Identity-based Matchmaking Encryption with Stronger Security and Instantiation on Lattices

Yuejun Wang[1], Baocang Wang[1], Qiqi Lai[2], and Yu Zhan[1]

[1] Xidian University
yuejun.w@stu.xidian.edu.cn, bcwang@xidian.edu.cn, zhanyu@xidian.edu.cn
[2] Shaanxi Normal University
laiqq@snnu.edu.cn

Abstract. An identity-based matchmaking encryption (IB-ME) scheme proposed at JOC 2021 supports anonymous but authenticated communications in a way that communication parties can both specify the senders or receivers on the fly. IB-ME is easy to be used in several network applications requiring privacy-preserving for its efficient implementation and special syntax. Despite the rigorous security proofs in previous security models, the existing IB-ME schemes are still possibly vulnerable to some potential neglected attacks. Aiming at the above problems, we provide a stronger security definition of authenticity considering new attacks to fit real-world scenarios and then propose a generic construction of IB-ME satisfying the new model. Inspired by the prior IB-ME construction of Chen *et al.*, the proposed scheme is constructed by combining 2-level anonymous hierarchical IBE (HIBE) and identity-based signature (IBS) schemes. In order to upgrade lattice-based IB-ME with better efficiency, we additionally improve a lattice IBS, as an independent technical contribution, to shorten its signature and thus reduce the final IB-ME ciphertext size. By combining the improved IBS and any 2-level adaptively-secure lattice-based HIBE with anonymity, we finally obtain the *first* lattice-based IB-ME construction achieving privacy and new-proposed stronger authenticity simultaneously.

1 Introduction

Matchmaking Encryption (ME) [AFNV21] is a quite useful primitive that allows any sender and receiver to predesignate policies that the other party should satisfy to reveal message. In an ME scheme, a sender uses the secret encryption key ek_σ associated with his attribute σ to generate ciphertexts with additional specifying policy $\mathbb{R}$. Each receiver obtains different decryption keys from the authority with just one key dk_ρ associated with his attribute ρ and others $\mathsf{dk}_\mathbb{S}$ related to his chosen policy $\mathbb{S}$. When decrypting a ciphertext linking $(\sigma,\ \mathbb{R})$ using dk_ρ and $\mathsf{dk}_\mathbb{S}$, the receiver recovers the plaintext by matching the attributes and policies of both participants. The entire procedure of policy matchmaking is privacy-preserved. In other words, nothing will be leaked except whether a match occurred or did not occur. Furthermore, malicious attackers fail to forge ciphertexts embedding fake attributes which were not certificated by the authority.

ME naturally supports several network applications requiring secret communication, such as the scenarios that the both communicating parties need to specify access polices to encrypted plaintext. Ateniese *et al.* [AFNV21] proposed two generic constructions of ME relying on either a 2-input Functional Encryption (FE) scheme [GGG+14] or a FE scheme supporting randomized functionalities (rFE) [GJKS15, AW17]. However, the ME scheme based on rFE only achieves security against bounded collusion. Another approach requiring 2-input FE for general circuits retains full security, but this construction can only be instantiated on a sub-exponentially secure indistinguishable obfuscation (iO) assumption. In fact, in the perspective of more fine-grained syntax, the encryption algorithm of 2-input FE scheme takes an attribute and a message as input. Thus, the underlying 2-input FE in [AFNV21] only requires the functions over message to be identity functions rather than general circuits (while the predicates over indexes to be arbitrary policies). Hence, Francati *et al.* [FFMV22] recently proposed a multi-key predicate encryption scheme (PE) built from learning with errors (LWE) directly and then used 2-key PE to construct ME supporting arbitrary policies with unbounded collusion.

Concept of IB-ME. By contrast, the ME scheme in a relatively restricted identity-based setting is more efficient than ME for general functions and is easy to implement. Identity-based matchmaking encryption (IB-ME) can also be used to construct an anonymous but authentic communication environment.

Being a special case of ME under the identity matching policy, IB-ME features that each sender is given a secret encryption key related to his identity σ, and each receiver has a secret decryption key for his identity ρ. Similarly, senders can select target receiver rcv and encrypt secretly. The receiver takes dk_ρ and arbitrary identity snd as input to decryption algorithm, without an additional decryption key for snd, and obtains messages if and only if identities equality policies both match ($\rho = \mathsf{rcv} \ \wedge \ \sigma = \mathsf{snd}$). The security requirements of IB-ME are privacy and authenticity. When mismatch happens ($\rho \neq \mathsf{rcv}$), privacy not only protects plaintext from illegal leaking, but also prevents decryptors from learning any extra information about sender's identity. Another property, namely authenticity, promises that the ciphertexts associated with σ could only be generated by encryption key ek_σ.

Existing work for IB-ME. The existing constructions for IB-ME are all based on the variants of discrete log problems. By amplifying a secure identity-based encryption (IBE) under chosen plaintext attack [BF01], Ateniese *et al.* [AFNV21] provided the first IB-ME from bilinear Diffie-Hellman (BDH) assumption in random oracle model. The follow-up work [FGRV21] presented an instantiation without random oracle based on non-standard augmented bilinear Diffie-Hellman exponent assumption (q-ABDHE), and its privacy relies on the underlying anonymous IBE [Gen06] in the standard model. Francati *et al.* [FGRV21] also provided a stronger notion of privacy named by enhanced privacy. The scheme also requires non-interactive zero knowledge proof (NIZK) to guarantee authenticity.

An IB-ME scheme based on symmetric external Diffie-Hellman (SXDH) assumption was proposed by Chen *et al.* [CLWW22] recently. The authors the scheme from a variant of anonymous IBE [CLL+13] by absorbing the idea of 2-level Hierarchical Predicate Encryption (HPE) [OT09] and is proven secure in the standard model. In the scheme, receivers obtain 1-level decryption key dk_ρ from the authority, and each sender obtains an encryption key ek_σ which is the signature for message σ (encoded in 2-level) signed by the authority using master secret key. Sender is allowed to use ek_σ to generate ciphertexts making decryption works correctly if the counterpart matches the corresponding equality policy. The privacy is relied on the anonymity property of 1-level IBE scheme, while the unforgeability of the underlying signature scheme is used to protect authenticity.

While the most of previous IB-ME schemes are proven secure against chosen-plaintext attacks (CPA), the follow-up constructions [CHHS23, LLC24] considered privacy against chosen-ciphertext attacks (CCA). Analogous to the distinction between CPA and CCA security for traditional public key cryptosystems, a CCA-private IB-ME scheme permits adversaries additional access to query the decryption oracle. As demonstrated in [CHHS23], applying the Fujisaki-Okamoto (FO) transformation [FO99] to a CPA-secure IB-ME scheme is sufficient to achieve CCA-privacy for free.

More general application scenarios. In previous security models, the authenticity is solely identity authentication, especially less relevant to encrypted message. In other words, the existing security models fail to prevent tampering with plaintexts, even forging. When considering some real-world application scenarios, there exists some classes of forgery of message might affect authenticity, meaning that it is necessary to model new security models capturing such attacks. A valid ciphertext is easily available for an adversary by eavesdropping and is also likely to be malleable and further forged. The first potential forgery is "*forging-to-itself*". In such scenarios, adversaries might get access to obtain ciphertexts from chosen sources, even decrypt partially. Suppose the dean of a faculty usually authorize the associate dean to act him while he is busy. IB-ME enables the dean to delegate part of powers to the associate dean, with the guarantee that any third party fails to get information about the encrypted content. However, once the associate dean can construct a fake authorization on his own, he might have the possession of arbitrary power and claim that he was authorized by the dean.

Another potential forgery is *tamper forgery*. Suppose IB-ME was applied to a bulletin board hidden service, everyone gets access to upload ciphertexts to open server and download ciphertexts from it. Then hackers might obtain and manipulate ciphertexts then upload them without needing any keys, receivers will thus get wrong information.

Nevertheless, the previous schemes [AFNV21, CLWW22] are proven secure under the original security model, these schemes still requires some additional adjustments to recognize the aforementioned forgeries due to the reason that these constructions mainly consider security under chosen-plaintext attacks. Thus, it is necessary to formally define a stronger authenticity property that can defend potential forgeries such as "*forging-to-itself*" and tamper forgery. To some extent, tamper forgeries could be identified simply relying on pre-existing coding rules of plaintext, as tampering will lead to decryption results that do not meet the rules with high probability. While using NIZK is another relatively direct way to solve the said potential forgeries in the same time. Intuitively, ciphertexts would contain additional witnesses to prove the certification of both plaintexts and the identities of sender, the decryption algorithm would also need checking whether the proof is valid or not. The soundness of NIZK guarantees that the witness generating by malicious adversary fails to pass the verification. On the other hand, nothing secret is leaked from the proof itself due to the zero-knowledge property.

Motivation. Although the prior schemes [AFNV21, FGRV21, CLWW22] could supply more practical applications using some tweaks, their security will be entirely broken down for attacks using quantum computers. Quantum algorithms can efficiently solve the mathematical problems such as factoring and discrete log problem, while the previous schemes rely on the latter to protect both privacy and authenticity. This leads us to consider the following question:

Can we build a post-quantum secure IB-ME
supporting more general applications?

1.1 This Work

The work gives several contributions for an IB-ME with stronger security.

- *Improved security definition.* We modified the security definition of authenticity to match more general application requirements. Specifically, we allow the adversary to forge to itself and obtain ciphertexts encrypted with its chosen source and destination by querying encryption oracle. Also the "forge-to-itself" ciphertexts are admissible.
- *Generic construction.* Inspired by the previous schemes, we propose a generic construction to satisfy the modified stronger security definition. The construction is based on a 2-level anonymous HIBE and an Identity-based Signature scheme (IBS), both with adaptive security. The privacy of IB-ME is implied by the recipient-anonymity and semantic security of underlying HIBE. The unforgeability of IBS can guarantee the authenticity.
- *Instantiation on lattices.* To further improve the efficiency of lattice-based IB-ME, we additionally modify an existing IBS based on SIS problem to achieve shorter signature (reduce by $n \cdot (\lceil \log q \rceil)^2$ bits) with better efficiency. Finally, by combining our improved IBS and any existing 2-level Hierarchical IBE (HIBE) with adaptive security and anonymity (e.g., LWE-based HIBE scheme [ABB10b]), we obtain the *first* lattice-based construction that achieves both privacy and new-proposed stronger authenticity in the random oracle model.

1.2 Technical Overview

Here we provide an overview of the technical approach to our IB-ME construction. We focus on showing our new and easy-understanding construction method to satisfy stronger security.

IB-ME from 2-level HIBE and IBS Intuitively, our generic construction approach can be separated into two steps. Our starting point is the similarity of the syntax of IB-ME and HIBE. According to this key observation, we could obtain an IB-ME scheme satisfying both correctness and privacy except authenticity. Then, we utilize an IBS scheme to generate witness that allows a sender to self-authenticate his identity, and combine the IBS with the construction from the first step, to obtain the final IB-ME scheme. Here we show a brief overview, the complete construction is given in section 4.

HIBE implies an imperfect IB-ME. Inspired by Chen *et al.* [CLWW22], we observe that a 2-level HIBE scheme already implies an IB-ME if taking authenticity aside for a while. Note that the main distinction between syntaxes of HIBE and IB-ME is that a receiver is allowed to assign sender in an IB-ME scheme. Thus, we allow decryptors to delegate key associated with $\mathsf{rcv} \mid \mathsf{snd}$ for any snd.

In more details, the IB-ME scheme could be constructed as follows:

- Setup: $(\mathsf{HIBE.mpk}, \mathsf{HIBE.msk}) \leftarrow \mathsf{HIBE.Setup}$, set $\mathsf{HIBE.mpk}$ and $\mathsf{HIBE.msk}$ to be mpk and msk, respectively.
- $\mathsf{SKGen}(\mathsf{msk}, \sigma)$: $\mathsf{ek}_\sigma := \sigma$.
- $\mathsf{RKGen}(\mathsf{msk}, \rho)$: $\mathsf{sk}_\rho \leftarrow \mathsf{HIBE.Keygen}(\mathsf{HIBE.msk}, \rho)$, set $\mathsf{dk}_\rho := \mathsf{sk}_\rho$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{ek}_\sigma, \mathsf{rcv}, m)$: $\mathsf{ct} := \mathsf{HIBE.Enc}(\mathsf{rcv} \mid \sigma, m)$.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{dk}_\rho, \mathsf{snd}, C)$:
  1. $\mathsf{sk}_{\rho|\mathsf{snd}} \leftarrow \mathsf{HIBE.Derive}(\mathsf{dk}_\rho, \rho \mid \mathsf{snd})$.
  2. m *or* $\perp \leftarrow \mathsf{HIBE.Dec}(\mathsf{sk}_{\rho|\mathsf{snd}}, \mathsf{ct})$.

