A preliminary version of this paper appears in Advances in Cryptology - ASIACRYPT 2021. This is the full version.

Identity-Based Encryption for Fair Anonymity Applications: Defining, Implementing, and Applying Rerandomizable RCCA-secure IBE

Yi Wang [*]
wangyi14@nudt.edu.cn

Rongmao Chen [†]
chromao@nudt.edu.cn

Xinyi Huang [‡]
xyhuang@fjnu.edu.cn

Jianting Ning [§]
jtning88@gmail.com

Baosheng Wang [¶]
bswang@nudt.edu.cn

Moti Yung [‖]
moti@cs.columbia.edu

September 20, 2021

Abstract

Our context is anonymous encryption schemes hiding their receiver, but in a setting which allows authorities to reveal the receiver when needed. While anonymous Identity-Based Encryption (IBE) is a natural candidate for such fair anonymity (it gives trusted authority access by design), the *de facto* security standard (a.k.a. IND-ID-CCA) is incompatible with the ciphertext rerandomizability which is crucial to anonymous communication. Thus, we seek to extend IND-ID-CCA security for IBE to a notion that can be meaningfully relaxed for rerandomizability while it still protects against active adversaries. To the end, inspired by the notion of replayable adaptive chosen-ciphertext attack (RCCA) security (Canetti *et al.*, Crypto'03), we formalize a new security notion called Anonymous Identity-Based RCCA (ANON-ID-RCCA) security for rerandomizable IBE and propose the first construction with rigorous security analysis. The core of our scheme is a novel extension of the double-strand paradigm, which was originally proposed by Golle *et al.* (CT-RSA'04) and later extended by Prabhakaran and Rosulek (Crypto'07), to the well-known Gentry-IBE (Eurocrypt'06). Notably, our scheme is the first IBE that simultaneously satisfies adaptive security, rerandomizability, and recipient-anonymity to date. As the application of our new notion, we design a new universal mixnet in the identity-based setting that does not require public key distribution (with fair anonymity). More generally, our new notion is also applicable to most existing rerandomizable RCCA-secure applications to eliminate the need for public key distribution infrastructure while allowing fairness.

[*]School of Computer, National University of Defense Technology, Changsha, China

[†]School of Computer, National University of Defense Technology, Changsha, China

[‡]Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China

[§]Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China & State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

[¶]School of Computer, National University of Defense Technology, Changsha, China

[‖]Google LLC & Columbia University, New York, USA

Contents

1 Introduction

Anonymity of encryption is a useful tool for building applications (such as various anonymous channels to unknown receivers). Anonymity typically is incorporated into systems in two ways: unconditional anonymity (without accountability), and fair anonymity (where a trusted authority may upon abuse revoke the anonymity). In this work, we are mainly interested in encryption schemes for the latter which gives a fair balance of privacy vs. anti-abuse measures (i.e., balancing individual privacy against societal safety). Anonymous Identity-Based Encryption (IBE) is a natural candidate for such a setting (it gives trusted authority access by design). Yet, other properties of such systems put some extra constraints: (1) ciphertext rerandomization: which is often used to hide connections of incoming and outgoing messages in various applications (in cryptographic applications such as anonymous communication protocol [3, 26], mixnet [13, 22], controlled function encryption [21] and cryptographic reverse firewalls [20, 9, 6]); and (2) protection against active attackers since often servers in the system can be probed with ciphertexts by anonymous parties.

The above combination of requirements, putting aside the accountability, points at the notion of replayable adaptive chosen ciphertext attack (RCCA) security, originally defined by Canetti *et al.* for public-key encryption (PKE) [4]. It is widely considered as a meaningful relaxation of CCA security, especially for its compatibility with ciphertext rerandomizability. Essentially, RCCA security is as strong as CCA security except that adversaries might have capability of mauling a ciphertext into a new one without changing the underlying plaintext. Such a relaxation makes the ciphertext possibly rerandomizable while still secure against active attackers. However, as it turns out, achieving rerandomizable RCCA (Rand-RCCA) security is quite challenging, and various specific efforts have been made to construct RCCA-secure PKE schemes for different anonymous applications (without accountability) [4, 15, 13, 24, 5, 18, 11, 10, 27].

As mentioned above, our goal of fair anonymity points at IBE. Thus, inspired by the RCCA security notion for PKE, we turn to study RCCA security in the context of IBE which, perhaps surprisingly, remains unsolved to date. Note that IBE was introduced by Shamir [25] in 1980s and has received extensive attentions in real-world applications since the first efficient realization in 2000s [2]. In an IBE system, the public key of a user is some unique information about his/her identity (e.g. email address). Thus, compared with typical PKE, IBE eliminates the need of public key distributions, making it also most desirable in applications which suffer costly public key certificate management.

Our main results. Starting with the *de facto* security notion—indistinguishability against adaptive chosen identity and ciphertext attack (IND-ID-CCA)—for typical IBE, we concretely seek how to define and realize a meaningful relaxation of IND-ID-CCA security for enabling rerandomizability. To the end, we come up with new results—in theoretical and practical aspects—as follows.

