such that Π and $NT(\Pi)$ satisfy* IND-ID-CPA $\wedge$ $\neg$L-CTXT *and* UF-CMA*, respectively.*

Proof of Theorem 4.5. There exist a number of examples, e.g. the CPA secure scheme in [Wat05]. $\square$

5 Separation Results

In the previous section, we showed that UF-CMA signature schemes can be derived from considerably weak IBE schemes, and especially, one-wayness of IBE plays an important role to provide secure signatures. Here, we show impossibility of proving UF-CMA security of Naor-transformed signatures (with a single verification) solely based on indistinguishability of underlying IBE. Especially, we demonstrate counterexamples indicating IND-ID-CCA $\nrightarrow_{NT}$ UF-CMA, which immediately implies IND-ID-CPA $\nrightarrow_{NT}$ UF-CMA as well. This result strongly supports that indistinguishability is not an essential requirement to provide secure Naor-transformed signatures but one-wayness is. In addition, we also present separation results on the relation among security notions for IBE and sUF-CMA security of signature.

5.1 IND-ID-CCA $\nrightarrow_{NT}$ UF-CMA

Technical Hurdles. It is not difficult to show IND-ID-CPA $\nrightarrow_{NT}$ UF-CMA since there exist natural and simple counterexamples for this, e.g. Cocks IBE [Co01]. Therefore, one may think it is immediate to build a chosen ciphertext secure counterexample from chosen plaintext secure one via generic methods to acquire chosen ciphertext security, e.g. Fujisaki-Okamoto conversion [FO99b]. However, it is not true. For example, suppose IND-ID-CCA secure Boneh-Franklin IBE [BF01] with one-bit message space. In this scheme, it is hard to generate a fake decryption key which maps a valid ciphertext to either 0 or 1 since the decryption algorithm returns only "$\perp$" without using a correct key due to validity checking functionality of Fujisaki-Okamoto. Namely, this scheme satisfies L-CTXT, and can not be a counterexample.

Counterexamples. We show the separation result by demonstrating two IND-ID-CCA IBE schemes with small message space whose validity check process is carried out without using a decryption key. Starting from this idea, we propose two natural and reasonably efficient schemes by different means. One is in the standard model, and the other is in the random oracle model. This implies that generally IND-ID-CCA and UF-CMA are separated under "NT".

Theorem 5.1 (IND-ID-CCA $\nrightarrow_{NT}$ UF-CMA) *There exists an* IND-ID-CCA *secure IBE scheme* Π *such that* $NT(\Pi)$ *is not* UF-CMA *secure.*

Proof of Theorem 5.1. From Theorem 4.3, it is sufficient to construct an IND-ID-CCA secure IBE scheme which satisfies neither L-PTXT nor L-CTXT. We present two such schemes whose security are analyzed in Lemma 5.1, 5.2 and Lemma 5.3, 5.4, respectively. Combining Lemma 5.1 and 5.2 or combining Lemma 5.3 and 5.4 leads to the theorem. □

Modified Waters-Canetti-Halevi-Katz IBE. Our first counterexample is based on Waters IBE [Wat05]. More precisely, this is the same as the chosen-ciphertext secure version of Waters IBE mentioned in [Wat05], where a technique from [CHK04] is used to achieve chosen-ciphertext security, except for a slight modification. This scheme is provably secure in the standard model. In this scheme, we introduce a (one-time) signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$.

Setup On input 1^k, generate groups $\mathbb{G}_1, \mathbb{G}_2$ with prime order p, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Pick a random $\alpha \in \mathbb{Z}_p^*$ and set $g_1 = g^\alpha$. Choose an injective mapping F which maps a verification key of Σ onto $\mathbb{Z}_p^*$.[2] Choose $g_2, g_3 \in \mathbb{G}_1$ randomly, and set a hash function $G : \mathbb{Z}_p^* \to \mathbb{G}_1$ as $G(x) = g_2^x g_3$. Choose $u_i \in \mathbb{G}_1$ for $0 \le i \le n$ randomly, and set a hash function $H : \{0,1\}^n \to \mathbb{G}_1$ as $H(x) = u_0 \prod_{i=1}^n {u_i}^{x_i}$, where x_i denotes i-th bit of x. Then, output public system parameter $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, g_2, g_3, F, G, H\rangle$ and master key g_2^α.

[2] If there exists no such a mapping, we can also use a collision-resistant hash function instead.

Extraction For identity $\mathsf{ID} \in \{0,1\}^n$, generate decryption key $\mathsf{SK_{ID}} = (d_1, d_2)$ as $d_1 = g_2^{\alpha} H(\mathsf{ID})^r$ and $d_2 = g^r$, where r is randomly picked from $\mathbb{Z}_p^*$.[3]

Encryption To encrypt message $m \in \{0,1\}$ for identity ID, generate a signature key pair as $(\mathsf{SigK}, \mathsf{VK}) \leftarrow \mathsf{Gen}(1^k)$, pick a random $s \in \mathbb{Z}_p^*$, and compute $c_1 = g^s$, $c_2 = H(\mathsf{ID})^s$, $c_3 = F(\mathsf{VK})^s$ and $c_4 = e(g_1, g_2)^{s+m}$. Then, output ciphertext C, where $C = (c_1, c_2, c_3, c_4, \sigma, \mathsf{VK})$ and $\sigma \leftarrow \mathsf{Sig}(\mathsf{SigK}, (c_1, c_2, c_3, c_4), \mathsf{VK})$.

Decryption To decrypt ciphertext $C' = (c_1', c_2', c_3', c_4', \sigma', \mathsf{VK}')$ for identity ID, if $\mathsf{Ver}(\mathsf{VK}', \sigma', (c_1', c_2', c_3', c_4'))$ $=$ `reject` or $e(g, c_3') \neq e(c_1', F(\mathsf{VK}))$, output "$\perp$". Else, output 1 if $mes = e(g_1, g_2)$, 0 if $mes = 1$, or a random bit $m' \in \{0,1\}$ otherwise, where $mes = c_4' \cdot e(c_2', d_2) \cdot e(d_1, c_1')^{-1}$.

Lemma 5.1 *The above scheme is* (t, q_e, q_d, ϵ)-IND-ID-CCA *secure, if the* $(t + O(\epsilon^{-2} \ln(\epsilon - 1)\lambda^{-1} \ln(\lambda^{-1}) + q_d \tau), \frac{\epsilon - \epsilon_s}{32(n+1)q_e})$*-DBDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$*, and* Σ *is* $(t, 1, \epsilon_s)$-sUF-CMA *secure, where* $\lambda = \frac{1}{8(n+1)q_e}$ *and* τ *is the maximum time for decryption of the above scheme.*

Notice that the above scheme is the same as the original (chosen-ciphertext version of) Waters IBE scheme except for its encoding rule for plaintexts. Therefore, proof of Lemma 5.1 can be straightforwardly done by the same proof methods of [Wat05] and [CHK04].