It is clear that when both match conditions satisfy, receiver can generate the correct 2-level key to help to recover message. Although authenticity has been ignored for the moment, privacy issues have been already fixed out. As long as the condition that $(\mathsf{rcv} \neq \rho)$ doesn't hold, receiver(malicious or not) cannot learn anything but decryption failure itself.

So far, our construction approach looks quite similar to the idea of the variant construction of 2-level IBE in [CLWW22]. However, the authenticity in their construction is related to the unforgeability of signature scheme, while in this paper, we choose another different way.

Guarantee authenticity by sign-then-encrypt. To further overcome authenticity problem, sender has to deliver a witness to persuade legal receivers that the received ciphertext came from claimed source exactly. In our setting, the witness is just an identity-based signature for message rcv generated by sender. Unlike Chen *et al.* [CLWW22], authority gives out the identity-based signing capability to each sender rather than the signature for message id. Thus, authenticity naturally guaranteed by the unforgeability of IBS. However, merely adding identity-based signature as part of ciphertexts would break privacy of IB-ME, because owners of non-target $\mathsf{dk}_{\mathsf{id}}$ could also verify and learn identity information of sender. The solution is let sender also encrypt witness under 2-level public key $\mathsf{rcv} \mid \mathsf{snd}$, which implies that only target receiver can check authenticity by verifying the validity of signature. For those illegal receivers whom $\mathsf{id} \neq \mathsf{rcv}$, nothing is leaked. Furthermore, in order to avoid the case that the receiver reuses the witness to forge ciphertexts, we tweak the above signature to contain encrypted plaintext additionally.

Instantiated with shorter ciphertext. The proposed generic construction can be instantiated from 2-level anonymous with adaptively security HIBE (e.g., based on lattice assumptions [ABB10a, CHKP12, ABB10b, BL16] or SXDH [LP20b, LP19, LP20a]) and adaptively secure IBS from various assumptions. As the final ciphertext contains the encryption of signature, we improve an existing IBS [PW21] based on short interger solution (SIS) [Ajt96] to reduce the signature size, thus obtain a shorter ciphertext.

In an IBS scheme [Sha84], any authorized user can generate signature using secret signing key, and everyone can verify whether the signature is valid or not by public parameters and user's identity. Pan and Wagner [PW21] proposed a tightly adaptively secure IBS from lattices using a new method, the resulting signature size independent of message length. Informally, the first step is constructing an unforgeable IBS with unforgeability under non-adaptive chosen message attacks (UF-naCMA), and the second step is upgrading UF-naCMA construction into adaptively secure (UF-CMA) one by generic transformations using tools like chameleon hash functions.

In our work, we will show a simpler signing algorithm and the length of signature can reduce by $n \cdot (\lceil \log q \rceil)^2$ bits. Intuitively, the signature in [PW21] is generated by firstly computing a matrix $\mathbf{H} := \mathsf{H}(m)$ by hashing the message and then sampling a pre-image vector $\mathbf{z}$ such that $[\mathbf{F}_{\mathsf{id}} | \mathbf{H}] \cdot \mathbf{z} = \mathbf{0}$. The signer id is given a trapdoor for identity-matrix $\mathbf{F}_{\mathsf{id}}$ as signing secret key to performing $\mathsf{SampleLeft}$ algorithm. Instead of encoding message at the 'left' pre-image position, we set the hashed message being the 'right' image, such that the signature

$\mathbf{z}'$ maps the $\mathbf{F}_{\mathsf{id}}$ to $\mathbf{h} := \mathsf{H}'(m)$. In such a case, the size of signatures is reduced from the column length of $[\mathbf{F}_{\mathsf{id}}|\mathbf{H}]$ to $\mathbf{F}_{\mathsf{id}}$. The resulting IBS will be further used to construct the IB-ME scheme.

Scheme /Techniques	**Privacy** CPA/CCA	**Authenticity** Stronger	**Assumptions**
[AFNV21]/ IBE[BF01]	CPA	×	BDH
[FGRV21] / Anon-IBE +NIZK+ReExt	CPA	×	q-ABDHE
[CLWW22]/ Anon-IBE	CPA	×	SXDH
[BL24]/ Anon-IBE +IBS+ReExt+Ext	CPA	✓	LWE+SIS
[CHHS23]/ CCA Anon-IBE +IBS+ReExt	CCA	✓	LWE
[LLC24]/ CCA Anon-IBE	CCA	×	SXDH
[CBDCF24]/ Anon-IBE +ReExt+HS	CPA	×	LWE+SIS
Ours/ CPA Anon-HIBE+IBS	CPA	✓	LWE+SIS
Ours/ CCA Anon-HIBE+IBS	CCA	✓	LWE+SIS

Table 1. Comparison with other schemes of IB-ME. ((Re)Ext stands for (reusable) randomness extractors. Anon-IBE and Anon-HIBE is short for anonymous IBE and anonymous HIBE, respectively. HS stands for homomorphic signature scheme.)

Scheme	[BL24]	[CHHS23]	Ours
Assumptions	$\mathsf{LWE}_{q,n,m,\mathcal{X}}$, $\mathsf{SIS}_{n',m',q,\beta}$	$\mathsf{LWE}_{q,n,m,\mathcal{X}}$, $\mathsf{SIS}_{n',m',q,\beta}$	$\mathsf{LWE}_{q,n,m,\mathcal{X}}$, $\mathsf{SIS}_{n',m',q,\beta}$
Instantiations	Anon-IBE[ABB10a], IBS(Section 5), ReExt[DKL09], Ext[Kra10]	Anon-IBE[ABB10a], IBS(Section 5), ReExt[DKL09],Ext[Kra10]	Anon-HIBE[ABB10b], IBS(Section 5)
$\lvert\mathsf{mpk}\rvert$	$((l+2)nm+n)\delta$ $+n'm'\delta$	$((l+2)nm+n)\delta$ $+n'm'\delta$	$n(m+1)\delta$ $+n'm'\delta$
$\lvert\mathsf{ek}\rvert$	$nm\delta^2+\omega(\log\lambda)$	$nm\delta^2+\omega(\log\lambda)$	$nm\delta^2+\omega(\log\lambda)$
$\lvert\mathsf{dk}\rvert$	$2m\delta$	$2m\delta$	$m^2\delta$
$\lvert\mathsf{ct}\rvert$	$(2m+l+1)\delta+$ $(m'+n'\delta)\delta+4\omega(\log\lambda)$	$2m\delta+m'\delta^2+$ $n'\delta^3+2\omega(\log\lambda)$	$m\delta+m'\delta^2+$ $n'\delta^3+2\omega(\log\lambda)$

Table 2. Comparison with other generic constructions of IB-ME satisfying the equivalent security level. All sizes are in bits, where δ denotes the size of an element in $\mathbb{Z}_q$.

1.3 Related Work

Discussions. Among all the existing IB-ME constructions, our work is the first to identify the potential limitations of the original authenticity definition and propose a stronger authenticity definition, as well as provide a generic construction of IB-ME based on an HIBE and an IBS scheme. Regarding privacy, although we proved CPA-privacy in this work, by applying the FO transformation, our construction can still achieve CCA security. We present a comparison of our IB-ME construction with other schemes in Table 1.

We also compare the efficiency of our scheme with other generic constructions [BL24, CHHS23] satisfying the same CPA-privacy and the stronger authenticity security in Table 2. Here, we focus on instantiating the constructions with the plain LWE and SIS based schemes. Especially, all used IBS schemes are the same construction that obtained by applying the generic transformation proposed in [PW21] on our improved $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ (Section 5). When based on the $\mathsf{LWE}_{q,n,m,\mathcal{X}}$ and $\mathsf{SIS}_{n',m',q,\beta}$ hardness assumptions of equivalent security level, the encryption key sizes of these constructions are the same, while our master public key and ciphertext sizes are both smaller than the other two constructions.

Authenticated identity-based encryption. Authenticated encryption (AE) [Zhe97] in the identity-based setting, namely identity-based signcryption [Mal02, Boy03, BLMQ05], enables intended receivers to decrypt and guarantees the authenticity that the underlying message is indeed from the claimed sender. However, the receivers in the identity-based signcryption scheme usually need to first recover the purported identity (besides the signature and the message) and then verify it. In an IB-ME scheme, a receiver just takes ciphertexts, its decryption key and an additional selected identity of sender as input, and finally gets messages only when matches happen. The whole decryption procedure implicitly contains the authentication to the message source and the message itself. Also the key generation mechanisms are different. There is only one KeyGen algorithm for users to encrypt or decrypt, while the authorities in IB-ME schemes will generate encryption keys and decryption keys, respectively.

2 Preliminaries

2.1 Notations

We denote the real numbers, the integers and the natural numbers by $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$, respectively. Let $\mathbb{Z}_q$ be $\mathbb{Z}/(q\mathbb{Z})$. For an integer $m \neq 0$, let $[m]$ be $\{1, \cdots, m\}$. We write vectors and matrices in bold letters (e.g., $\mathbf{z}$ or $\mathbf{Z}$). The Euclidean norm, or l_2 norm, of a vector is written as $\|\mathbf{z}\|$. We denote uniformly sampling as $x \xleftarrow{\$} D$. The Euclidean norm and spectral norm of a matrix $\mathbf{Z}$ is denoted by $\|\mathbf{Z}\|$ and $s_1(\mathbf{Z})$, respectively. The "p.p.t." stands for probabilistic polynomial-time. We make use of standard asymptotic notation for positive functions such as ω and O.

Suppose X and Y are probability distributions on a countable domain D, then the statistical distance is defined as $\Delta(X,Y) = \frac{1}{2}\sum_{d\in D} \mid X(d) - Y(d) \mid$. The distributions X and Y are said *statistically close* if $\Delta(X,Y)$ is negligible in n, denoted by $X \overset{s}{\approx} Y$. If $\mid \Pr[\mathcal{A}(1^n, \mathrm{X}) = 1] - \Pr[\mathcal{A}(1^n, \mathrm{Y}) = 1] \mid$ is negligible in n for every probabilistic poly-time algorithm $\mathcal{A}$, we say that distributions X and Y are *computationally indistinguishable*, and denote it by $X \overset{c}{\approx} Y$.

2.2 Lattices Background

A n-dimensional lattice Λ, being a discrete additive subgroup of $\mathbb{R}^n$, is the set $\mathcal{L}(\mathbf{b}_1, \cdots, \mathbf{b}_n) = \{\mathbf{Bz} = \sum_{i\in[n]} z_i \cdot \mathbf{b}_i \mid z_i \in \mathbb{Z}\}$ of all integral combinations of some n linearly independent vectors $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subset \mathbb{R}^n$. The sequence of vectors $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ is called a lattice basis.

The being used q-ary integer lattices in lattice-based cryptosystems are defined by a matrix over $\mathbb{Z}_q$. Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be arbitrary matrix for some positive integers n, m, q, define the full-rank m-dimensional q-ary lattices as follows

$$\Lambda(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \mid \exists\ \mathbf{s} \in \mathbb{Z}_q^n,\ s.t.\ \mathbf{A}^t\mathbf{s} = \mathbf{z} \mod q\}$$
$$\Lambda^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = \mathbf{0} \mod q\}.$$

For a fixed $\mathbf{u} \in \mathbb{Z}_q^n$, define a coset of $\Lambda^\perp$ as:

$$\Lambda_{\mathbf{u}}^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = \mathbf{u} \mod q\}.$$

Lemma 2.1 ([GPV08]) *Let n and q be positive integers with q prime, and let $m \geq 2n\log q$. Then for all but a negligible fraction of all $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and for any $s \geq \omega(\sqrt{\log m})$, the distribution of the syndrome $\mathbf{u} = \mathbf{A}\mathbf{e} \mod q$ is statistically close to uniform over $\mathbb{Z}_q^n$, where $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,s}$.*

Furthermore, fix $\mathbf{u} \leftarrow \mathbb{Z}_q^n$ and let $\mathbf{x} \leftarrow \mathbb{Z}^m$ be an arbitrary solution to $\mathbf{A}\mathbf{x} = \mathbf{u} \mod q$. Then the conditional distribution of $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,s}$ given $\mathbf{A}\mathbf{e} = \mathbf{u} \mod q$ is exactly $\mathcal{D}_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),s}$.

The lower bound of the min-entropy of a discrete Gaussian distribution is given in the following lemma.