- We formalize a new security notion called "anonymous identity-based RCCA" (ANON-ID-RCCA) security for rerandomizable IBE, which is essentially the same as the notion of IND-ID-CCA except that, (i) adversaries may be able to maul a ciphertext into a new one of the same plaintext and recipient; and (ii) the recipient is anonymous given the ciphertext.

- We show that our new notion is achievable via designing an IBE scheme that satisfies ANON-ID-RCCA security and (universal) rerandomizability. A rigorous analysis which turns out to be quite challenging is carefully conducted to prove the security and rerandomizability of our proposed scheme.

- To demonstrate the usefulness of our new notion, we present an identity-based universal mixnet where our proposed rerandomizable ANON-ID-RCCA secure IBE plays as the core building block. Our proposed mixnet could serve as a desirable tool to balance individual privacy against societal safety.

Remark. We note that in the sequel we do not discuss opening of ciphertexts by the authorities for fair anonymity and we do not try to optimize it. We simply assume the authority knows all active identities which were enabled to receive ciphertexts, and can try all private keys; further, the message has enough redundancy so the authority can identify the correct receiver. Optimizing this aspect further is left for future work.

2 Results Overview and Related Work

In this section we provide an overview of the results presented in this work.

Relaxing IND-ID-CCA security. Note that existing RCCA security notion—by Canetti et al. [4]—is originally defined for PKE scheme and thus can not be straightforwardly adopted for IBE schemes. Nevertheless, inspired by the definition of RCCA security, we first formalize the notion of identity-based RCCA (ID-RCCA) security by relaxing the decryption oracle of IND-ID-CCA game in the sense that the adversary is allowed to query any ciphertext but gets "`replay`" if the decryption result equals to either of the two challenge plaintexts. Further, we enhance ID-RCCA security with the notion of recipient-anonymity, which roughly says that an IBE ciphertext does not leak any information about the underlying recipient identity. We name such a new notion as anonymous identity-based RCCA (ANON-ID-RCCA) security and show it is achievable via proposing an ANON-ID-RCCA secure IBE scheme that is rerandomizable.

An overview of our construction. The core of our construction is a novel extension of the double-strand paradigm by Golle et al. [13] to the well-known Gentry-IBE construction [12] which satisfies recipient-anonymity. We provide an overview of our construction below and the full scheme is given in Section 4.2.

The double-strand paradigm by Golle et al. [13]. Recall that the ciphertext of message m in the ElGamal-based universal cryptosystem by Golle et al. [13] is $\zeta_y(m) = (g^{r_0}, m \cdot y^{r_0}, g^{r_1}, y^{r_1}) \in \mathcal{G}^4$ where g is a random generator of group $\mathcal{G}$, $y = g^x$ is the public key corresponding to secret key x and r_0, r_1 are randomnesses. In fact, this ciphertext is composed of two strands of ElGamal encryptions: $E_y(m) = (g^{r_0}, m \cdot y^{r_0})$ and $E_y(1) = (g^{r_1}, y^{r_1})$. By the homomorphic property of the ElGamal encryption, $E_y(1)$ can be used to rerandomize both $E_y(m)$ and itself correctly. The double-strand paradigm offers an elegant way to re-encrypt ciphertext without any public parameters.

Unfortunately, this paradigm cannot be applied to the well-known Gentry-IBE [12] directly, as it is of IND-ID-CCA security which contradicts to the homomorphic property. To overcome this issue, inspired by the Rand-RCCA-secure scheme of Prabhakaran and Rosulek [24], we conduct further specific treatments on adjusting the original Gentry-IBE. Before the further explanation of our proposed approaches, we first brief describe the Gentry-IBE scheme.

Overview of the Gentry-IBE scheme. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a symmetric bilinear map where $\mathbb{G}$ and $\mathbb{G}_T$ are groups of prime order p. Let P be a random generator of $\mathbb{G}$, $[a]$ denote aP and $[a]_T$ denote $e(P, P)^a$ for any $a \in \mathbb{Z}_p^*$. In the Gentry-IBE scheme, the ciphertext under identity $\mathsf{ID} \in \mathbb{Z}_p$ and public parameters $([\alpha], [\vec{h}] = ([h_1], [h_2], [h_3]))$ is

$$E_{\mathsf{ID}}(m) = ([X_1], [\vec{X}_{2,4}]_T) = (\underbrace{[s\alpha_{\mathsf{ID}}], [s]_T}_{\text{key ciphertext}}, \underbrace{m \cdot [-sh_1]_T}_{\text{data ciphertext}}, \underbrace{[s\vec{\beta}\vec{h}_{2,3}^{\top}]_T}_{\text{validity checking}})$$

where $s \in \mathbb{Z}_p$, $\alpha_{\mathsf{ID}} = \alpha - \mathsf{ID}$, $[\vec{h}_{2,3}] = ([h_2], [h_3])$, $\beta = H([X_1], [\vec{X}_{2,3}]_T)$ and $\vec{\beta} = (1, \beta)$. $\alpha \in \mathbb{Z}_p$ is the master key and H is a collision-resistant hash function. At the high level, ciphertext in the Gentry-IBE scheme consists of three parts: key ciphertext, data ciphertext and validity checking. During the decryption procedure, the validity checking part is used to test the validity of ciphertext, while the key ciphertext is decrypted to obtain the session key for recovering the encrypted data. Below we show how to adjust the Gentry-IBE scheme towards ANON-ID-RCCA security with (universal) rerandomizability.