Lemma 5.2 *Let* Π *denote the above IBE scheme. Then,* $NT(\Pi)$ *is not* UF-CMA *secure.*

The proof to Lemma 5.2 can be found in Appendix E.1.

Modified Boneh-Franklin IBE. Our second counterexample is based on Boneh-Franklin IBE [BF01]. The scheme is quite simple in form and provably secure in the random oracle model. We shall use a strongly unforgeable (one-time) signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$.

Setup. On input 1^k, generate groups $\mathbb{G}_1, \mathbb{G}_2$ with prime order p, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Choose two cryptographic hash functions $G : \{0,1\}^* \rightarrow \{0,1\}$, $H : \{0,1\}^* \rightarrow \mathbb{G}_1 \backslash \{1\}$, and a generator g of $\mathbb{G}_1$. Pick a random $s \in \mathbb{Z}_p^*$ and set $g_1 = g^s$. The public system parameter $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, G, H \rangle$ and the master key is s.

Extraction. For identity $\mathsf{ID} \in \{0,1\}^*$, generate decryption key $\mathsf{SK_{ID}}$ as $\mathsf{SK_{ID}} = H(\mathsf{ID})^s$.

Encryption. To encrypt a plaintext $M \in \{0,1\}$ for identity ID, generate a signature key pair as $(\mathsf{SigK}, \mathsf{VK}) \leftarrow \mathsf{Gen}(1^k)$, pick a random $r \in \mathbb{Z}_p^*$, and compute $c_1 = g^r$, $c_2 = m \oplus G(e(g_1, H(\mathsf{ID}))^r, \mathsf{VK}, c_1)$. Then, output ciphertext C as $C = (c_1, c_2, \sigma, \mathsf{VK})$ where $\sigma \leftarrow \mathsf{Sig}(\mathsf{SigK}, (c_1, c_2), \mathsf{VK})$.

Decryption. To decrypt a ciphertext $C' = (c_1', c_2', \sigma', \mathsf{VK}')$ for identity ID, if $\mathsf{Ver}(\mathsf{VK}', \sigma', (c_1', c_2')) =$ `accept`, output M', where $M' = c_2' \oplus G(e(c_1', \mathsf{SK_{ID}}), \mathsf{VK}', c_1')$. Else, output "$\perp$".

Lemma 5.3 *The scheme is* (t, q_e, q_d, ϵ) IND-ID-CCA *secure, if the* sUF-CMA *signature is* $(t, 1, \epsilon_s)$ *secure and* $(O(t + (q_G + q_H) \cdot \tau), q_d, \frac{\epsilon - \epsilon_s}{e q_e})$*-GBDH assumption holds, where* e *is the base of natural logarithm,* q_G, q_H *are numbers of queries to random oracles* G, H*, respectively and* τ *is the maximum time of one step of operation by* $\mathcal{B}$.

Lemma 5.4 *Let* Π *denote the above IBE scheme. Then,* $NT(\Pi)$ *is not* UF-CMA *secure.*

The proof to Lemma 5.3 and 5.4 are given in Appendix E.2 and E.3, respectively.

[3] If an identity is an arbitrary bit string, one can use a collision-resistant hash function to map it onto $\{0,1\}^n$.

5.2 $\mathsf{IND\text{-}ID\text{-}CCA} \wedge \mathsf{L\text{-}PTXT} \wedge \mathsf{L\text{-}CTXT} \nrightarrow_{NT} \mathsf{sUF\text{-}CMA}$

sUF-CMA security [ADR02] is stronger than UF-CMA, however, it is equivalent to UF-CMA, when the signing algorithm is deterministic, i.e., for a message, there is only a *unique* signature under the given public key. Thus, it is easy to see that a UF-CMA secure Naor-transformed signature scheme with a unique signature is sUF-CMA secure at the same time. However, we show that this is not true in a general sense, i.e. the most secure IBE does not always imply sUF-CMA secure signature via NT, even if this IBE meets both L-PTXT and L-CTXT.

Theorem 5.2 (IND-ID-CCA $\wedge$ L-PTXT $\wedge$ L-CTXT$\nrightarrow_{NT}$ sUF-CMA) *There exists* IND-ID-CCA *secure IBE* Π*, such that* Π *is both* L-PTXT *and* L-CTXT*, but* $NT(\Pi)$ *is not* sUF-CMA *secure.*

Proof of Theorem 5.2. Here we briefly introduce the idea behind our proof. In fact, we need an IND-ID-CCA secure IBE that has large plaintext space (L-PTXT) and is only privately verifiable (L-CTXT). Towards this goal, we present the following scheme, which can be regarded as an instantiation of the Boneh-Katz [BK05] methodology with the basic Waters IBE (combined with an sID secure IBE from [BB04a]).

Waters-Boneh-Katz IBE. Now we instantiate the Boneh-Katz methodology [BK05] with a 2-level HIBE with the first level being Waters IBE [Wat05] and the second level being sID secure IBE in [BB04a], which is similar to the fully secure Waters IBE. Let $\Phi = (\mathsf{Mac}, \mathsf{Vrfy})$ be a message authentication code and $\Psi = (\mathsf{Setup}, \mathsf{S}, \mathsf{R})$ be an encapsulation scheme, whose formal definitions are postponed to Appendix F.

Setup. On input 1^k, generate groups $\mathbb{G}_1, \mathbb{G}_2$ with prime order p, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Pick a random $\alpha \in \mathbb{Z}_p^*$ and set $g_1 = g^\alpha$. Choose an injective mapping F which maps $\{0,1\}^k$ onto $\mathbb{Z}_p^*$. Choose $g_2, g_3 \in \mathbb{G}_1$ randomly, and set a hash function $G : \mathbb{Z}_p^* \to \mathbb{G}_1$ as $G(x) = g_2^x g_3$. Choose $u_i \in \mathbb{G}_1$ for $0 \le i \le n$ randomly, and set a hash function $H : \{0,1\}^n \to \mathbb{G}_1$ as $H(x) = u_0 \prod_{i=1}^n u_i{}^{x_i}$, where x_i denotes i-th bit of x. Run $\mathsf{Setup}(1^k)$ to generate pub. Then the public system parameter $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, g_2, g_3, F, G, H, \mathsf{pub}\rangle$ and master key g_2^α.