Lemma 2.2 ([GPV08]) *Let n, m and q be positive integers with $m \geq 2n\log q$. For all but at most q^{-n} fraction of all $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, any vector $\mathbf{u} \in \mathbb{Z}_q^n$ and for any $s \geq \omega(\sqrt{\log m})$, we have $H_\infty(\mathcal{D}_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),s}) \geq m - 1$.*

The following lemma is the bound for spectral norm of random matrices from the non-asymptotic theory.

Lemma 2.3 ([MP12]) *Let $\mathbf{X} \in \mathbb{R}^{n\times m}$ be a δ-subgaussian random matrix with parameter s. There exists a universal constant C, which is very close to $1/\sqrt{2\pi}$ such that for any $t \geq 0$, we have $s_1(\mathbf{X}) \leq C \cdot s \cdot (\sqrt{m} + \sqrt{n} + t)$ except with probability at most $2\exp(\delta)\exp(-\pi t^2)$.*

Trapdoors and Sampling Algorithms. Here we recall some lattices trapdoors and Gaussian sampling algorithms.

The gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ is a primitive matrix defined by gadget vector $\mathbf{g}$ as $\mathbf{G} := \mathbf{I}_n \otimes \mathbf{g}^t \in \mathbb{Z}_q^{n\times nk}$. We usually consider gadget vector $\mathbf{g}^t := [1\ 2\ 4\ \cdots\ 2^{k-1}] \in \mathbb{Z}_q^{1\times k}$, where $k = \lceil \log_2 q \rceil$. Let n, m, q be any integers with $m \geq n\lceil \log q \rceil$. A trapdoor for a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is a matrix $\mathbf{R} \in \mathbb{Z}_q^{(m-n\lceil \log q \rceil)\times n\lceil \log q \rceil}$ such that $\mathbf{A} \cdot \begin{bmatrix} -\mathbf{R} \\ \mathbf{I}_{n\lceil \log q \rceil} \end{bmatrix} = \mathbf{G}$. In particular, matrix $\mathbf{R}$ consists of short integer vectors having "quality" s_1, where smaller is better. Usually, we can use the following $\mathsf{TrapGen}$ algorithm to compute a pair of matrix $\mathbf{A}$ and its trapdoor matrix $\mathbf{R}$ with bounded $s_1(\mathbf{R})$.

Lemma 2.4 ([MP12]) *Let n, m, k, q be any integers with $q \geq 2$, $n \geq 1$, $m = nk$ and $k = \lceil \log_2 q \rceil$, then there exists a primitive matrix $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$, and the lattice $\Lambda^\perp(\mathbf{G})$ has a public basis $\mathbf{S} \in \mathbb{Z}^{m\times m}$ with $\|\widetilde{\mathbf{S}}\| \leq \sqrt{5}$ and $\|\mathbf{S}\| \leq \max\{\sqrt{5}, \sqrt{k}\}$.*

Lemma 2.5 (TrapGen [MP12]) *There exists a probabilistic polynomial-time algorithm $\mathsf{TrapGen}(1^n, 1^m, s, q)$ that, given any integers $n \geq 1$, $q \geq 2$, $s > 0$ and sufficiently large $m = O(n\log q)$, it will output $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ being as a parity-check matrix and a trapdoor $\mathbf{R} \in \mathbb{Z}^{(m-w)\times w}$ where $w := n\lceil \log_2 q \rceil$, such that the distribution of $\mathbf{A}$ is statistically close to uniform, and the entries of $\mathbf{R}$ are sampled from $\mathcal{D}_{\mathbb{Z},s}$ holding that $s_1(\mathbf{R}) = s \cdot O(\sqrt{m-w} + \sqrt{w})$.*

Lemma 2.6 (SamplePre [MP12, PPS21]) *Let $q \geq 2$, $\mathbf{R}$ be the trapdoor for matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, for any $\mathbf{u} \in \mathbb{Z}_q^n$ and $s \geq \sqrt{s_1(\mathbf{R})^2 + 1} \cdot \|\widetilde{\mathbf{S}}\| \cdot \omega(\sqrt{\log n})$, there is a p.p.t. algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{R}, \mathbf{u}, s)$ that samples preimages from a distribution being statistically close to $\mathcal{D}_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),s}$.*

In particular, the output distribution of the following two experiments are with $\mathsf{negl}(n)$ statistical distance:

- *choose $\mathbf{z} \leftarrow \mathcal{D}_{\mathbb{Z},s}^m$, and output $(\mathbf{z}, \mathbf{u} = \mathbf{A} \cdot \mathbf{z} \in \mathbb{Z}_q^n)$.*
- *choose $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{z} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{R}, \mathbf{u}, s)$, and output $(\mathbf{e}, \mathbf{u})$.*

Lemma 2.7 (DelTrap [MP12]) *Let $q \geq 2$, for any pair of public matrix and its trapdoor $(\mathbf{A} \in \mathbb{Z}^{n\times m}, \mathbf{R})$ generated from TrapGen algorithm in Lemma 2.5, any extension matrix $\mathbf{A}_1 \in \mathbb{Z}^{n\times w}$, and $m' \geq m + w$, $s' \geq \omega(\sqrt{\log m})$, there exists a p.p.t. algorithm $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \mid \mathbf{A}_1], \mathbf{R}, s')$ that outputs a trapdoor $\mathbf{R}'$ for $\mathbf{A}'$ and $s_1(\mathbf{R}') \leq s' \cdot O(\sqrt{m} + \sqrt{w})$ with overwhelming probability. Usually, s' is required to be sufficiently large relative to $s_1(\mathbf{R})$ when implementing algorithm.*

Hardness Assumption.

Definition 1 (Short Integer Solution (SIS) [Ajt96, MR04]) *The short integer solution problem $SIS_{n,m,q,\beta}$ (in the l_2 norm) is defined as follows: Given an integer q, m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $\|\mathbf{z}\| \leq \beta$ such that $\mathbf{Az} = \sum_i \mathbf{a}_i \cdot z_i = \mathbf{0} \mod q$.*

Definition 2 (Learning with errors(LWE) [Reg05]) *Let $n \geq 1$ and $q \geq 2$ be integers, and let $\mathcal{X}$ be a probability distribution on $\mathbb{Z}_q$. For $\mathbf{s} \in \mathbb{Z}_q^n$, let $A_{\mathbf{s},\mathcal{X}}$ be the probability distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \in \mathbb{Z}_q$ according to $\mathcal{X}$ and outputting $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s}\rangle + e)$.*

The decision $\mathsf{LWE}_{q,n,\mathcal{X},m}$ problem is: given m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where each sample is either from $A_{\mathbf{s},\mathcal{X}}$ for uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$ (fixed for all samples), or uniformly random in $\mathbb{Z}_q^n \times \mathbb{Z}_q$, distinguish which is the case (with non-negligible advantage).

2.3 Hierarchical Identity-based Encryption

We now recall the definition of (anonymous) 2-level hierarchical identity-based encryption (HIBE) as we require it as building block to constructing IB-ME. Since we focus on 2-level case, we consider the encryption and decryption algorithms only for level-2 users. Such modifications apply to all existing HIBE schemes.

The following version of security game which implies a stronger privacy property called *indistinguishable from random* is adapted from [ABB10a, ABB10b]. Intuitively, the adversary is asked to distinguish the challenge ciphertext and a random element in the ciphertext space. Thus, as pointed by Agrawal *et al.*, such a definition captures both semantic security and recipient anonymity.

Definition 3 (2-level Hierarchical Identity-based Encryption [Gen06, ABB10a, ABB10b, KMT19]) *A 2-level HIBE scheme over an identity space $\mathcal{ID}$, a message space $\mathcal{M}$ is a tuple of algorithms $\Pi_{\mathsf{HIBE}} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Derive}, \mathsf{Enc}, \mathsf{Dec})$ with the following properties:*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$*: On input the security parameter λ, it outputs the master public key* mpk *and the master secret key* msk*.*
- $\mathsf{Extract}(\mathsf{msk}, \mathsf{id}_1) \to \mathsf{sk}_{\mathsf{id}_1}$*: On input the master secret key* msk *and a first-level identity* $\mathsf{id}_1 \in \mathcal{ID}$*, it outputs a secret key* $\mathsf{sk}_{\mathsf{id}_1}$*.*
- $\mathsf{Derive}(\mathsf{sk}_{\mathsf{id}_1}, \mathsf{id}_2) \to \mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2}$*: On input a secret key* $\mathsf{sk}_{\mathsf{id}_1}$ *and a second-level identity* $\mathsf{id}_2 \in \mathcal{ID}$*, it outputs a secret key* $\mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2}$*.*
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id} = (\mathsf{id}_1 \mid \mathsf{id}_2), m) \to \mathsf{ct}$*: On input the master public key* mpk*, a level-2 user's identity* $\mathsf{id} = (\mathsf{id}_1 \mid \mathsf{id}_2) \in (\mathcal{ID}|\mathcal{ID})$ *and a message $m \in \mathcal{M}$, it outputs a ciphertext* ct*.*
- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2}, \mathsf{ct}) \to m/\perp$*: On input a secret decryption key* $\mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2}$ *(for a level-2 user with* $\mathsf{id} = (\mathsf{id}_1 \mid \mathsf{id}_2)$*) and a ciphertext* ct*, it outputs either a message $m \in \mathcal{M}$ or a special symbol $\perp$.*

A 2-level HIBE scheme satisfies properties as follows:

Correctness. For all identities $\mathsf{id} = (\mathsf{id}_1 \mid \mathsf{id}_2) \in (\mathcal{ID}|\mathcal{ID})$, and all messages $m \in \mathcal{M}$, if set $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_{\mathsf{id}_1} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id}_1)$, $\mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2} \leftarrow \mathsf{Derive}(\mathsf{sk}_{\mathsf{id}_1}, \mathsf{id}_2)$, $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id} = (\mathsf{id}_1 \mid \mathsf{id}_2), m)$, then

$$\Pr[\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}_1|\mathsf{id}_2}, \mathsf{ct}) = \mathrm{m}] \geq 1 - \mathsf{negl}(\lambda)$$

Security. We define chosen-plaintext security for HIBE systems under chosen identity attacks via the following game $\textbf{ANON-IND-ID-CPA}^{\mathcal{A}}_{\mathsf{HIBE}}(\lambda)$.

- **Setup**: The challenger is given it the security parameter λ and then runs the Setup algorithm. Then, it sends the resulting master public key mpk to the adversary.
- **Pre-challenge querying Phase**:
  1. Level-1 secret key query
     The Adversary issues queries on identities $\mathsf{id}_1^1, \mathsf{id}_1^2, \cdots$, where each $\mathsf{id}_1^i \in \mathcal{ID}$. For each query, the challenger executes $\mathsf{sk}_{\mathsf{id}_1^i} \leftarrow \mathsf{Extract}\ (\mathsf{msk}, \mathsf{id}_1^i)$ and returns $\mathsf{sk}_{\mathsf{id}_1^i}$ to the adversary.
  2. Level-2 secret key query
     The Adversary issues queries on identities $(\mathsf{id}_1^1 \mid \mathsf{id}_2^1), (\mathsf{id}_1^2 \mid \mathsf{id}_2^2), \cdots$, where each $(\mathsf{id}_1^j \mid \mathsf{id}_2^j) \in (\mathcal{ID}|\mathcal{ID})$. For each query the challenger executes $\mathsf{sk}_{\mathsf{id}_1^j} \leftarrow \mathsf{Extract}(\mathsf{msk}, \mathsf{id}_1^j)$ and $\mathsf{sk}_{\mathsf{id}_1^j|\mathsf{id}_2^j} \leftarrow \mathsf{Derive}(\mathsf{sk}_{\mathsf{id}_1^j}, \mathsf{id}_2^j)$. Then the challenger returns $\mathsf{sk}_{\mathsf{id}_1^j|\mathsf{id}_2^j}$ to the adversary.
- **Challenge Phase**:
  Once the adversary decides that pre-challenge querying phase is over, it submits an identity $\mathsf{id}^* = (\mathsf{id}_1^* \mid \mathsf{id}_2^*) \in (\mathcal{ID}|\mathcal{ID})$ and a message $m \in \mathcal{M}$. The challenge identity id^* and its prefix must not have appeared in any secret key query (both level-1 and level-2) in pre-challenge querying phase. The challenger picks $b \xleftarrow{\$} \{0,1\}$ and a random ciphertext ct from ciphertext space. If $b = 0$, it sets the challenge ciphertext to $\mathsf{ct}^* := \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^* = (\mathsf{id}_1^* \mid \mathsf{id}_2^*), m)$. If $b = 1$, it sets $\mathsf{ct}^* := \mathsf{ct}$ and then sends ct^* to the adversary.
- **Post-challenge querying phase**:
  The adversary queries for additional level-1 and level-2 keys, and the challenger responds as in the pre-challenge querying phase, except that the adversary should not request a sk for id^* or for the prefix of id^*.
- **Guess**: Adversary submits a guess bit b' and wins when b' equals to b.