THE FIRST ATTEMPT. One can note that the first three elements $([X_1], [\vec{X}_{2,3}]_T)$ in $E_{\mathsf{ID}}(m)$ are analogous to the ElGamal encryption $E_y(m)$, and the value of last element $[X_4]_T$ varies with $([X_1], [\vec{X}_{2,3}]_T)$. Due to the collision resistance of hash function H, the value of β in $E_{\mathsf{ID}}(m)$ is different from that in $E_{\mathsf{ID}}(1)$. Thus, re-encrypting $E_{\mathsf{ID}}(m)$ with $E_{\mathsf{ID}}(1)$ would not derive a valid Gentry-IBE ciphertext. Consider that re-encryption does not change the underlying message m, we set the value of β in $E_{\mathsf{ID}}(m)$ and $E_{\mathsf{ID}}(1)$ as hash value $H(m)$, and obtain a Gentry-IBE-based universal cryptosystem with ciphertext $\zeta_{\mathsf{ID}}(m) = (\vec{X}, \vec{Y})$ where

$$\begin{array}{lllll} \vec{X} & = ([s\alpha_{\mathsf{ID}}], & [s]_T, & m \cdot [-sh_1]_T, & [s\vec{\mu}\vec{h}_{2,3}^{\top}]_T), \\ \vec{Y} & = ([t\alpha_{\mathsf{ID}}], & [t]_T, & [-th_1]_T, & [t\vec{\mu}\vec{h}_{2,3}^{\top}]_T) \end{array}$$

and $s, t \in \mathbb{Z}_p, \vec{\mu} = (1, H(m))$. A re-encryption of $\zeta_{\mathsf{ID}}(m)$ is $(\vec{X}', \vec{Y}') = (\vec{X} + s'\vec{Y}, t'\vec{Y})$ where $s', t' \in \mathbb{Z}_p$. One can verify that $(\vec{X}', \vec{Y}')$ is valid ciphertext with randomnesses $s + s't$ and $t't$.

Unfortunately, the above ID-based universal cryptosystem does not satisfy ID-RCCA security. Let $\zeta_{\mathsf{ID}}(m_b) = (\vec{X}, \vec{Y})$ be the challenge ciphertext in the ID-RCCA security game with $b \leftarrow_{\$} \{0, 1\}$. Adversary $\mathcal{A}$ guesses the bit b', computes a new strand

$$\vec{X}^* = \left([s'X_1], [s'X_2]_T, [s'X_3]_T/(m_{b'}^{s'-1}), [s'X_4]_T\right)$$

from $\vec{X}$ where $s' \in \mathbb{Z}_p$ and queries $(\vec{X}^*, \vec{Y})$ to the decryption oracle. If $b = b'$, then $(\vec{X}^*, \vec{Y})$ is a valid ciphertext and the oracle outputs `replay`; otherwise, it is invalid and the oracle outputs $\perp$. Thus, $\mathcal{A}$ can verify the guess and win the security game with overwhelming advantage.

RESTRICTING THE RERANDOMIZATION MANNER. We remark that a similar issue as above also occurs when Prabhakaran and Rosulek tried to apply the double-strand paradigm for the first realization of Rand-RCCA-secure PKE scheme in the standard model [24]. They proposed a clever idea of restricting the rerandomization of ciphertext by placing fixed vector $\vec{z} = (z_1, z_2, z_3, z_4)$ and random mask u on the key ciphertext part. Specifically, let $\mathbb{G}$ be a cyclic group of prime order p, g_1, g_2, g_3, g_4 are generators of $\mathbb{G}$ and $C, D, E \in \mathbb{G}$ belong to the public key, the first two strands in the ciphertext of message m are as follows.

$$(X_1, X_2, X_3, X_4, m \cdot C^x, (DE^{H(m)})^x, Y_1, Y_2, Y_3, Y_4, C^y, (DE^{H(m)})^y)$$

where $X_i = g_i^{(x+z_i)u}$ and $Y_i = g_i^{yu}$ for $i = 1, 2, 3, 4$. Unfortunately, while Prabhakaran and Rosulek's construction sheds some light on restricting the rerandomization manner, their approach requires the key ciphertext part to be extended to a vector, and thus is not feasible for the Gentry-IBE. Therefore, as it turns out as follows, further specific treatments are required for our construction.