Extraction. For identity $\mathsf{ID} \in \{0,1\}^n$, generate decryption key $\mathsf{SK_{ID}} = (d_1, d_2)$ as $d_1 = g_2^\alpha H(\mathsf{ID})^r$ and $d_2 = g^r$, where r is randomly picked from $\mathbb{Z}_p^*$.

Encryption. To encrypt a message M for identity ID, first encapsulate a random value by running $\mathsf{S}(1^k, \mathsf{pub})$ to obtain $(r, \mathsf{com}, \mathsf{dec})$. Pick a random $s \in \mathbb{Z}_p^*$, and compute $c_1 = g^s$, $c_2 = H(\mathsf{ID})^s$, $c_3 = G(F(\mathsf{com}))^s$ and $c_4 = (M||\mathsf{dec}) \cdot e(g_1, g_2)^s$. We require $M||\mathsf{dec}$ is encoded as an element of $\mathbb{G}_2$, and such encoding is efficiently invertible. Denote $c = (c_1, c_2, c_3, c_4)$ and $\mathsf{tag} = \mathsf{Mac}_r(c)$. The ciphertext is $C = \langle c, \mathsf{com}, \mathsf{tag}\rangle$.

Decryption. To decrypt a ciphertext $C' = \langle c', \mathsf{com}', \mathsf{tag}'\rangle$ for identity ID, parse $c = (c_1', c_2', c_3', c_4')$ and compute $(M'||\mathsf{dec}') = c_4' \cdot e(c_2', d_2) \cdot e(d_1, c_1')^{-1}$, especially, output "$\perp$" if this fails or $e(g, c_3') \neq e(c_1', G(F(\mathsf{com})))$. Run $\mathsf{R}(\mathsf{pub}, \mathsf{com}', \mathsf{dec}')$ to obtain a string r'; outputs M' if $r' \neq \perp$ and $\mathsf{Vrfy}(c', \mathsf{tag}')$ $= 1$, otherwise "$\perp$".

We base our proof on the following lemmas, whose proofs can be found in Appendix F.

Lemma 5.5 *The above IBE scheme is* IND-ID-CCA *secure and* L-PTXT*.*

Lemma 5.6 *The above IBE scheme is* L-CTXT*.*

Lemma 5.7 *Let* Π *denote the above IBE scheme. Then,* $NT(\Pi)$ *is not* sUF-CMA *secure.*

Combining Lemma 5.5, 5.6 and 5.7, Theorem 5.2 is proven. □

Analyses on the original Boneh-Franklin IBE (using FO conversion [FO99b] thus with random oracles) and Gentry IBE [Ge06] (without random oracles but based on a stronger assumption) also support our statement of Theorem 5.2. It is also worth repeating that the above examples show L-CTXT is a natural security definition.

References

[ADR02] J. H. An, Y. Dodis and T. Rabin. "On the Security of Joint Signature and Encryption". In *Advances in Cryptology-Eurocrypt 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 83-107, 2002.

[An97] R. Anderson. "Two Remarks on Public Key Cryptology". Invited Lecture, ACM-CCS 1997, available at http://www.cl.cam.ac.uk/ftp/users/rja14/forwardsecure.pdf

[BB04a] D. Boneh and X. Boyen. "Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles". In *Advances in Cryptology-Eurocrypt 2004*, Lecture Notes in Computer Science, Vol. 3027, Springer-Verlag, pp. 223-238, 2004.

[BB04b] D. Boneh and X. Boyen. "Secure Identity Based Encryption Without Random Oracles". In *Advances in Cryptology-Crypto 2004*, Lecture Notes in Computer Science, Vol. 3152, Springer-Verlag, pp. 443-459, 2004.

[BDOP04] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano. "Public Key Encryption with Keyword Search". In *Advances in Cryptology-Eurocrypt 2004*, Lecture Notes in Computer Science, Vol. 3027, Springer-Verlag, pp. 506-522, 2004.

[BF01] D. Boneh and M. Franklin. "Identity-Based Encryption from the Weil Pairing". Extended abstract in *Advances in Cryptology-Crypto 2001*, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001. See also http://eprint.iacr.org/2001/090/

[BFM88] M. Blum, P. Feldman and Silvio Micali. "Non-Interactive Zero-Knowledge and Its Applications" (Extended Abstract). In *ACM Symposium on Theory of Computing (STOC) 1988*, pp. 103-112, 1988.

[BK05] D. Boneh and J. Katz. "Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption". In *Topics in Cryptology-CT-RSA'05*, Lecture Notes in Computer Science, Vol. 3376, Springer-Verlag, pp. 87-103, 2005.

[BLS01] D. Boneh, B. Lynn and H. Shacham. "Short Signatures from the Weil Pairing". In *Advances in Cryptology-Asiacrypt 2001*, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, pp. 514-532, 2001.

[BP02] M. Bellare and A. Palacio. "Protecting against Key Exposure: Strongly Key-Insulated Encryption with Optimal Threshold", available at http://eprint.iacr.org/2002/064/

[BSW06] D. Boneh, E. Shen, and B. Waters " Strongly Unforgeable Signatures Based on Computational Diffie-Hellman" In *International Conference on Theory and Practice of Public-Key Cryptography (PKC) 2006*, Lecture Notes in Computer Science, Vol. 3958, Springer-Verlag, pp. 229-240, 2006.

[CHK03] R. Canetti, S. Halevi and J. Katz, "A Forward Secure Public Key Encryption Scheme", In *Advances in Cryptology-Eurocrypt 2003*, Lecture Notes in Computer Science, Vol. 2656, Springer-Verlag, pp.255-271, 2003.

[CHK04] R. Canetti, S. Halevi and J. Katz. "Chosen-Ciphertext Security from Identity-Based Encryption". In *Advances in Cryptology-Eurocrypt 2004*, Lecture Notes in Computer Science, Vol. 3027, Springer-Verlag, pp. 207-222, 2004.

[Co01] C. Cocks. "An Identity Based Encryption Scheme Based on Quadratic Residues". In *IMA. International Conference 2001*, Lecture Notes in Computer Science, Vol. 2260, Springer-Verlag, pp. 360-363, 2001.

[CFH+07] Y. Cui, E. Fujisaki, G. Hanaoka, H. Imai, and R. Zhang. "Formal Security Treatments for Signatures from Identity-Based Encryption". In *ProvSec 2007*, Lecture Notes in Computer Science, Vol. 4784, Springer-Verlag, pp. 218-227, 2007.

[DKXY02] Y. Dodis, J. Katz, S. Xu and M. Yung. "Key-Insulated Public Key Cryptosystems", In *Advances in Cryptology-Eurocrypt 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp.65-82, 2002.