Such an adversary is said to be an ANON-IND-ID-CPA adversary.

Definition 4 (ANON-IND-ID-CPA secure 2-level HIBE) *A 2-level HIBE is* ANON-IND-ID-CPA *secure if for all p.p.t. adversaries* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\text{ANON-IND-ID-CPA}}_{\Pi,\mathcal{A}}(\lambda) :=\mid \Pr[\mathrm{b} = \mathrm{b}'] - \tfrac{1}{2} \mid \leq \mathsf{negl}(\lambda).$$

2.4 Identity-based Signature

Definition 5 (Identity-based Signature [Sha84, PW21]) *An IBS scheme is specified by four algorithms* $\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sign}, \mathsf{Ver})$ *with polynomial running time. The first three may be randomized while the last is deterministic.*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$*: The trusted authority takes security parameters as input and run the setup algorithm to obtain a master public key* mpk *and a master secret key* msk*. Note that* mpk *implicitly specified an identity space* $\mathcal{ID}$ *and a message space* $\mathcal{M}$*.*
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$*: On input* msk *and an identity* id*, it outputs a secret signing key* $\mathsf{sk}_{\mathsf{id}}$ *for* $\mathsf{id} \in \mathcal{ID}$*.*
- $\mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, m) \to \sigma$*: On input secret signing key* $\mathsf{sk}_{\mathsf{id}}$ *and message* $m \in \mathcal{M}$*, user with identity* id *will obtain a signature* σ*, which is the output of signing algorithm.*
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, m, \sigma) \to 0/1$*: On input a master public key* mpk*, a user identity* id*, a message* m *and a signature* σ*, verifying algorithm returns 1 if signature is valid for* id *and* m*, otherwise returns 0.*

Correctness. For every $(\mathsf{mpk}, \mathsf{msk})$ generated as above, $m \in \mathcal{M}$, $\mathsf{id} \in \mathcal{ID}$, it holds that:

$$\Pr[\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathrm{m}, \sigma) = 1 \mid \mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{msk},\ \mathsf{id}), \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, \mathrm{m})] = 1 - \mathsf{negl}(\lambda)$$

Security. We define the unforgeability for IBS systems under chosen message attacks via the following game $\mathbf{UF\text{-}CMA}^{\mathcal{A}}_{\mathsf{IBS}}(\lambda)$. Oracles $\mathsf{Key}, \mathsf{Sig}$ are implemented by $\mathsf{KeyExt}(\cdot)$, $\mathsf{Sign}(\cdot)$, respectively. H is a random oracle. Lists $\mathcal{L}_{id}$ and $\mathcal{L}_m$ are updated after each query.

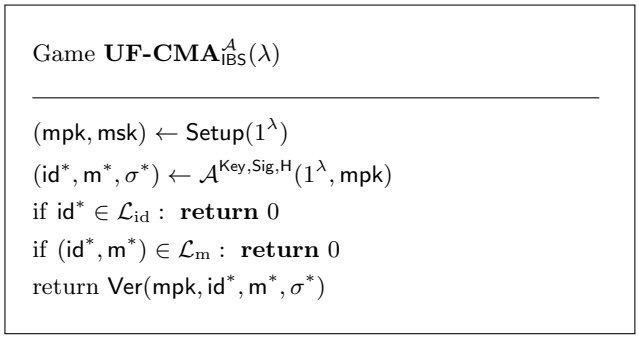

Fig. 1. Game $\mathbf{UF\text{-}CMA}^{\mathcal{A}}_{\mathsf{IBS}}(\lambda)$

Definition 6 (UF-(na)CMA) *Let* $\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sign}, \mathsf{Ver})$ *be an IBS scheme. We say that the IBS scheme is* UF-CMA *secure, if for every p.p.t algorithm* $\mathcal{A}$*, the following advantage is negligible in* λ*:*

$$\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathcal{A},\mathsf{IBS}} := \Pr[\mathbf{UF\text{-}CMA}^{\mathcal{A}}_{\mathsf{IBS}}(\lambda)=1]$$

UF-naCMA security is defined similarly, but with additional restriction that the adversary should submit all the signing key queries $\mathcal{L}_{id}$ *and signature queries* $\mathcal{L}_m$ *before setup phase, where the list* $\mathcal{L}_{id}$ *consists of all the identities that the adversary asking for corresponding signing keys and the list* $\mathcal{L}_m$ *consists of all the identity and message pairs that the adversary asking for signatures.*

We define an IBS scheme as UF-naCMA *secure, if for every p.p.t algorithm* $\mathcal{A}$*, the following advantage is negligible in* λ*:*

$$\mathsf{Adv}^{\mathsf{UF\text{-}naCMA}}_{\mathcal{A},\mathsf{IBS}} := \Pr[\mathbf{UF\text{-}naCMA}^{\mathcal{A}}_{\mathsf{IBS}}(\lambda)=1]$$

3 Improved Formal Definitions for Identity-based Matchmaking Encryption

In this section, we will firstly recall the original syntax and the formal definitions of correctness and privacy property for IB-ME. Then we will propose the improved security definition of authenticity to match general and practical security requirements. As we will discuss in detail later, our security definition of authenticity is able to capture more real-world attacks including "forging-to-itself" and tamper forgeries than previous ones [AFNV21, FGRV21, CLWW22].

Definition 7 (Identity-based Matchmaking Encryption [AFNV21]) *A IB-ME scheme is a tuple of polynomial-time algorithms* $\mathsf{IB\text{-}ME} = (\mathsf{Setup}, \mathsf{SKGen}, \mathsf{RKGen}, \mathsf{Enc}, \mathsf{Dec})$*. We define it as follows:*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$*: Upon input the security parameter* 1^λ*, the setup algorithm outputs the master public key* mpk *and the master secret key* msk*. Denote the identity space by* $\mathcal{ID}$*, the message space by* $\mathcal{M}$*, and the ciphertext space by* $\mathcal{C}$*. We implicitly assume that all other algorithms take* mpk *as input.*
- $\mathsf{SKGen}(\mathsf{msk}, \phi) \to \mathsf{ek}_\phi$*: On input* msk*, and an identity* ϕ*, the key generator outputs a secret encryption key* ek_ϕ *for identity* ϕ*.*
- $\mathsf{RKGen}(\mathsf{msk}, \rho) \to \mathsf{dk}_\rho$*: On input* msk *and an identity* ρ*, the key generator outputs a secret decryption key* dk_ρ *for identity* ρ*.*

- $\mathsf{Enc}(\mathsf{ek}_\phi, \mathsf{rcv}, m) \to c$: *On input a secret encryption key* ek_ϕ *for identity* ϕ*, a target receiver's identity* rcv*, and a message* $m \in \mathcal{M}$*, it produces a ciphertext* c *linked to both* ϕ *and* rcv*.*
- $\mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c) \to m/\perp$: *On input a secret decryption key* dk_ρ *for identity* ρ*, a target sender's identity* snd *and a ciphertext* c*, the decryption algorithm outputs either a message* m *or* $\perp$*.*

Correctness. Intuitively, the output of decryption algorithm for the ciphertext encrypted under encryption key for ϕ and target identity rcv using decryption key for ρ and target identity snd will be the original plaintext iff. the receiver's identity ρ matches the identity rcv chosen by the encryptor, and the identity ϕ of sender matches the identity snd selected by the decryptor in the meantime.

Definition 8 (Correctness of IB-ME) *For all identities* $\phi, \rho, \mathsf{rcv}, \mathsf{snd} \in \mathcal{ID}$ *such that* $\rho = \mathsf{rcv} \wedge \phi = \mathsf{snd}$*, and all messages* $m \in \mathcal{M}$*, if we set* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$*,* $\mathsf{ek}_\phi \leftarrow \mathsf{SKGen}(\mathsf{msk}, \phi)$*,* $\mathsf{dk}_\rho \leftarrow \mathsf{RKGen}(\mathsf{msk}, \rho)$*, then*

$$\Pr[\mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, \mathsf{Enc}(\mathsf{ek}_\phi, \mathsf{rcv}, \mathrm{m})) = \mathrm{m}] \geq 1 - \mathsf{negl}(\lambda)$$

Security Definitions. The security of an IB-ME scheme can be viewed as two properties, called *privacy* and *authenticity*.

$\mathrm{G}^{\mathsf{priv}}_{\Pi,\mathcal{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$

$(\mu_0, \mu_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \phi_0, \phi_1, \alpha) \leftarrow \mathcal{A}_1^{\mathsf{O}_S, \mathsf{O}_R}(1^\lambda, \mathsf{mpk})$

$b \xleftarrow{\$} \{0, 1\}$

$\mathsf{ek}_{\phi_b} \leftarrow \mathsf{SKGen}(\mathsf{msk}, \phi_b)$

$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{ek}_{\phi_b}, \mathsf{rcv}_b, \mu_b)$

$b' \leftarrow \mathcal{A}_2^{\mathsf{O}_S, \mathsf{O}_R}(1^\lambda, \mathsf{ct}, \alpha)$

If $(\mathrm{b}' = \mathrm{b})$ **return** 1

Else **return** 0

Fig. 2. $\mathrm{Game}^{\mathsf{priv}}_{\Pi,\mathcal{A}}(\lambda)$

Here, we firstly recall the original definition of privacy for IB-ME. We focus on the privacy in the case of mismatch, which means that on condition that the malicious receiver does not own the decryptable key, he cannot learn anything about message and the information about the sender's identity. Here we do not consider the condition of match is due to the reason that match cases obviously imply $\rho = \mathsf{rcv} \wedge \phi = \mathsf{snd}$. The privacy game $\mathrm{G}^{\mathsf{priv}}_{\Pi,\mathcal{A}}$ is showed in Fig. 2, where the role of α is a state value.

Definition 9 *(Privacy of IB-ME). An IB-ME* Π *is said to satisfy privacy if for all admissible p.p.t algorithms* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{A},\mathsf{IB\text{-}ME}} \coloneqq |\Pr[\mathrm{G}^{\mathsf{priv}}_{\Pi,\mathcal{A}} = 1] - \tfrac{1}{2}| \leq \mathsf{negl}(\lambda).$$

Oracles $\mathsf{O}_S, \mathsf{O}_R$ *are implemented by* $\mathsf{SKGen}(\cdot)$ *and* $\mathsf{RKGen}(\cdot)$*, respectively. An adversary* $\mathcal{A}$ *is admissible if for all decryption key queried identities* ρ*, it holds that* $\rho \neq \mathsf{rcv}_0 \wedge \rho \neq \mathsf{rcv}_1$*.*

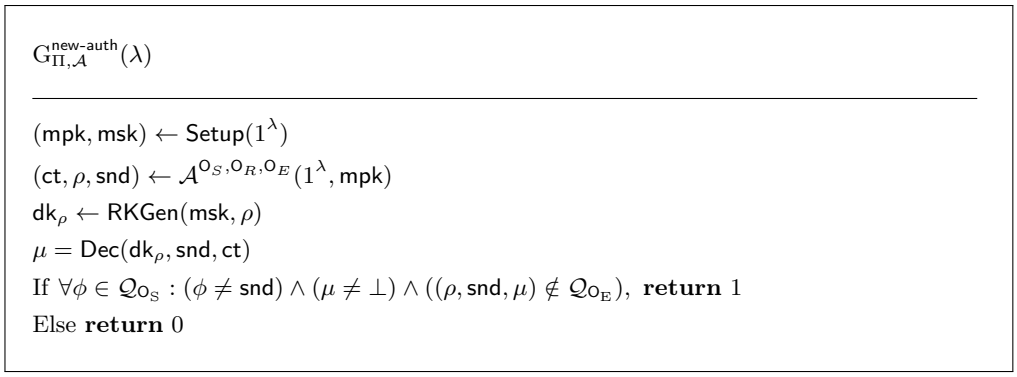

Fig. 3. $\text{Game}^{\text{new-auth}}_{\Pi,\mathcal{A}}(\lambda)$

We then provide our modified security definition of authenticity. Authenticity guarantees that adversary, without corresponding encryption keys, cannot produce ciphertexts embedding fake identities. We observe that the previous security definitions [AFNV21, FGRV21, CLWW22] fail to capture the possible forgeries like "forging-to-itself" or tamper forgeries. Hence, we modify the authenticity game to cancel the restrictions on the challenge receivers' identities and give adversaries access to encryption oracle. In other words, the improved game enables attackers to obtain ciphertexts with known plaintexts from chosen sources, also it is admissible for adversaries to submit forgeries of corrupted target receivers. The modified authenticity game is presented in Fig. 3.