To defend against the aforementioned attack, we disable the manner of rerandomization on strand $\vec{X}$ by introducing extra component in the validity checking part of both strands and perturbing the randomness in strand $\vec{X}$ with additional vector (z_0, z_1), and the strands in ciphertext $\zeta_{\mathsf{ID}}(m)$ are as follows.

$$\begin{array}{lllllll} \vec{X} & = ([s\alpha_{\mathsf{ID}}], & [s]_T, & m \cdot [-sh_1]_T, & [(s+z_0)\vec{\mu}\vec{h}_{2,3}^{\top}]_T, & [(s+z_1)\vec{\mu}\vec{h}_{4,5}^{\top}]_T); \\ \vec{Y} & = ([t\alpha_{\mathsf{ID}}], & [t]_T, & [-th_1]_T, & [t\vec{\mu}\vec{h}_{2,3}^{\top}]_T, & [t\vec{\mu}\vec{h}_{4,5}^{\top}]_T), \end{array}$$

where $\vec{h}_{4,5} = ([h_4], [h_5])$ are newly added public parameters. Although the aforementioned re-encryption is prohibited by the vector (z_0, z_1), it is still possible to rerandomize strand $\vec{X}$ by performing multiplication. Concretely, let b' be the guess of adversary $\mathcal{A}$, then $\mathcal{A}$ can compute a new strand $\vec{X}^*$ from $\vec{X}$ as follows:

$$\vec{X}^* = ([X_1 + s'\alpha_{\mathsf{ID}}],\ [X_2 + s']_T,\ [X_3 - s'h_1]_T,\ [X_4 + s'\vec{\mu}_{b'}\vec{h}_{2,3}^{\top}]_T,\ [X_5 + s'\vec{\mu}_{b'}\vec{h}_{4,5}^{\top}]_T),$$

where $s' \in \mathbb{Z}_p$ and $\vec{\mu}_{b'} = (1, H(m_{b'}))$. If $b = b'$, then the strand $\vec{X}^*$ is valid; otherwise, it is invalid.

To restrict the manner of rerandomization further, we mask the validity checking part with a secret value $u \in \mathbb{G}_T$, and encapsulate u with another two strands (i.e., $\vec{U}$ and $\vec{V}$). The ciphertext $\zeta_{\mathsf{ID}}(m)$ now consists of following four strands.

$$\begin{array}{lllll}
\vec{X} = & ([s\alpha_{\mathsf{ID}}], & [s]_T, & m \cdot [-sh_1]_T, & [\sigma(s+z_0)\vec{\mu}\vec{h}_{2,3}^{\top}]_T, \quad [\sigma(s+z_1)\vec{\mu}\vec{h}_{4,5}^{\top}]_T); \\
\vec{Y} = & ([t\alpha_{\mathsf{ID}}], & [t]_T, & [-th_1]_T, & [\sigma t\vec{\mu}\vec{h}_{2,3}^{\top}]_T, \quad [\sigma t\vec{\mu}\vec{h}_{4,5}^{\top}]_T); \\
\vec{U} = & ([\hat{s}\alpha_{\mathsf{ID}}], & [\hat{s}]_T, & u \cdot [-\hat{s}h_6]_T, & [\sigma\hat{s}h_7]_T); \\
\vec{V} = & ([\hat{t}\alpha_{\mathsf{ID}}], & [\hat{t}]_T, & [-\hat{t}h_6]_T, & [\sigma\hat{t}h_7]_T),
\end{array}$$

where $\hat{s}, \hat{t} \in \mathbb{Z}_p$, $\sigma = H(u) \in \mathbb{Z}_p$, $[h_6]$ and $[h_7]$ are newly added public parameters. It is worth mentioning that $[\sigma\hat{s}h_7]_T$ and $[\sigma\hat{t}h_7]_T$ are used to obstruct any ad-hoc multiplication operations on strands $\vec{U}$ and $\vec{V}$. The random mask u shared among $\vec{X}$, $\vec{Y}$, $\vec{U}$ and $\vec{V}$ prevents adversary from obtaining valid ciphertext by mixing strands in different ciphertexts (with same underlying plaintext) or rerandomizing strand with public key. Consequently, the only way to rerandomize ciphertext $\zeta_{\mathsf{ID}}(m)$ is as follows.

$$\vec{X}' = \vec{X} + s'\vec{Y}; \quad \vec{Y}' = t'\vec{Y}; \quad \vec{U}' = \vec{U} + \hat{s}'\vec{V}; \quad \vec{V}' = \hat{t}'\vec{V},$$

where $s', t', \hat{s}', \hat{t}' \in \mathbb{Z}_p$. We remark that the current Gentry-IBE-based universal cryptosystem is ANON-ID-RCCA secure. First, the ciphertext alone does not reveal any information about underlying message m and identity ID. Second, since the manner of re-encryption is restricted and adversary $\mathcal{A}$ cannot (partially) re-encrypt the ciphertext with challenge messages and identities correctly, the decryption oracle would not leak the bits picked by challenger.

To prove the ANON-ID-RCCA security, we make negligible modifications to the simulation of security game step by step. First, the setup and extraction algorithms are modified to generate secret keys without master key. Then, the challenge ciphertext is computed using alternative encryption algorithm such that its distribution is independent of the underlying identity and plaintext. Finally, the challenger answers all the decryption queries via a time-unbounded decryption algorithm that uses public parameters and challenge ciphertext only to decrypt ciphertext. At this time, the extraction and decryption queries do not provide extra information about master key and private keys to the adversary, and challenge ciphertext perfectly hides the identity and plaintext. So the advantage of adversary is 0. More details will be given in the proof of Theorem 4.2.