[FO99a] E. Fujisaki and T. Okamoto. "How to Enhance the Security of Public-Key Encryption at Minimum Cost". In *Public-Key Cryptography (PKC) 1999*, Lecture Notes in Computer Science, 1560, pp.53-68. Springer-Verlag, 1999.

[FO99b] E. Fujisaki and T. Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In *Advances in Cryptology-Crypto 1999*, volume 1666 of Lecture Notes in Computer Science, pp.537–554. Springer-Verlag, 1999.

[Ge06] C. Gentry. "Practical Identity-Based Encryption Without Random Oracles". In *Advances in Cryptology-Eurocrypt 2006*, Lecture Notes in Computer Science, Vol. 4004, Springer-Verlag, pp. 445-464, 2006.

[GS02] C. Gentry and A. Silverberg. "Hierarchical ID-Based Cryptography". In *Advances in Cryptology-Asiacrypt 2002*, Lecture Notes in Computer Science, Vol. 2501, Springer-Verlag, pp. 548-566, 2002.

[GM84] S. Goldwasser and S. Micali. "Probabilistic Encryption". In *Journal of Computer Security*, Vol. 28, pp. 270-299, 1984.

[GMR88] S. Goldwasser, S. Micali and R. Rivest. "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks". In *SIAM Journal of Computing* 17(2), pp. 281-308, 1988.

[HL02] J. Horwitz and B. Lynn. "Toward Hierarchical Identity-Based Encryption". In *Advances in Cryptology-Eurocrypt 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 466-481, 2002.

[NY90] M. Naor and M. Yung. "Public-Key Cryptosystems Provably-Secure against Chosen-Ciphertext Attacks". In *ACM Symposium on Theory of Computing (STOC) 1990*, pp. 427-437, 1990.

[OP01] T. Okamoto and D. Pointcheval. "The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes". In Topics in Cryptology - CT-RSA'01, Lecture Notes in Computer Science, Vol. 2020, Springer-Verlag, pp. 159-175, 2001.

[RS91] C. Rackoff and D. Simon. "Non-interactive Zero-knowledge Proof of Knowledge and Chosen Ciphertext Attack". In *Advances in Cryptology-Crypto 1991*, Lecture Notes in Computer Science, Vol. 576, Springer-Verlag, pp. 433-444, 1992.

[Sa99] A. Sahai. "Non-Malleable Non-Interactive Zero Knowledge and Adaptive Chosen-Ciphertext Security". In *IEEE Symposium on Foundations of Computer Science (FOCS) 1999*, pp. 543–553, 1999.

[Sh84] A. Shamir. "Identity-Based Cryptosystems and Signature Schemes". In *Advances in Cryptology-Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47-53, 1984.

[Sti05] D. Stinson. "Cryptography Theory and Practice", Third Edition CRC Press, 2005

[Wat05] B. Waters. "Efficient Identity-Based Encryption Without Random Oracles". In *Advances in Cryptology-Eurocrypt 2005*, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, pp.114-127, 2005. See also http://eprint.iacr.org/2004/180/

A Waters IBE [Wat05]

Waters proposed the first efficient IND-ID-CCA secure IBE scheme without using random oracle. We abstract their scheme in the following.

Setup On input 1^k, generate groups $\mathbb{G}_1, \mathbb{G}_2$ with prime order p, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Pick up a secret $\alpha \xleftarrow{R} \mathbb{Z}_p$. Compute $g_1 = g^\alpha$ from a random generator g of $\mathbb{G}_1$, and select $g_2 \xleftarrow{R} \mathbb{G}_2$. Choose $u_i \xleftarrow{R} \mathbb{G}_1$ for $0 \leq i \leq n$, and set a hash function $H : \{0,1\}^n \rightarrow \mathbb{G}_1$ as $H(x) = u_0 \prod_{i=1}^{n} u_i{}^{x_i}$, where x_i denotes i-th bit of x. The public system parameter is $\langle \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, H \rangle$, the master key is g_2^α.

Extraction For identity $\mathsf{ID} \in \{0,1\}^n$, pick up $r \xleftarrow{R} \mathbb{Z}_p$, the private key $\mathsf{SK}_{\mathsf{ID}} = (d_1, d_2)$ is produced by computing $d_1 = g_2^{\alpha} \cdot H(\mathsf{ID})^r,\ d_2 = g^r$.

Encryption On input message M and ID, choose $s \xleftarrow{R} \mathbb{Z}_p$, and output ciphertext as $C = (c_1, c_2, c_3)$ s.t. $c_1 = g^s,\ c_2 = H(\mathsf{ID})^s,\ c_3 = M \cdot e(g_1, g_2)^s$.

Decryption Let $C' = (c'_1, c'_2, c'_3)$ be a ciphertext for ID. Use the $\mathsf{SK}_{\mathsf{ID}} = (d_1, d_2)$ to recover message as: $M' = c'_3 \cdot e(c'_2, d_2) \cdot e(c'_1, d_1)^{-1} = c'_3 \cdot e(H(\mathsf{ID})^s, g^r) \cdot e(g_1, g_2)^{-s} \cdot e(H(\mathsf{ID})^r, g^s)^{-1}$.

B Proof of Theorem 4.2

The proof can be straightforwardly done. However, we properly address it. Towards a contradiction, assuming that there exists a $\mathsf{UF\text{-}CMA}$ forger $\mathcal{A}$ against $NT(\Pi)$ with running time t, q signature queries, and succeeding probability $\epsilon_{\mathcal{A}} > \epsilon$, we build an $\mathsf{L\text{-}CTXT}$ adversary $\mathcal{B}$ against Π with running time $t+O(\tau)$, q key extraction queries, and succeeding probability $\epsilon_{\mathcal{B}} \geq \epsilon_{\mathcal{A}}$.

For a given public system parameter PK, $\mathcal{B}$ passes it to $\mathcal{A}$. When $\mathcal{A}$ asks a signing query on a message m_i for $1 \leq i \leq q$, $\mathcal{B}_1$ queries its own key extraction oracle $\mathcal{O}_e$ on "identity" m_i to get the corresponding decryption key, and delivers it to $\mathcal{A}$ as the signature σ_i for m_i. This simulation is, of course, perfect. When $\mathcal{A}$ outputs (σ^*, m^*), $\mathcal{B}$ also outputs $(\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*})$, where $\mathsf{ID}^* = m^*$ and $\mathsf{SK}'_{\mathsf{ID}^*} = \sigma^*$. Since $\Pr[M' = M | M \xleftarrow{R} \mathcal{M}; C \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}^*}, C, \mathsf{PK})] = \epsilon_{\mathcal{A}}$ and $M \in \mathcal{M}$, we have that $\epsilon_{\mathcal{B}} \geq \epsilon_{\mathcal{A}}$. □

C Proof of Lemma 4.1

Towards a contradiction, assuming that there exists a $\mathsf{L\text{-}CTXT}$ adversary $\mathcal{A}$ against Π with running time t, q key extraction queries, and succeeding probability $\epsilon_{\mathcal{A}} > \epsilon$, we build an $\mathsf{IND\text{-}ID\text{-}CPA}$ adversary $\mathcal{B}$ against Π with running time $t + O(\tau)$, q key extraction queries, and advantage $\epsilon_{\mathcal{B}} \geq \frac{\gamma\epsilon_{\mathcal{A}} - \epsilon_s}{2-2\gamma}$.