Definition 10 *(Stronger Authenticity of IB-ME).An IB-ME* Π *is said to satisfy stronger authenticity if for all p.p.t algorithms* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\text{new-auth}}_{\mathcal{A},\text{IB-ME}} := |\Pr[G^{\text{new-auth}}_{\Pi,\mathcal{A}} = 1]| \leq \mathsf{negl}(\lambda).$$

Oracles $\mathsf{O}_S, \mathsf{O}_R, \mathsf{O}_E$ *are implemented by* $\mathsf{SKGen}(\cdot)$, $\mathsf{RKGen}(\cdot)$ *and* $\mathsf{Enc}(\cdot)$ *respectively.*

4 Generic Construction of IB-ME

In this section, we provide the details about our generic construction of IB-ME satisfying stronger security definitions. Namely, we show how to construct an IB-ME scheme by combining a 2-level HIBE scheme and an IBS scheme. We require that both underlying schemes to be adaptively secure, so that IB-ME achieving adaptive security.

4.1 IB-ME from 2-level HIBE and IBS

Construction 1 (Identity-based Matchmaking Encryption). *We write* $\mathcal{ID}$ *as an identity space and* $\mathcal{M}$ *as a message space. We also require the primitives as follows:*

- *Let* IBS *be an identity-based signature scheme with identity space* $\mathcal{ID}$*, message space* $\mathcal{ID}|\mathcal{M}$ *and signature space* $\mathcal{S}$*.*
- *Let* HIBE *be an anonymous 2-level HIBE schemes with identity space* $\mathcal{ID}|\mathcal{ID}$ *and message space* $\mathcal{M}|\mathcal{S}$*.*

We construct our IB-ME with identity space $\mathcal{ID}$ *and message space* $\mathcal{M}$ *as follows:*

- $\mathsf{Setup}(1^\lambda)$*: On input the security parameter* 1^λ*, it generates* $(\mathsf{HIBE.mpk}, \mathsf{HIBE.msk}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$*,* $(\mathsf{IBS.mpk}, \mathsf{IBS.msk}) \leftarrow \mathsf{IBS.Setup}(1^\lambda)$*, and outputs*

$$\mathsf{mpk} = (\mathsf{HIBE.mpk}, \mathsf{IBS.mpk}) \text{ and } \mathsf{msk} = (\mathsf{HIBE.msk}, \mathsf{IBS.msk}).$$

- $\mathsf{SKGen}(\mathsf{msk}, \phi)$*: On input the master secret key* msk *and an identity* ϕ*, it computes signing key* $\mathsf{IBS.sk}_\phi \leftarrow \mathsf{IBS.KeyExt}\ (\mathsf{IBS.msk}, \phi)$*. It outputs* $\mathsf{ek}_\phi \leftarrow \mathsf{IBS.sk}_\phi$*.*
- $\mathsf{RKGen}(\mathsf{msk}, \rho)$*: On input* msk *and an identity* ρ*, the receiver key-generation algorithm generates* $\mathsf{HIBE.sk}_\rho \leftarrow \mathsf{HIBE.Extract}(\mathsf{HIBE.msk}, \rho)$*. Then, it returns* $\mathsf{dk}_\rho \leftarrow \mathsf{HIBE.sk}_\rho$*.*
- $\mathsf{Enc}(\mathsf{ek}_\phi, \mathsf{rcv}, \mu)$*: On input* mpk*, secret encryption key* ek_ϕ*, target identity* rcv *and message* $\mu \in \mathcal{M}$*, the encryption algorithm firstly generate identity-based signature* $\boldsymbol{t} \leftarrow \mathsf{IBS.Sign}(\mathsf{IBS.}\ \mathsf{sk}_\phi, \mathsf{rcv} \mid \mu)$*. It then computes ciphertext under* HIBE *public key* $\mathsf{rcv} \mid \phi$ *to obtain*

$$\mathsf{HIBE.ct}^{\boldsymbol{t}|\mu} \leftarrow \mathsf{HIBE.Enc}(\mathsf{HIBE.mpk}, \mathsf{rcv} \mid \phi, \boldsymbol{t}|\mu),$$

  where rcv *and* ϕ *refers to the first and second level identity for* HIBE *scheme, respectively. Finally, it outputs ciphertext* $\mathsf{ct} = \mathsf{HIBE.ct}^{\boldsymbol{t}|\mu}$*.*
- $\mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, \mathsf{ct})$*: On input a secret decryption key* dk_ρ*, a ciphertext* ct *and a selected sender's identity* snd*, the decryption algorithm first delegates key* $\mathsf{dk}_{\rho|\mathsf{snd}} \leftarrow \mathsf{HIBE.Derive}(\mathsf{dk}_\rho, \rho \mid \mathsf{snd})$*, and recovers* $\boldsymbol{t}|\mu \leftarrow \mathsf{HIBE.Dec}(\mathsf{dk}_{\rho|\mathsf{snd}}, \mathsf{ct})$*. Then it verifies the validity of signature* $(0/1) \leftarrow \mathsf{IBS.Verify}(\mathsf{IBS.mpk}, \boldsymbol{t}, \rho \mid \mu)$*. If signature is not valid, it aborts and returns* $\perp$*. Otherwise, it outputs* μ*.*

Theorem 4.1 (Correctness) *If underlying* HIBE *and* IBS *are both correct, then* $\mathsf{IB\text{-}ME}$ *from Construction 1 is correct.*

Proof. Take a message $m \in \mathcal{M}$, a target receiver's identity $\mathsf{rcv} \in \mathcal{ID}$, and a sender's identity $\phi \in \mathcal{ID}$. Take an identity of receiver $\rho \in \mathcal{ID}$, and an identity of target sender $\mathsf{snd} \in \mathcal{ID}$. Take $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{ek}_\phi \leftarrow \mathsf{SKGen}(\mathsf{msk}, \phi)$, $\mathsf{dk}_\rho \leftarrow \mathsf{RKGen}(\mathsf{msk}, \rho)$, $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{ek}_\phi, \mathsf{rcv}, \mu)$.

In this case, $\mathsf{mpk} = (\mathsf{HIBE.mpk},\ \mathsf{IBS.mpk}$ and $\mathsf{msk} = (\mathsf{HIBE.msk},\ \mathsf{IBS.msk})$, ek_ϕ is the signing key output by $\mathsf{IBS.KeyExt}(\mathsf{IBS.msk}, \phi)$, dk_ρ is the decryption key obtained by $\mathsf{HIBE.sk}_\rho \leftarrow \mathsf{HIBE.Extract}(\mathsf{HIBE.msk}, \rho)$, and $\mathsf{ct} = \mathsf{HIBE.ct}^{\mathbf{t}|\mu}$ is output by $\mathsf{HIBE.ct}^{\mathbf{t}|\mu} \leftarrow \mathsf{HIBE.Enc}(\mathsf{HIBE.mpk}, \mathsf{rcv} \mid \phi, \mathbf{t}|\mu)$, where $\mathbf{t}$ is the identity-based signature corresponding to ϕ of message $\mathsf{rcv}|\mu$. It is obvious that when $\rho = \mathsf{rcv} \wedge \phi = \mathsf{snd}$, $\mathsf{rcv} \mid \phi = \rho \mid \mathsf{snd}$, the receiver with identity ρ can generate decryption keys for $\rho \mid \mathsf{snd}$ using its key dk_ρ and then recover signature $\mathbf{t}$ and message μ. Moreover, signature $\mathbf{t}$ is signed by sender with identity ϕ for $\mathsf{rcv} \mid \mu$, we have $1 \leftarrow \mathsf{IBS.Verify}(\mathsf{IBS.pk}, \mathbf{t}, \rho \mid \mu)$ with high probability. Thus, the correctness of $\mathsf{IB\text{-}ME}$ follows by the correctness of underlying HIBE and IBS. □

□

4.2 The Security Analysis

We provide the formal security analysis of the identity-based matchmaking encryption scheme from Construction 1.

Theorem 4.2 (Security) *Let* HIBE*,* IBS *be as above. Suppose that* Π_{HIBE} *is* $\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}$ *secure (Def.4),* IBS *is* $\mathsf{UF\text{-}CMA}$ *secure (Def.6), then* $\Pi_{\mathsf{IB\text{-}ME}}$ *from Construction 1 is secure.*

Proof. We prove privacy and authenticity respectively.

Lemma 4.1 *If* Π_{HIBE} *is* $\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}$ *secure (Def.4), then* $\Pi_{\mathsf{IB\text{-}ME}}$ *from Construction 1 satisfies privacy(Def.9). In particular, for every p.p.t. algorithm* $\mathcal{A}$ *there is a p.p.t. algorithm* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{A},\mathsf{IB\text{-}ME}}(\lambda) \leq\ 2\mathsf{Adv}^{\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{B},\mathsf{HIBE}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. We proceed with the following hybrid games:

- Hyb_0: This is experiment $\mathrm{G}^{\mathsf{priv}}_{\Pi,\mathcal{A}}(\lambda)$ for case that $b = 0$. For challenge query $(\mu_0, \mu_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \phi_0, \phi_1)$, the challenger will return the ciphertext $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{ek}_{\phi_0}, \mathsf{rcv}_0, \mu_0)$, where $\mathsf{ek}_{\phi_0} \leftarrow \mathsf{SKGen}(\mathsf{msk}, \phi_0)$.
- Hyb_1: Same as Hyb_0, except that the challenger sets the ct as a random ciphertext from ciphertext space of HIBE.

- Hyb_2: Same as Hyb_1, except the challenger ciphertext is $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{ek}_{\phi_1}, \mathsf{rcv}_1, \mu_1)$, where $\mathsf{ek}_{\phi_1} \leftarrow \mathsf{SKGen}(\mathsf{msk}, \phi_1)$.

We denote the advantage of adversary $\mathcal{A}$ in each game as $\mathsf{Adv}_i(\mathcal{A}) := \Pr[\mathsf{Hyb}_i^{\mathcal{A}} \Rightarrow 1]$. Note that the Hyb_2 is the experiment $\mathrm{G}^{\mathsf{priv}}_{\Pi,\mathcal{A}}(\lambda)$ for case that $b = 1$. We can obtain the advantage of $\mathcal{A}$ by $\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{A},\mathsf{IB\text{-}ME}}(\lambda) = | \mathsf{Adv}_0(\mathcal{A}) - \mathsf{Adv}_2(\mathcal{A}) |$.

We now show that every connected pair of hybrid arguments are computationally close.

- Hybrids Hyb_0 and Hyb_1 are computationally indistinguishable due to the ANON-IND-ID-CPA security (Def.4) of HIBE. Specifically, suppose that there exists an efficient adversary $\mathcal{A}$ being able to distinguish Hyb_0 from Hyb_1. We then use $\mathcal{A}$ to build an adversary $\mathcal{B}$ for the ANON-IND-ID-CPA security game of HIBE:
  1. At the beginning of the ANON-IND-ID-CPA security game, adversary $\mathcal{B}$ receives the public parameters $\mathsf{HIBE.mpk}$ from the challenger of ANON-IND-ID-CPA security game. Additionally, it runs $\mathsf{IBS.Setup}$ to obtain $\mathsf{IBS.mpk}$ and $\mathsf{IBS.msk}$. Then $\mathcal{B}$ sets mpk as $(\mathsf{HIBE.mpk}, \mathsf{IBS.mpk})$ and sends it to the adversary $\mathcal{A}$.
  2. When $\mathcal{A}$ queries a decryption key for an identity $\rho \in \mathcal{ID}$, $\mathcal{B}$ deliveries a key-generation query on level-1 identity ρ to obtain a key $\mathsf{HIBE.sk}_\rho$. It then sets $\mathsf{dk}_\rho \leftarrow \mathsf{HIBE.sk}_\rho$ and forwards it to $\mathcal{A}$. When $\mathcal{A}$ queries an encryption key query for an identity $\phi \in \mathcal{ID}$, $\mathcal{B}$ generates $\mathsf{IBS.sk}_\phi \leftarrow \mathsf{IBS.KeyExt}(\mathsf{IBS.msk}, \phi)$. $\mathcal{B}$ sets $\mathsf{ek}_\phi \leftarrow \mathsf{IBS.sk}_\phi$ and sends it to $\mathcal{A}$.
  3. When $\mathcal{A}$ makes a challenge query on $(\mu_0, \mu_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \phi_0, \phi_1)$, algorithm $\mathcal{B}$ firstly sets the bit $b = 0$, computes $\mathsf{IBS.sk}_{\phi_0} \leftarrow \mathsf{IBS.KeyExt}\ (\mathsf{IBS.msk}, \phi_0)$ and $\mathbf{t}^0 \leftarrow \mathsf{IBS.Sign}\ (\mathsf{IBS.sk}_{\phi_0}, \mathsf{rcv}_0|\mu_0)$. The adversary $\mathcal{B}$ submits the pair $(\mathsf{rcv}_0|\phi_0, \mathbf{t}_0|\mu_0)$ to its challenger as challenge query. The challenger replies to $\mathcal{B}$ with ct^*. Then, the algorithm $\mathcal{B}$ sets the received ciphertext as the challenge ciphertext and sends it to adversary $\mathcal{A}$.
  4. Finally, algorithm $\mathcal{B}$ sets the output of $\mathcal{A}$ to be its own guessing output.