Applications of rerandomizable ANON-ID-RCCA security. To show the usefulness of our new notion, we present an ID-based universal mixnet based on rerandomizable ANON-ID-RCCA secure IBE. The notion of universal mixnet was defined by Golle et al. [13] and has various applications such as anonymous communication and RFID tag anonymization. Roughly, a universal mix network mainly consists of a list of mix-servers which perform rerandomization and shuffle to break the linkability between incoming and outgoing messages. Universal mixnet

is attractive due to its elimination of public key distribution among on-path mix-servers when sending message. In this work, based on rerandomizable ANON-ID-RCCA secure IBE, we design an ID-based universal mixnet which could be viewed as an extension of universal mix network in the identity-based setting to further eliminate the public key certificate management and to provide a more covert way of communication for end users. Also, our proposed mixnet enjoys fair anonymity where a trusted authority may upon abuse revoke the anonymity and thus gives a fair balance of privacy vs. anti-abuse measures. Compared with previous work [16], our construction satisfies stronger unlinkability where the adversary is allowed to probe the system with ciphertexts.

It is worth noting that our notion could be generally applicable to extend other Rand-RCCA-secure applications to the identity-based setting to eliminate the public-key certification management and support fair anonymity.

Other related work. The first perfect Rand-RCCA-secure scheme, where one cannot link a ciphertext to its re-encryptions, is proposed by Groth [15] under the generic group model. The ciphertext size of this scheme grows linearly with the bit-length of the plaintext. Phan and Pointcheval [23] presented an efficient framework for RCCA-secure PKE, whereas the rerandomizability of its instantiation in [22] suffers from active attacks. Then, inspired by the Cramer-Shoup encryption [7], Prabhakaran and Rosulek [24] proposed the first perfect Rand-RCCA-secure PKE in the standard model. Their scheme is universally rerandomizable—no public key is involved for ciphertext rerandomization—due to the adoption of double-strand structure by Golle et al. [13]. Chase et al. [5] designed a perfect Rand-RCCA-secure scheme satisfying public verifiability from malleable NIZKs. Libert et al. [18] improved the scheme of Chase et al., but the ciphertext size of their scheme is still large due to the usage of NIZK. Faonio et al. [11] presented a structure-preserving Rand-RCCA-secure PKE based on matrix Diffie-Hellman assumption. Their scheme does not consider universal rerandomizability and thus is more efficient than the construction by Prabhakaran and Rosulek [24]. Faonio and Fiore [10] presented an efficient Rand-RCCA-secure PKE achieving weak rerandomizability under the random oracle model. Badertscher et al. [1] found that RCCA security cannot achieve the confidentiality benchmark in the setting of constructive cryptography [19], and proposed three natural variants of RCCA security that correspond to different benchmark applications.

Recently, Wang et al. [27] proposed a generic framework for receiver-anonymous Rand-RCCA-secure PKE and solved the open problem left by [24]. In fact, although our construction is not trivially implied by their framework, our core idea could be viewed as a novel extension of their construction to the identity-based setting. It is worth noting that while our scheme only achieves computational rerandomizability, it is sufficient for some privacy-related applications.

3 Preliminaries

Let $n \in \mathbb{N}$ denote the security parameter and $\mathsf{negl}(n)$ denote the negligible function. Let $\vec{a} = (a_1, \cdots, a_n)$ be a n-tuple vector. We use $\vec{a}_{i,j}$ to denote vector $(a_i, \cdots, a_j)$ for any $i, j \in \{1, \cdots, n\}$ with $i < j$. A symmetric bilinear group is a tuple $(p, \mathbb{G}, \mathbb{G}_T, e, P)$ where $\mathbb{G}$ and $\mathbb{G}_T$ are groups of prime order p, P is a generator of $\mathbb{G}$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is an efficiently computable, non-degenerate bilinear map. For clarity, we use $[a]$ to denote element aP in $\mathbb{G}$ and $[a]_T$ to denote element $e(P, P)^a$ in $\mathbb{G}_T$. Given $a, b \in \mathbb{Z}_p$, we define $[ab] \coloneqq abP$ and $[a] \cdot [b] \coloneqq e([a], [b]) = [ab]_T$. Given $\vec{a} \in \mathbb{Z}_p^n$, we define $[\vec{a}] \coloneqq ([a_1], \cdots, [a_n])$ and $[\vec{a}]_T \coloneqq ([a_1]_T, \cdots, [a_n]_T)$.