For a given public system parameter PK, $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ interacts $\mathcal{A}$ as follows:

Algorithm $\mathcal{B}_1^{\mathcal{O}_e}(\mathsf{PK})$	**Algorithm** $\mathcal{B}_2^{\mathcal{O}_e}(s, C^*)$
$(\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*}) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{PK})$;	$(\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*}, \mathsf{PK}) \leftarrow s$;
$(M_0, M_1) \xleftarrow{R} \mathcal{M}^2$;	$M' \leftarrow \mathsf{Dec}(\mathsf{SK'}_{\mathsf{ID}^*}, C^*, \mathsf{PK})$;
$s \leftarrow (\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*}, \mathsf{PK})$;	if $M' = M_\beta$ for $\beta \in \{0,1\}$, $b' \leftarrow 1 - \beta$;
return $(\mathsf{ID}^*, M_0, M_1, s)$	else, $b' \xleftarrow{R} \{0,1\}$;
	return b'

When $\mathcal{A}$ issues a key extraction query on identity "ID", $\mathcal{B}$ queries its own key extraction oracle for the same identity, and forwards the secret key $\mathsf{SK}_{\mathsf{ID}}$ to $\mathcal{A}$. This simulation is, of course, perfect. $\mathcal{S}$ denotes the simulated signing oracle by $\mathcal{B}$. For a challenge ciphertext C^*, $\mathcal{B}$ decrypts it with $\mathsf{SK}'_{\mathsf{ID}^*}$ which is $\mathcal{A}$'s output, and returns $1 - b'$ if the decryption result M' is identical to $M_{b'}$ for $b' \in \{0,1\}$, or a random bit otherwise. Now, we estimate $\mathcal{B}$'s advantage $\epsilon_{\mathcal{B}}$, that is,

$$\epsilon_{\mathcal{B}} = |\Pr[M' = M_{1-b} | \mathsf{Exp}] + \frac{1}{2}\Pr[M' \notin \{M_0, M_1\} | \mathsf{Exp}] - \frac{1}{2}|,$$

where Exp denotes $[(\mathsf{PK}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^k); (\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}}) \leftarrow \mathcal{A}^{\mathcal{S}}(\mathsf{PK}); b \xleftarrow{R} \{0,1\}; C^* \leftarrow \mathsf{Enc}(\mathsf{ID}^*, M_b, \mathsf{PK}); M' \leftarrow \mathsf{Dec}(\mathsf{SK'}_{\mathsf{ID}^*}, C^*, \mathsf{PK})]$. Since $\mathcal{A}$ breaks $\mathsf{L\text{-}CTXT}$ with probability $\epsilon_{\mathcal{A}}$, we have that $\Pr[M' \in \mathcal{M} | \mathsf{Exp}] \geq \epsilon_{\mathcal{A}}$.

Furthermore, since $N(\Pi)$ is (t, q, ϵ_s)-$\mathsf{UF\text{-}CMA}$, we have that $\Pr[M' = M_b|\mathsf{Exp}] \leq \epsilon_s$. Then, $\epsilon_{\mathcal{B}}$ is estimated as follows. Since M_{1-b} is independent of both $\mathsf{SK'}_{\mathsf{ID}^*}$ and C^*, $\Pr[M' = M_{1-b}|\mathsf{Exp}]$ is estimated as

$$\Pr[M' = M_{1-b}|\mathsf{Exp}] \geq \frac{1}{|\mathcal{M}|-1}\Pr[M' \in \mathcal{M}\backslash\{M_b\}|\mathsf{Exp}]] \geq \frac{\epsilon_{\mathcal{A}} - \epsilon_s}{|\mathcal{M}|-1}.$$

We also have that $\Pr[M' \notin \{M_0, M_1\}|\mathsf{Exp}] + \Pr[M' = M_{1-b}|\mathsf{Exp}] \geq 1 - \epsilon_s$, and consequently,

$$\begin{aligned} \epsilon_{\mathcal{B}} &= |\frac{1}{2}\Pr[M' = M_{1-b}|\mathsf{Exp}] + \frac{1}{2}(\Pr[M' \notin \{M_0, M_1\}|\mathsf{Exp}] + \Pr[M' = M_{1-b}|\mathsf{Exp}]) - \frac{1}{2}| \\ &\geq \frac{1}{2}(\frac{\epsilon_{\mathcal{A}} - |\mathcal{M}|\epsilon_s}{|\mathcal{M}|-1}) \geq \frac{1}{2}(\frac{\gamma\epsilon_{\mathcal{A}} - \epsilon_s}{1-\gamma}). \end{aligned}$$

We note that $\gamma < 1/|\mathcal{M}|$ since we assume Π does not satisfy γ-$\mathsf{L\text{-}PTXT}$. The running time of $\mathcal{B}$ is $t+O(\tau)$, and $\mathcal{B}$ asks exactly q key extraction queries, which are easily verified from the description of $\mathcal{B}$. This completes the proof of Lemma 4.1. □

D Proof of Theorem 4.4

We modify Waters IBE in the following way: the setup and key extraction algorithms are the same as Waters IBE. Notations follow those addressed in Appendix A. To encrypt a message $M \in \{0,1\}$, randomly selecting $s \in \mathbb{Z}_p$, we set its ciphertext as $C = (c_1, c_2, c_3)$, s.t. $c_1 = g^s, c_2 = H(\mathsf{ID})^s, c_3 = e(g_1, g_2)^{s+M}$. The decryption algorithm is also the same as Waters IBE except that it returns 1 if $mes = e(g_1, g_2)$, 0 if $mes = 1$, or "$\perp$" otherwise. Here mes is defined by $mes = c_3' \cdot e(c_2', d_2) \cdot e(c_1', d_1)^{-1} = e(g_1, g_2)^{s+M} \cdot e(H(\mathsf{ID})^s, g^r) \cdot (e(g_1, g_2)^s \cdot e(H(\mathsf{ID})^r, g^s))^{-1}$.