  Firstly, we argue that $\mathcal{B}$ is admissible for the ANON-IND-ID-CPA game of HIBE. Since $\mathcal{A}$ is admissible for the privacy game, then for all decryption key generation queries $\rho \in \mathcal{ID}$ made by $\mathcal{A}$, it must satisfy that $\rho \neq \mathsf{rcv}_0 \wedge \rho \neq \mathsf{rcv}_1$. Due to the reason that the challenge query submitted by $\mathcal{B}$ forms of $(\mathsf{rcv}_0 \mid \phi_0, \mathbf{t}_0|\mu_0)$ and all key generation queries it issued are exactly identities ρ which queried by $\mathcal{A}$, this means that $\mathcal{B}$ never asked secret key for challenge identity or its prefix. Thus, $\mathcal{B}$ is admissible for the ANON-IND-ID-CPA game of HIBE. By construction, if $\mathsf{ct}^* \leftarrow \mathsf{HIBE.Enc}(\mathsf{HIBE.mpk}, \mathsf{rcv}_0|\phi_0, \mathbf{t}_0|\mu_0)$, then $\mathcal{B}$ perfectly simulated Hyb_0 for $\mathcal{A}$, and if ct^* is the random ciphertext chosen by challenger, then $\mathcal{B}$ perfectly simulated Hyb_1 for $\mathcal{A}$. Thus,

$$| \mathsf{Adv}_0(\mathcal{A}) - \mathsf{Adv}_1(\mathcal{A}) | \leq \mathsf{Adv}^{\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{B},\mathsf{HIBE}}(\lambda)$$

- Hybrids Hyb_1 and Hyb_2 are computationally indistinguishable by ANON-IND-ID-CPA security (Def.4) of HIBE via the same argument used to claim indistinguishability of hybrids Hyb_0 and Hyb_1. Thus,

$$| \mathsf{Adv}_1(\mathcal{A}) - \mathsf{Adv}_2(\mathcal{A}) | \leq \mathsf{Adv}^{\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{B},\mathsf{HIBE}}(\lambda)$$

Thus, we can obtain that

$$\mathsf{Adv}^{\mathsf{priv}}_{\mathcal{A},\mathsf{IB\text{-}ME}}(\lambda) \leq\ 2\mathsf{Adv}^{\mathsf{ANON\text{-}IND\text{-}ID\text{-}CPA}}_{\mathcal{B},\mathsf{HIBE}}(\lambda) + \mathsf{negl}(\lambda).$$

□
□

Lemma 4.2 *If* Π_{IBS} *is* UF-CMA *secure (Def. 6), then* $\Pi_{\mathsf{IB\text{-}ME}}$ *from Construction 1 satisfies stronger authenticity(Def. 10). In particular, for every p.p.t. algorithm* $\mathcal{A}$ *there is a p.p.t. algorithm* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathsf{new\text{-}auth}}_{\mathcal{A},\mathsf{IB\text{-}ME}}(\lambda) \leq \mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathcal{B},\mathsf{IBS}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. The proof strategy of Lemma 4.2 is based on a contradiction, i.e. we assume that there exists an adversary $\mathcal{A}'$ which can break the authenticity of Construction 1 with non-negligible advantage, then we could build an attacker $\mathcal{B}'$ that breaks UF-CMA of IBS. And the reduction procedure is in the following way:

1. At the beginning, algorithm $\mathcal{B}'$ receives $\mathsf{IBS.mpk}$ from the challenger. Then, it executes $(\mathsf{HIBE.mpk}, \mathsf{HIBE.msk}) \leftarrow \mathsf{HIBE.Setup}(1^\lambda)$, and sends $\mathsf{mpk} = (\mathsf{HIBE.mpk}, \mathsf{IBS.mpk})$ to adversary $\mathcal{A}'$.
2. For the queries issued by $\mathcal{A}'$, $\mathcal{B}'$ proceeds as follows:
   - When $\mathcal{A}'$ issues encryption key queries for ϕ, $\mathcal{B}'$ queries its challenger for secret signing key on input identity ϕ. $\mathcal{B}'$ sets the ek_ϕ as the signing key sk_ϕ received from the challenger, and sends it back to $\mathcal{A}'$.
   - When $\mathcal{A}'$ issues decryption key queries for ρ, $\mathcal{B}'$ generates $\mathsf{HIBE.sk}_\rho \leftarrow \mathsf{HIBE.Extract}(\mathsf{HIBE.msk}, \rho)$, sets $\mathsf{dk}_\rho \leftarrow \mathsf{HIBE.sk}_\rho$ and returns it to $\mathcal{A}'$.
   - When $\mathcal{A}'$ issues ciphertext queries for $(\phi, \mathsf{rcv}, \mu)$, $\mathcal{B}'$ first queries its challenger for signature on input $(\phi, \mathsf{rcv} \mid \mu)$ and receivers $\mathbf{t}$, then runs the encryption algorithm to obtain $\mathsf{ct}^{\mathbf{t}|\mu}$. Finally, it sends $\mathsf{ct} = \mathsf{ct}^{\mathbf{t}|\mu}$ to $\mathcal{A}'$.
3. Once the algorithm $\mathcal{B}'$ receives the forgery output $(\mathsf{ct}, \rho, \mathsf{snd})$ from adversary $\mathcal{A}'$, $\mathcal{B}'$ executes in the following way:
   - If $\mathcal{A}'$ ever asked encryption key for snd, returns 0.
   - Else, $\mathcal{B}'$ firstly generate $\mathsf{HIBE.sk}_\rho \leftarrow \mathsf{HIBE.Extract}(\mathsf{HIBE.msk}, \rho)$ and delegates the level-2 decryption key $\mathsf{dk}_{\rho|\mathsf{snd}} \leftarrow \mathsf{HIBE.Derive}(\mathsf{HIBE.sk}_\rho, \rho \mid \mathsf{snd})$. Then, it recovers $\mathbf{t}|\mu \leftarrow \mathsf{HIBE.Dec}(\mathsf{dk}_{\rho|\mathsf{snd}}, \mathsf{ct}^{\mathbf{t}|\mu})$ and verify the identity-based signature. It is clear that the decryption algorithm will output μ only when the signature $\mathbf{t}$ is valid corresponding to $(\mathsf{snd}, \rho \mid \mu)$.
   - If either $\mu = \perp$ or $\mathcal{A}'$ ever asked ciphertext for the same identities and message pair $(\mathsf{snd}, \rho \mid \mu)$, returns 0.
   - Else, $\mathcal{B}'$ returns $(\mathsf{snd}, \rho \mid \mu, \mathbf{t})$ as forgery signature to its challenger.

The secret key oracle and signing oracle of IBS challenger enables $\mathcal{B}$ to simulate all the queried oracles of $\mathcal{A}'$. The validity for forgery signature is also obvious, because the valid conditions of authenticity forgery output already contains the checking conditions for IBS. Concretely, $\mathcal{A}'$ is forbidden to query secret key for snd or signature for $(\mathsf{snd}, \rho \mid \mu)$, so as $\mathcal{B}'$. Thus, we extract $(\mathsf{snd}, \rho \mid \mu, \mathbf{t})$ as a valid forgery to break the UF-CMA of IBS. □

□

By combining Lemma 4.1 and Lemma 4.2, we can conclude that Construction 1 is secure. □

□

5 Adaptively Secure Identity-Based Signature

To improve the efficiency of IB-ME instantiation based on lattices assumptions, we shorten the signature size of an existing lattice-based IBS scheme to reduce the final IB-ME ciphertext sizes. Note that Pan and Wagner [PW21] proposed two generic transformations from non-adaptive IBS to adaptive one. We follow the same approach to obtain adaptive IBS. In other words, we pay attention to improving non-adaptive IBS from SIS assumptions respectively, and proving non-adaptive security. Using the lattice-based 2-level HIBE scheme of Agrawal *et al.* [ABB10b] and our improved IBS with adaptive security, our result implies the first lattice-based construction that implements IB-ME directly.

5.1 Improved Non-adaptive IBS from SIS

We provide our improved SIS-based IBS scheme in Fig.4. The intuition of improvement is reduce the signature size by slightly changing the "hash-and-sign" approach in the signing algorithm. The signature in [PW21] is generated by firstly computing a matrix $\mathbf{H} := \mathsf{H}(m)$ by hashing the message and then sampling a pre-image vector $\mathbf{z}$ such that $[\mathbf{F}_{\mathsf{id}}|\mathbf{H}] \cdot \mathbf{z} = \mathbf{0}$. The signer id is given a trapdoor for identity-matrix $\mathbf{F}_{\mathsf{id}}$ as signing secret key to performing $\mathsf{SampleLeft}$ algorithm. Instead of encoding message at the "left" pre-image position, we set the hashed message being the "right" image, such that the signature $\mathbf{z}'$ maps the $\mathbf{F}_{\mathsf{id}}$ to $\mathbf{h} := \mathsf{H}'(m)$. In such a case, the size of signatures is reduced from the column length of $[\mathbf{F}_{\mathsf{id}}|\mathbf{H}]$ to $\mathbf{F}_{\mathsf{id}}$.

$\mathsf{Setup}(1^\lambda)$

$(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q, s_0)$
$\mathsf{mpk} := \mathbf{A} \in \mathbb{Z}_q^{n \times m}$
$\mathsf{msk} := \mathbf{T}_{\mathbf{A}}$

$\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id})$

$\mathbf{H}_1 \leftarrow \mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$
$\mathbf{F}_{\mathsf{id}} \leftarrow [\mathbf{A} \mid \mathbf{H}_1]$
$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}(\mathbf{F}_{\mathsf{id}}, \mathbf{T}_{\mathbf{A}}, s)$
$\mathsf{sk}_{\mathsf{id}} := \mathbf{T}_{\mathsf{id}}$

Note: Hash functions $\mathsf{H}_1, \mathsf{H}_2$ are random oracles.
$\mathsf{H}_1 : \{0,1\}^* \to \mathbb{Z}_q^{n \times n\lceil \log q \rceil}$, $\mathsf{H}_2 : \{0,1\}^* \to \mathbb{Z}_q^n$.

$\mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m})$

$\mathbf{h}_2 \leftarrow \mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$
$\mathbf{z} \leftarrow \mathsf{SamplePre}(\mathbf{F}_{\mathsf{id}}, \mathbf{T}_{\mathsf{id}}, \mathbf{h}_2, s')$
s.t. $\mathbf{F}_{\mathsf{id}} \cdot \mathbf{z} = \mathbf{h}_2$
return $\sigma := \mathbf{z}$

$\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \mathbf{z})$

$\mathbf{H}_1 \leftarrow \mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$
$\mathbf{F}_{\mathsf{id}} \leftarrow [\mathbf{A} \mid \mathbf{H}_1]$
$\mathbf{h}_2 \leftarrow \mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$
if $\mathbf{z} = \mathbf{0} \vee \mathbf{F}_{\mathsf{id}} \cdot \mathbf{z} \neq \mathbf{h}_2$: return 0
else if $\|\mathbf{z}\| \leq s' \sqrt{m + n\lceil \log q \rceil}$

Fig. 4. Improved $\mathsf{na\text{-}IBS}_{\mathsf{SIS}} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sign}, \mathsf{Ver})$.

Correctness. For correctness, we check that verification algorithm will accept valid signatures generated by user id with overwhelming probability.