Definition 3.1 (Truncated Decision Augmented Bilinear Diffie-Hellman Exponent Assumption [12])**.** The truncated decision q-ABDHE assumption holds for $(\mathbb{G}, \mathbb{G}_T, e)$ if for any PPT

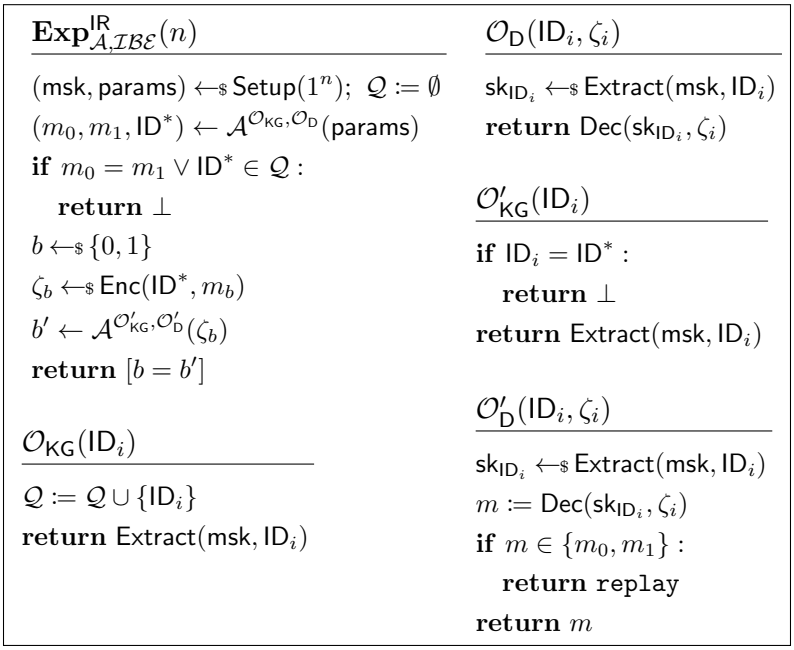

Figure 1: The ID-RCCA security game.

adversary $\mathcal{A}$,

$$\left|\Pr\left[\mathcal{A}\left([\beta], [\beta\alpha^{q+2}], [1], [\alpha], \cdots, [\alpha^q], [\beta\alpha^{q+1}]_T\right) = 0\right]\right.$$
$$\left. - \Pr\left[\mathcal{A}\left([\beta], [\beta\alpha^{q+2}], [1], [\alpha], \cdots, [\alpha^q], Z\right) = 0\right]\right| \leq \mathsf{negl}(n)\,,$$

where the probability is over random generators $[1], [\beta] \leftarrow\!\!\$\ \mathbb{G}$, random $\alpha \leftarrow\!\!\$\ \mathbb{Z}_p$, random $Z \leftarrow\!\!\$\ \mathbb{G}_T$ and the coin tosses of adversary $\mathcal{A}$. We use $\mathcal{P}_{ABDHE}$ to denote the distribution on the left and $\mathcal{R}_{ABDHE}$ to denote the distribution on the right.

4 Rerandomizable ANON-ID-RCCA IBE: Definitions and Construction

4.1 Definitions

Identity-Based Encryption (IBE). An IBE scheme $\mathcal{IBE}$ is specified by four algorithms: Setup, Extract, Enc and Dec.

- Setup takes as input 1^n where n is the security parameter and returns master key msk and system parameters params including message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.
- Extract takes as input params, msk and arbitrary $\mathsf{ID} \in \{0,1\}^*$, and returns a private key $\mathsf{sk}_{\mathsf{ID}}$.
- Enc takes as input params, ID and $m \in \mathcal{M}$, and returns a ciphertext $\zeta \in \mathcal{C}$.
- Dec takes as input params, $\mathsf{sk}_{\mathsf{ID}}$ and $\zeta \in \mathcal{C}$, and returns $m \in \mathcal{M}$ or $\perp$.

We omit the system parameters from the input to Extract, Enc and Dec. The scheme is *correct* if for $(\mathsf{msk}, \mathsf{params}) \leftarrow\!\!\$\ \mathsf{Setup}(1^n)$, any $m \in \mathcal{M}$, any $\mathsf{ID} \in \{0,1\}^*$ and $\mathsf{sk}_{\mathsf{ID}} = \mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$, $\Pr[\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \mathsf{Enc}(\mathsf{ID}, m)) \neq m] \leq \mathsf{negl}(n)$.