1. The scheme can be also proven to be $\mathsf{IND\text{-}ID\text{-}CPA}$ secure under the DBDH assumption. Note that by setting $M = e(g_1, g_2)^m$ as the plaintext for Waters IBE, we get the original scheme.
2. Since the message space is only one-bit, it does not meet $\mathsf{L\text{-}PTXT}$ (however, it meets $\mathsf{L\text{-}CTXT}$!).
3. The Naor-transformed signature from the above IBE scheme is $\mathsf{UF\text{-}CMA}$ under the CBDH assumption. Roughly speaking, if it is possible for an adversary to come with $(\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*})$ such that $m = \mathsf{Dec}(\mathsf{SK}'_{\mathsf{ID}^*}, \mathsf{Enc}(\mathsf{ID}^*, m, \mathsf{PK}), \mathsf{PK})$, then for a given BDH instance (g_1, g_2, g^t), it is also possible to extract $e(g_1, g_2)^t$ by using SK'_{ID^*}.

Summarize all these points, we prove the theorem. □

E Proof of Theorem 5.1

E.1 Proof of Lemma 5.2

We prove the lemma by demonstrating a successful forgery of a signature. For a given verification key $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, g_2, g_3, F, G, H\rangle$, pick $\mathsf{SK}'_{\mathsf{m}} = (d_1', d_2') \in \mathbb{G}_1^2$ randomly, and set it as a forged signature for a message m. Then, verification process is carried out as follows. First, a verifier picks a random $M \in \{0,1\}$ and encrypts it by using identity "m". Let $C = (c_1, c_2, c_3, c_4, \sigma, \mathsf{VK})$ denote the ciphertext. If M is recovered from C by using $\mathsf{SK}'_{\mathsf{m}}$, the forgery is considered successful. First, the verifier tests validity of σ and c_3. Since σ and c_3 are generated in a correct manner, the verifier decides it as a valid ciphertext. Note that $\mathsf{SK}'_{\mathsf{m}}$ is not used for the validity check, and consequently, "$\perp$" is never output in this process. Then, the verifier calculates $mes = c_4 \cdot e(c_2, d_2') \cdot e(d_1', c_1)^{-1}$. From the encoding rule, the recovered plaintext is 1 if $mes = e(g_1, g_2)$, 0 if $mes = 1$, or a random bit $m' \in \{0,1\}$ otherwise. This means the verifier outputs `accept` with probability 1/2, which is non-negligible. $\square$

We note that in the proof of Lemma 5.2, public verifiability of [CHK04] functions significantly. Therefore, for example, Waters IBE with another transform in [BK05] for chosen-ciphertext security, cannot be a counterexample for Theorem 5.1.

E.2 Proofs of Lemma 5.3

Proof of Lemma 5.3 $\mathcal{B}$ is an adversary that wants to either solves GBDH problem defined on $(\mathbb{G}_1, \mathbb{G}_2)$, or break the unforgeability of Σ. At first, $\mathcal{B}$ is given a random instance $\langle g, g^a, g^b, g^c\rangle$, where g is a generator of $\mathbb{G}_1$. $\mathcal{B}$ is also given the verification key VK^*, generated by $\mathsf{Gen}(1^\mathsf{k})$. $\mathcal{B}$ can access two oracles: a DBDH oracle $\mathcal{O}$ and a signing oracle $\mathcal{O}_s$. $\mathcal{B}$ then interacts an IND-ID-CCA adversary $\mathcal{A}$ as follows:

Setup $\mathcal{B}$ gives $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, G, H\rangle$, where G, H are random oracles controlled by $\mathcal{B}$.

***G*-queries** Let G-list be a list with 6-entries $(T_i, \mathsf{VK}_i, c_{1i}, \omega_i, M_i, c_{2i})$ $(1 \le i \le q_G)$, initially empty. On a query $(T_i, \mathsf{VK}_i, c_{1i})$, $\mathcal{B}$ searches G-list for $(T_i, \mathsf{VK}_i, c_{1i}, \omega_i, M_i, c_{2i})$ where $(T_i, \mathsf{VK}_i, c_{1i}, \omega_i)$ has been defined already. If it has been queried before, $\mathcal{B}$ returns ω_i. Otherwise, $\mathcal{B}$ checks if M_i and c_{2i} are already defined. If yes, $\mathcal{B}$ returns sets $\omega_i = M_i \oplus c_{2i}$ and adds $(T_i, \mathsf{VK}_i, c_{1i}, \omega_i)$ to G-list. If no such data is found, $\mathcal{B}$ randomly returns $\omega_i \in \{0,1\}$ and appends $(T_i, \mathsf{VK}_i, c_{1i}, \omega_i)$ to G-list.

***H*-queries** $\mathcal{B}$ maintains a H-list with 4-entries $(\mathsf{ID}_i, h_i, \beta_i, coin_i)$, $(1 \le i \le q_H)$, initially empty. where ID_i is the i-th query on H, h_i is the response, β_i is chosen at random, and $coin_i$ is an internal coin tossing that shows "0" with probability δ determined later. On a query on ID_i, if ID_i has appeared in the H-list, returns h_i. Otherwise, randomly pick β_i from $\mathbb{Z}_p^*$, and flip a biased coin, which gets 0 with probability δ to be decided later. If $coin_i = 0$, then set $h_i = g^{\beta_i}$; if $coin_i = 1$, then set the $h_i = (g^b)^{\beta_i}$ as the response.

Extraction queries On key extraction query on ID_i, $\mathcal{B}$ searches in H-list, if $coin_i = 0$, then returns $\mathsf{SK}_{\mathsf{ID}_i} = (g^a)^{\beta_i}$; otherwise reports failure and quits with an output $T \stackrel{R}{\leftarrow} \mathbb{G}_2$.

Encryption queries On the ID^* chosen by $\mathcal{A}$, without loss of generality, suppose it has appeared somewhere in the H-list as ID_i. $\mathcal{B}$ chooses $M^* \stackrel{R}{\leftarrow} \{0,1\}$ and $c_2^* \stackrel{R}{\leftarrow} \{0,1\}$, and asks the signing oracle $\mathcal{O}_s$ on signature of $((g^c)^{1/\beta^*}, c_2^*)$ with respect to VK^*, and gets a signature σ^* from $\mathcal{O}_s$. $\mathcal{B}$ then returns $\langle (g^c)^{1/\beta^*}, c_2^*, \sigma^*, \mathsf{VK}^*\rangle$ as the challenge ciphertext.