Lemma 5.1 *The identity-based signature scheme* $\mathsf{IBS}_{\mathsf{SIS}}$ *in Fig.4 is correct with overwhelming probability.*

Proof. For master public key and master secret key $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{Setup}(1^\lambda)$, an identity $\mathsf{id} \in \mathcal{ID}$ and message $m \in \mathcal{M}$. Let $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \mathsf{id})$ and $\mathbf{z} \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m})$. According to the definition of key generation algorithm, signing key $\mathsf{sk}_{\mathsf{id}}$ is the trapdoor for matrix $\mathbf{F}_{\mathsf{id}} := [\mathbf{A} \mid \mathbf{H}_1]$, which is an extension of public matrix $\mathbf{A}$. Thus, the trapdoor $\mathbf{T}_{\mathsf{id}}$ can be used to sample preimages in the signing algorithm. And the output vector $\mathbf{z}$ is sampled from the distribution statistically close to $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{h}_2}(\mathbf{A}), s'}$ by Lemma 2.6. In other word, $\mathbf{z}$ satisfies $\mathbf{h}_2 = \mathbf{F}_{\mathsf{id}} \cdot \mathbf{z}$ and $\|\mathbf{z}\| \leq s' \sqrt{m + n\lceil \log q \rceil}$. □
□

Parameter Selection. We provide the parameters to satisfy following restrictions.

- Let $m \geq 2n\lceil \log q \rceil$ and $s_0 > 0$ so that algorithm TrapGen of Lemma 2.5 works as specified.
- Let $s \gg s_1(\mathbf{T}_{\mathbf{A}})$ so that algorithm DelTrap of Lemma 2.7 works as specified.
- Let $s' \geq \sqrt{s_1(\mathbf{T}_{\mathsf{id}})^2 + 1} \cdot \|\widetilde{\mathbf{S}}\| \cdot \omega(\sqrt{\log n})$ so that algorithm SamplePre of Lemma 2.6 works as specified.
- Let the modulus q be sufficiently large relative to β, so that the hardness assumption of related SIS problem applies.

An appropriate choice of parameters is as follows:

$$n = \mathsf{poly}(\lambda),\ m = O(n\lceil \log q \rceil),\ \beta = s \cdot s' \cdot O(m + n\lceil \log q \rceil)$$
$$s_0 = \omega(\sqrt{\log m}),\ s = s_0 \cdot O(\sqrt{m - n\lceil \log q \rceil} + \sqrt{n\lceil \log q \rceil})$$
$$s' = s \cdot O(m + n\lceil \log q \rceil + \sqrt{m \cdot n\lceil \log q \rceil}) \cdot \omega(\sqrt{\log n})$$

We obtain the following keys and signature sizes:

- Master public key mpk is in $\mathbb{Z}_q^{n \times m}$ and hence has size $m \cdot n\lceil \log q \rceil$ bits.
- Master secret key msk is in $\mathbb{Z}_q^{(m-n\lceil \log q \rceil) \times (n\lceil \log q \rceil)}$ and hence has size $(m - n\lceil \log q \rceil) \times n \cdot \lceil \log q \rceil^2$ bits.
- Signing keys $\mathsf{sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$ are in $\mathbb{Z}_q^{m \times (n\lceil \log q \rceil)}$ and hence have size $m \cdot n \cdot \lceil \log q \rceil^2$ bits.
- Signatures $\mathbf{z}$ are in $\mathbb{Z}_q^{m+n\lceil \log q \rceil}$ and hence have size $(m + n\lceil \log q \rceil) \cdot \lceil \log q \rceil$ bits, which are $n \cdot \lceil \log q \rceil^2$ bits shorter than signatures in [PW21].

Remark 1 *Due to space limit, we only focus on the improved IBS construction bases on SIS hardness. As to RSIS-based instantiation construction, the high-level construction idea and proving method are quite similar. And we can also reduce the signature size following the similar improvement approach. Concretely, the size of signatures can be $h \cdot n \cdot \lceil \log q \rceil$ bits shorter than that in [PW21], where h refers to the dimension of gadget vector $\mathbf{g}$.*

Remark 2 *The proposed $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ scheme can be transformed into an adaptively secure through the generic transformations proposed by Pan and Wagner [PW21]. One transformation (in the standard model) relies on a chameleon hash function and another one (with random oracles) utilizes regular hash functions.*

5.2 The Security Proof

Here we prove the UF-naCMA security of $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ scheme showed in Fig.4 in the random oracle model. Using the generic transformations presented in [PW21], the final scheme will achieve the adaptive UF-CMA security.

Theorem 5.1 *Assuming the hardness of $\mathrm{SIS}_{n,m,q,\beta}$, then the identity-based signature scheme described in Fig. 4 achieves UF-naCMA security (Def.6) in the random oracle model. In particular, for every p.p.t. algorithm $\mathcal{A}$ there is a p.p.t. algorithm $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\mathsf{UF\text{-}naCMA}}_{\mathcal{A},\mathsf{na\text{-}IBS}}(\lambda) \leq \mathsf{Adv}^{\mathsf{SIS}_{n,m,q,\beta}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda).$$

Proof. We prove the UF-naCMA security of $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ by constructing an algorithm $\mathcal{B}$, presented in Fig. 5, which can solve SIS problem by interacting with adversary $\mathcal{A}$. The details of reduction process are as follows:

At the beginning of security reduction, algorithm $\mathcal{B}$ was given random SIS problem instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ as input. After receiving the lists $\mathcal{L}_{id}$ and $\mathcal{L}_m$ from the adversary $\mathcal{A}$, $\mathcal{B}$ sets $\mathbf{A}$ as master public key for $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ scheme and sends it to adversary $\mathcal{A}$.

- For every identity $\mathsf{id} \in \mathcal{L}_{id}$, $\mathcal{B}$ firstly selects matrix $\hat{\mathbf{R}}_{\mathsf{id}}$ from $\mathcal{D}_{\mathbb{Z},s}^{m \times n\lceil \log q \rceil}$, and program the random oracle H_1 as $h[1, \mathsf{mpk}, \mathsf{id}] := \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}} + \mathbf{G}$. Thus, $\hat{\mathbf{R}}_{\mathsf{id}}$ is a trapdoor for matrix $\mathbf{F}_{\mathsf{id}} := [\mathbf{A} \mid \mathsf{H}_1(\mathsf{mpk}, \mathsf{id})]$, also a secret signing key $\mathsf{sk}_{\mathsf{id}}$ for identity id, as it supports a connection with gadget matrix $\mathbf{G}$ for further operation like Gaussian sampling. Moreover, according to the definition of UF-naCMA security, adversary has not queried random oracles until now, which means programming is available. The distribution of the secret keys $\mathsf{sk}_{\mathsf{id}} := \hat{\mathbf{R}}_{\mathsf{id}}$ is statistically close to the real secret keys.
- For every identity and message pair $(\mathsf{id}, \mathsf{m}) \in \mathcal{L}_m$, $\mathcal{B}$ samples vector $\mathbf{z}_{\mathsf{id},\mathsf{m}}$ from distribution $\mathcal{D}_{\mathbb{Z},s'}^{m+n\lceil \log q \rceil}$, then program the random oracle as $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}] := [\mathbf{A} \mid \mathbf{H}_1] \cdot \mathbf{z}_{\mathsf{id},\mathsf{m}}$, and set vector $\mathbf{z}_{\mathsf{id},\mathsf{m}}$ to be the signature for $(\mathsf{id}, \mathsf{m})$. The programming is also available as the hash values have not been asked for. The signature generated by algorithm $\mathcal{B}$ is statistically close to the honest signatures.

After receiving the list of secret signing keys $\mathcal{L}_{sk}$ and signatures $\mathcal{L}_{sig}$, $\mathcal{A}$ queries random oracles H_1 and H_2 adaptively.

- For every identity id, for which adversary $\mathcal{A}$ queries for $\mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$, algorithm $\mathcal{B}$ first checks whether the hash value $\mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$ has been defined or not. If it has not been defined yet, then $\mathcal{B}$ draws matrix $\hat{\mathbf{R}}_{\mathsf{id}} \leftarrow \mathcal{D}_{\mathbb{Z},s}^{m \times n\lceil \log q \rceil}$, and programs $h[1, \mathsf{mpk}, \mathsf{id}] := \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}}$.
- For every identity and message pair $(\mathsf{id}, \mathsf{m})$, for which adversary $\mathcal{A}$ queries for $\mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$, algorithm $\mathcal{B}$ first checks whether the hash value $\mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$ has been defined or not. If it has not been defined yet, then $\mathcal{B}$ samples vector $\mathbf{z}'_{\mathsf{id},\mathsf{m}} \leftarrow \mathcal{D}_{\mathbb{Z},s'}^{m+n\lceil \log q \rceil}$, and programs $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}] := [\mathbf{A} \mid \mathbf{H}_1] \cdot \mathbf{z}'_{\mathsf{id},\mathsf{m}}$. Note that $\mathcal{B}$ only returns $\mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$ back to $\mathcal{A}$, and keeps $\mathbf{z}'_{\mathsf{id},\mathsf{m}}$ secret to its own.

At the end of UF-naCMA security game, adversary $\mathcal{A}$ outputs forgery signature $(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*)$. If the forgery is valid, in other words $\mathcal{A}$ wins the security game successfully, then by definition of UF-naCMA security $\mathsf{id}^* \notin \mathcal{L}_{id} \wedge (\mathsf{id}^*, \mathsf{m}^*) \notin \mathcal{L}_m$, and $[\mathbf{A} \mid \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}^*}]\mathbf{z}^* = \mathbf{h}_2$. Recall that when answering the query for random oracle H_2, challenger $\mathcal{B}$ additionally sampled a vector $\mathbf{z}'_{\mathsf{id}^*,\mathsf{m}^*}$ from gaussian distribution with parameter s', therefore the following equation holds: $[\mathbf{A} \mid \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}^*}]\mathbf{z}'_{\mathsf{id},\mathsf{m}} = \mathbf{h}_2$. It implies that

$$[\mathbf{A} \mid \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}^*}]\mathbf{z}^* = \mathbf{h}_2 = [\mathbf{A} \mid \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}^*}]\mathbf{z}'_{\mathsf{id},\mathsf{m}},$$

and then $\mathcal{B}$ can set the solution to SIS problem as

$$\mathbf{z} := [\mathbf{I}_m \mid \hat{\mathbf{R}}_{\mathsf{id}^*}](\mathbf{z}^* - \mathbf{z}'_{\mathsf{id},\mathsf{m}}).$$

It remains to show that $\mathbf{z}$ is a valid solution for $\mathrm{SIS}_{n,m,q,\beta}$ problem, i.e. $\mathbf{z} \neq \mathbf{0}$ and $\|\mathbf{z}\| \leq \beta$.

We prove that $\mathbf{z}$ is non-zero firstly. According to Lemma 2.1, the vector $\mathbf{z}'_{\mathsf{id},\mathsf{m}}$ follows the Gaussian distribution $\mathcal{D}_{\mathbb{Z},s'}^{m+n\lceil \log q \rceil}$ given $\mathbf{h}_2$ and $[\mathbf{A}|\mathbf{H}_1]$ to the adversary. Thus, $(\mathbf{z}^* - \mathbf{z}'_{\mathsf{id},\mathsf{m}}) \neq \mathbf{0}$ with high probability. Then set $\overline{\mathbf{z}} := (\mathbf{z}^* - \mathbf{z}'_{\mathsf{id},\mathsf{m}})$, write $\overline{\mathbf{z}} = [\overline{\mathbf{z}}_1 \in \mathbb{Z}_q^m \mid \ \overline{\mathbf{z}}_2 \in \mathbb{Z}_q^{n\lceil \log q \rceil}]^t$, $\mathbf{z}$ can be represented as

$$\mathbf{z} = \overline{\mathbf{z}}_1 + \hat{\mathbf{R}}_{\mathsf{id}^*} \cdot \overline{\mathbf{z}}_2.$$

If $\mathbf{z} = \mathbf{0}$, then it cannot be the case that $\overline{\mathbf{z}}_2 = \mathbf{0}$, because it implies that $\overline{\mathbf{z}}_1 = \mathbf{0}$ which makes $\overline{\mathbf{z}} = \mathbf{0}$. Thus, assume that $\overline{\mathbf{z}}_2$ has non-zero components $\overline{z}_{2,j}$ for some $j \in [n\lceil \log q \rceil]$. Denote each column of $\hat{\mathbf{R}}_{\mathsf{id}^*}$ as $\hat{\mathbf{r}}_{\mathsf{id}^*,i}$, where $i \in [n\lceil \log q \rceil]$. Based on the analysis above, assume that $\mathbf{z} = \mathbf{0}$, it turns out that $\hat{\mathbf{r}}_{\mathsf{id}^*,j}$ has to satisfy the following equation:

$$\hat{\mathbf{r}}_{\mathsf{id}^*,j} = -\tfrac{1}{\overline{z}_{2,j}}(\overline{\mathbf{z}}_1 + \sum_{i \neq j} \overline{z}_{2,i} \cdot \hat{\mathbf{r}}_{\mathsf{id}^*,i}).$$

On the other hand, the adversary $\mathcal{A}$ cannot touch $\hat{\mathbf{r}}_{\mathsf{id}^*,j}$ itself rather than a column of the programmed hash value $h[1, \mathsf{mpk}, \mathsf{id}] := \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}}$. Denote the corresponding column by $\mathbf{h}$, then by Lemma 2.1, $\hat{\mathbf{r}}_{\mathsf{id}^*,j}$ is distributed as $D_{\Lambda_{\mathbf{h}}^{\perp}(\mathbf{A}),s}$ from the view of the adversary $\mathcal{A}$. Note that by lemma 2.2, this distribution has a large min-entropy with overwhelming probability over $\mathbf{A} \xleftarrow{\$} \mathbf{Z}_q^{n \times m}$. Hence, the above equation holds with negligible probability. In other words, the probability that $\mathbf{z} = \mathbf{0}$ is negligible.