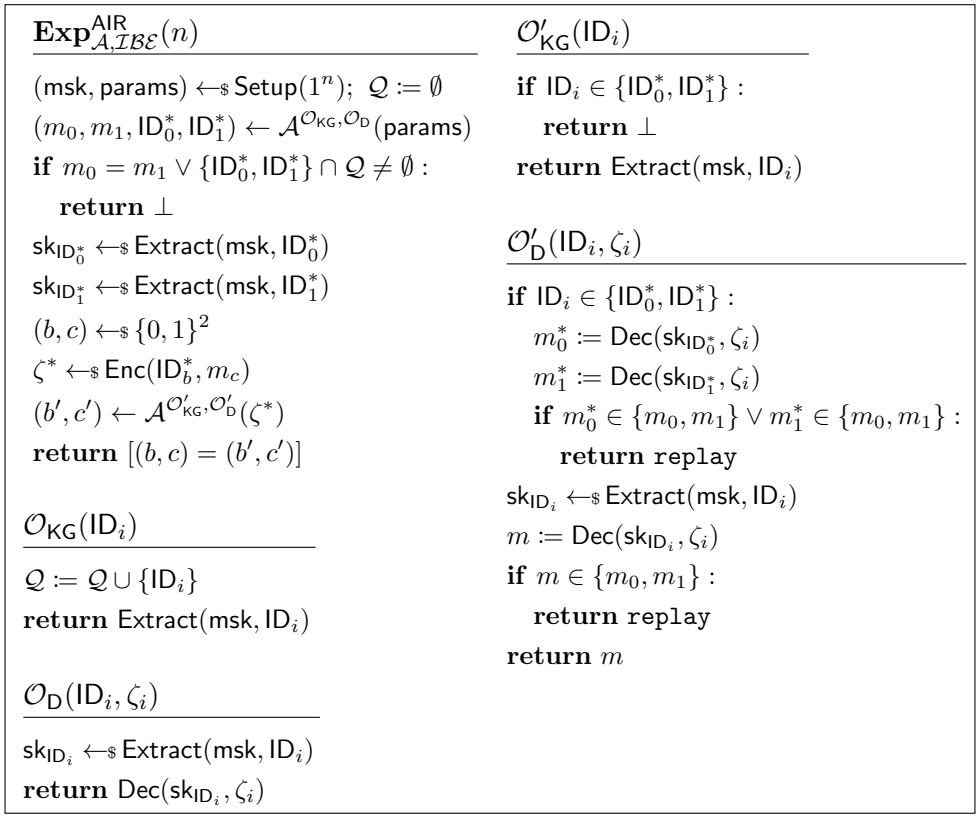

Figure 2: The ANON-ID-RCCA security game.

Below we define a new notion named ID-RCCA security for IBE. It can be viewed as a slight relaxation of ID-CCA security.

Definition 4.1 (ID-RCCA Security)**.** Let $\mathcal{IBE} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Consider the security game $\mathbf{Exp}^{\mathsf{IR}}_{\mathcal{A},\mathcal{IBE}}$ in Fig. 1, we say $\mathcal{IBE}$ is secure against replayable chosen ciphertext attacks (ID-RCCA secure) if for any PPT adversary $\mathcal{A}$,

$$\mathbf{Adv}^{\mathsf{IR}}_{\mathcal{A},\mathcal{IBE}}(n) := \left|\Pr\left[\mathbf{Exp}^{\mathsf{IR}}_{\mathcal{A},\mathcal{IBE}}(n) = 1\right] - 1/2\right| \leq \mathsf{negl}(n)\,.$$

We say that an IBE scheme is "anonymous" if for any PPT adversary two ciphertexts generated under different identities are computationally indistinguishable. Formally, we incorporate the property of anonymity into game $\mathbf{Exp}^{\mathsf{IR}}_{\mathcal{A},\mathcal{IBE}}$ and obtain the game for ANON-ID-RCCA security as shown in Fig. 2.

Definition 4.2 (ANON-ID-RCCA Security)**.** Let $\mathcal{IBE} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ be an IBE scheme. Consider the security game $\mathbf{Exp}^{\mathsf{AIR}}_{\mathcal{A},\mathcal{IBE}}$ in Fig. 2, we say $\mathcal{IBE}$ is anonymous and ID-RCCA secure (ANON-ID-RCCA secure) if for any PPT adversary $\mathcal{A}$,

$$\mathbf{Adv}^{\mathsf{AIR}}_{\mathcal{A},\mathcal{IBE}}(n) := \left|\Pr\left[\mathbf{Exp}^{\mathsf{AIR}}_{\mathcal{A},\mathcal{IBE}}(n) = 1\right] - 1/4\right| \leq \mathsf{negl}(n)\,.$$

We now define rerandomizability for ID-RCCA secure IBE. In fact, it can be viewed as the weak rerandomizability by Faonio and Fiore [10] in the identity-based setting. Besides, we mainly consider "universal rerandomizability" [13, 24] which essentially means that no public key is involved for rerandomization.

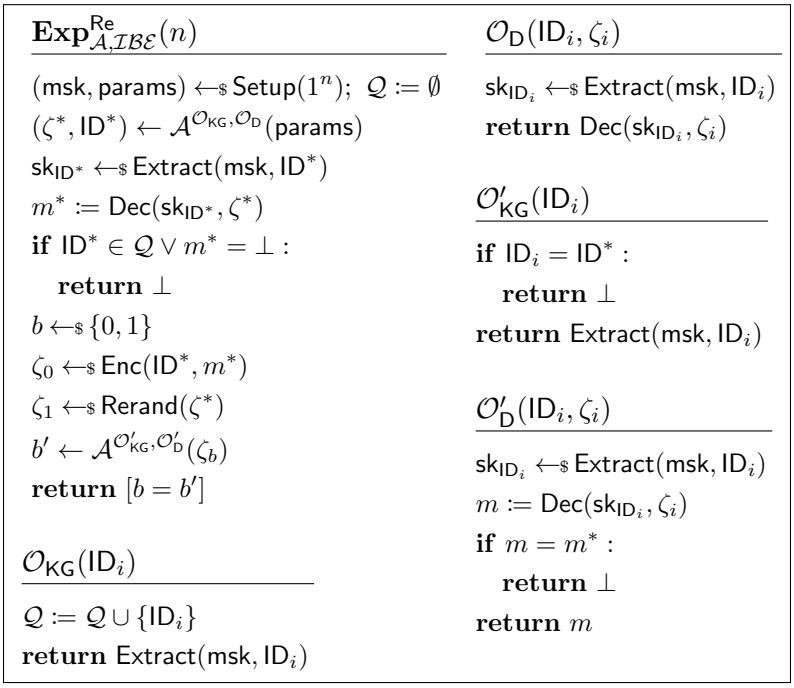

Figure 3: The security game of rerandomizability.