Decryption queries On a decryption query $(c_{1j}, c_{2j}, \sigma_j, \mathsf{VK}_j)$, $\mathcal{B}$ checks if σ_j is a correct signature on (c_{1j}, c_{2j}) with respect to VK_j. If not, $\mathcal{B}$ returns $\perp$. Otherwise, $\mathcal{B}$ searches G-list for $(T_j, \mathsf{VK}_j, c_{1j}, \omega_j, M_j, c_{2j})$ such that $(T_j, \mathsf{VK}_j, c_{1j}, \omega_j)$ has been defined already. If yes, $\mathcal{B}$ sets $M_j = c_{2j} \oplus \omega_j$. Otherwise, $\mathcal{B}$ chooses $M_j \in \{0,1\}$ and sets $\omega_j = M_j \oplus c_{2j}$. In both cases, $\mathcal{B}$ appends $c_{1j}, c_{2j}, M_j, \mathsf{VK}_i$ to G-list and returns M_j as required plaintext. If $\mathcal{A}$ submits a ciphertext $(c_{1j}, c_{2j}, \sigma_j, \mathsf{VK}^*)$ with $\mathsf{Ver}(\mathsf{VK}^*, \sigma_j, (c_{1j}^*, c_{2j}^*)) = \texttt{accept}$ but $\sigma_j \ne \sigma^*$, $\mathcal{B}$ simply terminates simulation and returns σ_j as the forgery to the signature scheme.

If $\mathcal{A}$ asks further queries after it gets the challenge, $\mathcal{B}$ interacts with $\mathcal{A}$ similarly as the above with the only limitation that $\mathcal{A}$ may not ask decryption query on the challenge ciphertext.

After $\mathcal{A}$ outputs a guess b' on bit b, $\mathcal{B}$ searches T_i in the G-list such that $\langle g, g^a, g^b, g^c, T_i\rangle$ is a BDH-tuple.

If $\mathcal{B}$ does not acquire a valid forgery on VK^* via decryption queries, $\mathcal{A}$ can only get any advantage in the game by querying T to G oracle, since the information of M_b is perfectly hidden because G's output is always random. In this case, if $\mathcal{B}$ doesn't abort, $\mathcal{B}$ always succeeds in outputting $T = e(g, g)^{abc}$. Since the H-oracle, G-oracle and decryption queries are perfectly simulated, $\mathcal{B}$ may only fail in replying the challenge query or extraction queries. We have,

$$\epsilon_{\mathcal{B}} \geq \delta^{q_e}(1-\delta)(\epsilon_{\mathcal{A}} - \epsilon_s) \geq (\epsilon_{\mathcal{A}} - \epsilon_s)/(eq_e)$$

as claimed, where the probability $\delta^{q_e}(1-\delta) \approx 1/(eq_e)$ gets maximized at $\delta = q_e/(q_e+1)$ for large q_e. The claimed time bounds, queries to $\mathcal{O}$ and $\mathcal{O}_s$ is easily verified as $O(t + (q_H + q_G)\tau)$, 1, q_G respectively. □

E.3 Proof of Lemma 5.4

It is interesting that the signature is not even UF-CMA, though the underlying IBE builds on an sUF-CMA signature. It is proven by showing a counterexample that there exists a forgery with non-negligible probability. Namely, for a given public system parameter $\langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, G, H \rangle$, choose $\mathsf{SK}'_{\mathsf{ID}} = s' \in \mathbb{Z}_p^*$ at random. Set it as a signature for certain message m. The verifier first chooses randomly a $M \in \{0, 1\}$, $r \in \mathbb{Z}_p^*$ and obtains the verification key VK generated by one-time signature $\sum$. Further, encrypts M with the public key m, such as, $C = (c_1, c_2, \mathsf{VK}, \sigma)$, where $c_1 = g^r, c_2 = M \oplus G(e(g_1, H(m))^r, \mathsf{VK}, g^r))$. If the same M could be recovered by $\mathsf{SK}'_{\mathsf{ID}}$, the forgery is considered successful. Since in decryption the $\mathsf{SK}'_{\mathsf{ID}}$ is only used for recovering the M, but not for checking the validity of the ciphertext, verifier will finally get a message $M' = c_2 \oplus G(e(c_1, \mathsf{SK}'_{\mathsf{ID}}), \mathsf{VK}, c_1)$, s.t. $M' \in \{0, 1\}$ without outputting $\perp$. As G is assumed a random oracle, the output will be uniformly distributed. Therefore, M' is also uniformly distributed in $\{0, 1\}$ no matter what $\mathsf{SK}'_{\mathsf{ID}}$ is, which means the verifier outputs `accept` with probability 1/2, obviously non-negligible. □

F Proof of Theorem 5.2

We first review definition on message authentication code and encapsulation from [BK05] below.

Message Authentication Code. A message authentication code scheme consists of a pair of PPT algorithms: $\Phi = (\mathsf{Mac}, \mathsf{Vrfy})$. The authentication algorithm Mac takes as input a key sk and a message M, and outputs a string tag. The verification algorithm Vrfy takes as input a key sk, a message M, and a string tag and outputs either "0" or "1". We require that for all sk and M, $\mathsf{Vrfy}_{sk}(M, \mathsf{Mac}_{sk}(M)) = 1$. For simplicity, we assume that Mac and Vrfy are deterministic.

Definition F.1 (Secure MAC) *A message authentication code* $\Phi = (\mathsf{Mac}, \mathsf{Vrfy})$ *is secure, if for any algorithm* $\mathcal{A}$, $\Pr[\mathsf{Exp}^{\mathsf{mac}}_{\mathcal{A},\Phi}(k) = 1]$ *is negligible, where* $\mathsf{Exp}^{\mathsf{mac}}_{\mathcal{A},\Phi}(k)$: $[sk \stackrel{R}{\leftarrow} \{0,1\}^k; (M, s) \leftarrow \mathcal{A}(k); \mathsf{tag} \leftarrow \mathsf{Mac}_{sk}(M); (M', \mathsf{tag}') \leftarrow \mathcal{A}(\mathsf{tag}, s); \text{return 1 if } (M', \mathsf{tag}') \neq (M, \mathsf{tag}) \wedge \mathsf{Vrfy}_{sk}(M', \mathsf{tag}') = 1, \text{ or 0 otherwise}]$.

Encapsulation. An encapsulation scheme is a triple of PPT algorithms $\Psi = (\mathsf{Setup}, \mathsf{S}, \mathsf{R})$. The Setup algorithm Setup takes as input the security parameter 1^k and outputs a string pub. The encapsulating algorithm S takes as input 1^k and pub, and outputs $(r, \mathsf{com}, \mathsf{dec})$ with $r \in \{0,1\}^k$. We refer to com as the public commitment string and dec as the de-commitment string. The reconstruction algorithm R takes as input (pub,com,dec) and outputs an $r \in \{0,1\}^k \cup \{\perp\}$. We require for pub output by Setup and for all $(r, \mathsf{com}, \mathsf{dec})$ output by $\mathsf{S}(1^k, \mathsf{pub})$, $\mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}) = r$. For simplicity, we assume com and dec have fixed lengths for any given value of security parameter.