At last, we check the norm of $\mathbf{z}$. As in Lemma 2.3, $s_1(\hat{\mathbf{R}}_{\mathsf{id}^*}) \leq s \cdot O(\sqrt{m} + \sqrt{n\lceil \log q \rceil})$ with overwhelming probability. Then

$$\begin{aligned}
\|\mathbf{z}\| &\leq \|\overline{\mathbf{z}}_1\| + \|\hat{\mathbf{R}}_{\mathsf{id}^*}\| \cdot \|\overline{\mathbf{z}}_2\| \\
&\leq (1 + s \cdot O(\sqrt{m} + \sqrt{n\lceil \log q \rceil}))s' \cdot O(\sqrt{m + n\lceil \log q \rceil}) \\
&= s' \cdot O(\sqrt{m + n\lceil \log q \rceil}) + s \cdot s' \cdot O(\sqrt{m} + \sqrt{n\lceil \log q \rceil})O(\sqrt{m + n\lceil \log q \rceil}) \\
&\leq s' \cdot O(\sqrt{m + n\lceil \log q \rceil}) + s \cdot s' \cdot O(m + n\lceil \log q \rceil) \\
&\leq s \cdot s' \cdot O(m + n\lceil \log q \rceil) \leq \beta,
\end{aligned}$$

which means that $\mathbf{z}$ is a valid solution for $\mathrm{SIS}_{n,m,q,\beta}$ problem. Hence, we conclude that $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$ scheme is UF-naCMA secure. □

□

Algorithm $\mathcal{B}$ (Given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$)

1. $(\mathcal{L}_{id}, \mathcal{L}_m, St) \leftarrow \mathcal{A}(1^\lambda)$
2. $\mathsf{mpk} := \mathbf{A}$
3. **for** $\mathsf{id} \in \mathcal{L}_{id}$:
   - $\hat{\mathbf{R}}_{\mathsf{id}} \leftarrow \mathcal{D}_{\mathbb{Z},s}^{m \times n\lceil \log q \rceil}$
   - $h[1, \mathsf{mpk}, \mathsf{id}] := \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}} + \mathbf{G}$
   - $\mathsf{sk}_{\mathsf{id}} := \hat{\mathbf{R}}_{\mathsf{id}}$
   - $\mathcal{L}_{sk} := \mathcal{L}_{sk} \cup \{\mathsf{sk}_{\mathsf{id}}\}$
4. **for** $(\mathsf{id}, m) \in \mathcal{L}_m$:
   - $\mathbf{H}_1 \leftarrow \mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$
   - $\mathbf{z}_{\mathsf{id},\mathsf{m}} \leftarrow \mathcal{D}_{\mathbb{Z},s'}^{m+n\lceil \log q \rceil}$
   - $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}] := [\mathbf{A} \mid \mathbf{H}_1] \cdot \mathbf{z}_{\mathsf{id},\mathsf{m}}$
   - $\mathcal{L}_{sig} := \mathcal{L}_{sig} \cup \{\mathbf{z}_{\mathsf{id},\mathsf{m}}\}$

Oracle $\mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$

if $h[1, \mathsf{mpk}, \mathsf{id}] = \perp$:

- $\hat{\mathbf{R}}_{\mathsf{id}} \leftarrow \mathcal{D}_{\mathbb{Z},s}^{m \times n\lceil \log q \rceil}$
- $h[1, \mathsf{mpk}, \mathsf{id}] := \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}}$

return $h[1, \mathsf{mpk}, \mathsf{id}]$

5. $(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*) \leftarrow \mathcal{A}^{\mathsf{H}_1, \mathsf{H}_2}(St, \mathsf{mpk}, \mathcal{L}_{sk}, \mathcal{L}_{sig})$
6. **if** $\mathsf{id}^* \in \mathcal{L}_{id} \vee (\mathsf{id}^*, \mathsf{m}^*) \in \mathcal{L}_m$:
   return $\perp$
   if $\|\mathbf{z}^*\| > s'\sqrt{m + n\lceil \log q \rceil} \vee \mathbf{z}^* = \mathbf{0}$:
   return $\perp$
7. $\mathbf{F}_{\mathsf{id}^*} \leftarrow [\mathbf{A} \mid \mathbf{A}\hat{\mathbf{R}}_{\mathsf{id}^*}]$
   $\mathbf{h}_2 \leftarrow \mathsf{H}_2(\mathsf{mpk}, \mathsf{id}^*, \mathsf{m}^*)$
   if $\mathbf{F}_{\mathsf{id}^*}\mathbf{z}^* \neq \mathbf{h}_2$:
   return $\perp$
8. $\mathbf{z} := [\mathbf{I}_m \mid \hat{\mathbf{R}}_{\mathsf{id}^*}](\mathbf{z}^* - \mathbf{z}'_{\mathsf{id}^*,\mathsf{m}^*})$
   return $\mathbf{z}$

Oracle $\mathsf{H}_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})$

if $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}] = \perp$:

- $\mathbf{H}_1 \leftarrow \mathsf{H}_1(\mathsf{mpk}, \mathsf{id})$
- $\mathbf{z}'_{\mathsf{id},\mathsf{m}} \leftarrow \mathcal{D}_{\mathbb{Z},s'}^{m+n\lceil \log q \rceil}$
- $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}] := [\mathbf{A} \mid \mathbf{H}_1] \cdot \mathbf{z}'_{\mathsf{id},\mathsf{m}}$
- $\mathcal{L}'_{sig} := \mathcal{L}'_{sig} \cup \{\mathbf{z}'_{\mathsf{id},\mathsf{m}}\}$

return $h[2, \mathsf{mpk}, \mathsf{id}, \mathsf{m}]$

Fig. 5. Algorithm $\mathcal{B}$ aiming to solve $\mathrm{SIS}_{n,m,q,\beta}$ problem, revoking an adversary $\mathcal{A}$ for the UF-naCMA security of $\mathsf{na\text{-}IBS}_{\mathsf{SIS}}$

6 Conclusion

In this paper, we provide an IB-ME satisfying stronger security. We first proposed the improved security definition considering practical application requirements. Then we present a generic construction of IB-ME, which is proven secure under stronger security definition, from 2-level HIBE and IBS. To improve the efficiency of IB-ME instantiated on lattices, we further modify an existing SIS-based IBS to obtain shorter signatures along with simpler signature algorithm. By combining the improved IBS and any 2-level adaptively-secure lattice-based HIBE with anonymity, we finally obtain the first lattice-based IB-ME construction that achieves privacy and new-proposed stronger authenticity simultaneously.

References

ABB10a. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572, May / June 2010.

ABB10b. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 98–115, August 2010.

AFNV21. Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi. Match me if you can: Matchmaking encryption and its applications. *Journal of Cryptology*, 34(3):16, July 2021.

Ajt96. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

AW17. Shashank Agrawal and David J. Wu. Functional encryption: Deterministic to randomized functions from simple assumptions. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 30–61, April / May 2017.

BF01. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229, August 2001.

BL16. Xavier Boyen and Qinyi Li. Towards tightly secure lattice short signature and id-based encryption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 404–434, December 2016.

BL24. Xavier Boyen and Qinyi Li. Identity-based matchmaking encryption with enhanced privacy – a generic construction with practical instantiations. In Gene Tsudik, Mauro Conti, Kaitai Liang, and Georgios Smaragdakis, editors, *Computer Security – ESORICS 2023*, pages 425–445, Cham, 2024. Springer Nature Switzerland.

BLMQ05. Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In Bimal K. Roy, editor, *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 515–532. Springer, Heidelberg, December 2005.

Boy03. Xavier Boyen. Multipurpose identity-based signcryption (a swiss army knife for identity-based cryptography). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 383–399, August 2003.

CBDCF24. Roberta Cimorelli Belfiore, Andrea De Cosmo, and Anna Lisa Ferrara. Identity-based matchmaking encryption from standard lattice assumptions. In Christina Pöpper and Lejla Batina, editors, *Applied Cryptography and Network Security*, pages 163–188, Cham, 2024. Springer Nature Switzerland.

CHHS23. Sohto Chiku, Keitaro Hashimoto, Keisuke Hara, and Junji Shikata. Identity-based matchmaking encryption, revisited: Strong security and practical constructions from standard classical and post-quantum assumptions. Cryptology ePrint Archive, Paper 2023/1435, 2023. https://eprint.iacr.org/2023/1435.

CHKP12. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, October 2012.

CLL+13. Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Hoeteck Wee. Shorter IBE and signatures via asymmetric pairings. In Michel Abdalla and Tanja Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 122–140, May 2013.

CLWW22. Jie Chen, Yu Li, Jinming Wen, and Jian Weng. Identity-based matchmaking encryption from standard assumptions. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part III*, volume 13793 of *LNCS*, pages 394–422, December 2022.

DKL09. Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 621–630. ACM Press, May / June 2009.

FFMV22. Danilo Francati, Daniele Friolo, Giulio Malavolta, and Daniele Venturi. Multi-key and multi-input predicate encryption from learning with errors. Cryptology ePrint Archive, Report 2022/806, 2022.

FGRV21. Danilo Francati, Alessio Guidi, Luigi Russo, and Daniele Venturi. Identity-based matchmaking encryption without random oracles. In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *Progress in Cryptology – INDOCRYPT 2021*, pages 415–435, Cham, 2021. Springer International Publishing.

FO99. Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In Hideki Imai and Yuliang Zheng, editors, *PKC'99*, volume 1560 of *LNCS*, pages 53–68, March 1999.

Gen06. Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, May / June 2006.

GGG+14. Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. Multi-input functional encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 578–602, May 2014.

GJKS15. Vipul Goyal, Abhishek Jain, Venkata Koppula, and Amit Sahai. Functional encryption for randomized functionalities. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 325–351, March 2015.

GPV08. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

KMT19. Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 441–471, April 2019.

Kra10. Hugo Krawczyk. Cryptographic extraction and key derivation: The HKDF scheme. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 631–648, August 2010.

LLC24. Shen Lin, Yu Li, and Jie Chen. Cca-secure identity-based matchmaking encryption from standard assumptions. In Chunpeng Ge and Moti Yung, editors, *Information Security and Cryptology*, pages 253–273, Singapore, 2024. Springer Nature Singapore.

LP19. Roman Langrehr and Jiaxin Pan. Tightly secure hierarchical identity-based encryption. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 436–465, April 2019.

LP20a. Roman Langrehr and Jiaxin Pan. Hierarchical identity-based encryption with tight multi-challenge security. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 153–183, May 2020.

LP20b. Roman Langrehr and Jiaxin Pan. Unbounded HIBE with tight security. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 129–159, December 2020.

Mal02. John Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002.

MP12. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718, April 2012.

MR04. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. In *45th FOCS*, pages 372–381. IEEE Computer Society Press, October 2004.

OT09. Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231, December 2009.

PPS21. Chris Peikert, Zachary Pepin, and Chad Sharp. Vector and functional commitments from lattices. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part III*, volume 13044 of *LNCS*, pages 480–511, November 2021.

PW21. Jiaxin Pan and Benedikt Wagner. Short identity-based signatures with tight security from lattices. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, pages 360–379, 2021.

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

Sha84. Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53, August 1984.

Zhe97. Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption). In Burton S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 165–179, August 1997.