An encapsulation scheme $\Psi = (\mathsf{Setup}, \mathsf{S}, \mathsf{R})$ is ϵ_h-hiding if for any algorithm $\mathcal{A}$,

$\epsilon_h \geq \Pr[\mathsf{Exp}^{\mathsf{hiding}}_{\mathcal{A},\Psi}(k) = 1] - 1/2$, where $\mathsf{Exp}^{\mathsf{hiding}}_{\mathcal{A},\Psi}(k) : [\mathsf{pub} \leftarrow \mathsf{Setup}(1^k); r_0 \xleftarrow{R} \{0,1\}^k; (r_1, \mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{S}(1^k, \mathsf{pub});$
$b \xleftarrow{R} \{0,1\};$ return 1 if $\mathcal{A}(1^k, \mathsf{pub}, \mathsf{com}, r_b) = b,$ or 0 otherwise].

An encapsulation scheme $\Psi = (\mathsf{Setup}, \mathsf{S}, \mathsf{R})$ is ϵ_b-binding, if for any algorithm $\mathcal{A}$, $\epsilon_b \geq \Pr[\mathsf{Exp}^{\mathsf{binding}}_{\mathcal{A},\Psi}(k) = 1]$, where $\mathsf{Exp}^{\mathsf{binding}}_{\mathcal{A},\Psi}(k) : [\mathsf{pub} \leftarrow \mathsf{Setup}(1^k); (r, \mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{S}(1^k, \mathsf{pub}); \mathsf{dec}' \leftarrow \mathcal{A}(\mathsf{pub}, r, \mathsf{com}, \mathsf{dec});$
return 1 if $\mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}') \notin \{\perp, r\},$ or 0 otherwise].

Definition F.2 (Secure Encapsulation) *An encapsulation scheme Ψ is secure if it is ϵ_h-hiding and ϵ_b-binding where ϵ_h and ϵ_b are negligible.*

Proof of Lemma 5.5. The IND-ID-CCA security can be straightforwardly proven by [Wat05] and [BK05]. Denote $\mathcal{M}$ as the message space, from the above specification, $1/|\mathcal{M}|$ is a negligible function of the security parameter k. □

Proof of Lemma 5.6. Let Π denote the Waters-Boneh-Katz IBE scheme given in Section 5.2. Let $\mathsf{PK} = \langle \mathbb{G}_1, \mathbb{G}_2, e, p, g, g_1, g_2, g_3, F, G, H, \mathsf{pub} \rangle$ be the public system parameter of Π. Assume that there exists an adversary $\mathcal{A}$ such that $\Pr[\mathsf{Exp}^{\mathsf{l\text{-}ctxt}}_{\mathcal{A},\Pi}(k) = 1]$ is non-negligible, and that $(\mathsf{ID}^*, \mathsf{SK}'_{\mathsf{ID}^*}(= (d'_1, d'_2))) \leftarrow \mathcal{A}^{\mathcal{O}_e}(\mathsf{PK})$. Let $C = \langle c, \mathsf{com}, \mathsf{tag} \rangle$ be a ciphertext, where $(r, \mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{S}(1^k, \mathsf{pub})$, $M \xleftarrow{R} \mathcal{M}$, and C is generated under PK, identity "ID^*", plaintext M, and encapsulation $(r, \mathsf{com}, \mathsf{dec})$. Let $c = (c_1, c_2, c_3, c_4)$ and $(M' || \mathsf{dec}') = c_4 \cdot e(c_2, d'_2) \cdot e(d'_1, c_1)^{-1}$. $r' \leftarrow \mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}')$. It is sufficient to show that assuming Π is not L-CTXT leads to a contradiction to the security of Ψ.

Claim F.1 *Suppose* Π *is* IND-ID-CCA *secure. If* $\Pr[\mathsf{Exp}^{\mathsf{l\text{-}ctxt}}_{\mathcal{A},\Pi}(k) = 1]$ *is non-negligible,* $\Pr[\mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}') = \mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}) = r]$ *is also non-negligible.*

Proof of Claim F.1. Since $\mathsf{Exp}^{\mathsf{l\text{-}ctxt}}_{\mathcal{A},\Pi}(k) = 1$, in order to pass the verification of Mac, there should be $\mathsf{tag} = \mathsf{Mac}_{r'}(c)$ for some r'. We claim $r' = r$. Assume this is not the case, then there exists dec', using which com can be opened to r' other than r, which contradicts the binding property of the encapsulation. So it must be $r' = r$, i.e., $\Pr[\mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}') = \mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}) = r]$ happens with non-negligible probability. □

Claim F.2 *If the above scheme is* IND-ID-CCA, $\mathsf{dec}' \neq \mathsf{dec}$ *with overwhelming probability.*

Proof of Claim F.2. Without loss of generality, write $\mathsf{SK}'_{\mathsf{ID}^*} = (d_1, d_2) = (g_2^{\alpha} H(\mathsf{ID})^{r_1}, g^{r_2})$. If $r_1 = r_2$, the adversary has recovered the correct secret key for ID^*, thus is able to break IND-ID-CCA security. So $r_1 \neq r_2$, which implies $r_2 - r_1 \neq 0$. It is verifiable that this time, $(M' || \mathsf{dec}') = (M || \mathsf{dec}) e(H(\mathsf{ID}), g)^{s(r_2 - r_1)}$. This immediately leads to the claim that $\mathsf{dec}' \neq \mathsf{dec}$ with overwhelming probability, since s is chosen randomly by the verifier. □

Finally, suppose for dec' (computed from $\mathsf{SK}'_{\mathsf{ID}^*}$) where $\mathsf{dec}' \neq \mathsf{dec}$, if $\mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}') = \mathsf{R}(\mathsf{pub}, \mathsf{com}, \mathsf{dec}) = r$ holds with non-negligible probability, Ψ is no longer hiding, which contradicts the assumption that Ψ is a secure encapsulation scheme. This completes the proof of Lemma 5.6. □

Proof of Lemma 5.7. For any given signature $\sigma = (s_1, s_2)$ on a message m, one can easily re-randomize σ output a different signature $\sigma' = (s_1 \cdot H(m)^{r'}, s_2 \cdot g^{r'})$ with $r' \xleftarrow{R} \mathbb{Z}_p^*$. It is easily verified this is a successful forgery. □

Theorem 5.2 then follows Lemma 5.5, 5.6 and 5.7. □