Definition 4.3 (Rerandomizability)**.** Let $\mathcal{IBE}$ be an ID-RCCA secure IBE, we say $\mathcal{IBE}$ is rerandomizable if following conditions are satisfied.

- **(Correctness)** There exists a PPT algorithm Rerand that takes as input ciphertext ζ and outputs a new ciphertext ζ'; and for $(\mathsf{msk},\mathsf{params}) \leftarrow\!\!\$\ \mathsf{Setup}(1^n)$, any $\mathsf{ID} \in \{0,1\}^*$, $\mathsf{sk}_{\mathsf{ID}} = \mathsf{Extract}(\mathsf{msk},\mathsf{ID})$, any ciphertext ζ,

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}},\zeta') \neq \mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}},\zeta) : \zeta' \leftarrow\!\!\$\ \mathsf{Rerand}(\zeta)\right] \leq \mathsf{negl}(n)\,;$$

- **(Indistinguishability)** For any PPT adversary $\mathcal{A}$ in Fig. 3,

$$\mathbf{Adv}^{\mathsf{Re}}_{\mathcal{A},\mathcal{IBE}}(n) := \left|\Pr\left[\mathbf{Exp}^{\mathsf{Re}}_{\mathcal{A},\mathcal{IBE}}(n) = 1\right] - 1/2\right| \leq \mathsf{negl}(n)\,;$$

- **(Tightness of Decryption)** For $(\mathsf{msk},\mathsf{params}) \leftarrow\!\!\$\ \mathsf{Setup}(1^n)$, any $\mathsf{ID} \in \{0,1\}^*$, $\mathsf{sk}_{\mathsf{ID}} = \mathsf{Extract}(\mathsf{msk},\mathsf{ID})$ and any (possibly unbounded) adversary $\mathcal{A}$,

$$\Pr\left[m \neq \perp \wedge \zeta \notin \mathsf{Enc}(\mathsf{ID},m) : \begin{array}{l}\zeta \leftarrow \mathcal{A}(\mathsf{params},\mathsf{ID}) \\ m := \mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}},\zeta)\end{array}\right] \leq \mathsf{negl}(n)\,,$$

  where $\zeta \notin \mathsf{Enc}(\mathsf{ID},m)$ means ζ is not in the range of $\mathsf{Enc}(\mathsf{ID},m)$.

4.2 Our Proposed Scheme

We are now ready to describe our full scheme with security analysis. Let $(p,\mathbb{G},\mathbb{G}_T,e,P)$ denote a symmetric bilinear group and $H : \mathbb{G}_T \to \mathbb{Z}_p$ be a collision-resistant hash function. Our rerandomizable ANON-ID-RCCA secure IBE scheme $\mathcal{IBE}$ is shown in Fig. 4. Below we analyse the correctness and security of our proposed scheme.

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

$[\vec{h}] \coloneqq ([h_1], \cdots, [h_7]) \leftarrow\!\$\, \mathbb{G}^7$
$\alpha, z_0, z_1 \leftarrow\!\$\, \mathbb{Z}_p$; $\mathsf{msk} \coloneqq \alpha$
$\mathsf{params} \coloneqq ([1], [\alpha], [\vec{h}], z_0, z_1)$
return $(\mathsf{msk}, \mathsf{params})$

$\mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$

if $\mathsf{ID} = \alpha$, **return** $\perp$
$\vec{r}_{\mathsf{ID}} \coloneqq (r_{\mathsf{ID},1}, \cdots, r_{\mathsf{ID},7}) \leftarrow\!\$\, \mathbb{Z}_p^7$
$\alpha_{\mathsf{ID}} \coloneqq \alpha - \mathsf{ID}$; $\vec{h}_{\mathsf{ID}} \coloneqq (\vec{h} - \vec{r}_{\mathsf{ID}})/\alpha_{\mathsf{ID}}$
return $\mathsf{sk}_{\mathsf{ID}} \coloneqq (\vec{r}_{\mathsf{ID}}, [\vec{h}_{\mathsf{ID}}])$

$\mathsf{Enc}(\mathsf{ID}, m \in \mathbb{G}_T)$

$s, t, \hat{s}, \hat{t} \leftarrow\!\$\, \mathbb{Z}_p$; $u \leftarrow\!\$\, \mathbb{G}_T$; $\sigma \coloneqq H(u)$; $\vec{\mu} \coloneqq (1, H(m))$; $(s^\dagger, s^\ddagger) \coloneqq (s + z_0, s + z_1)$
$\vec{X} \coloneqq ([X_1], [\vec{X}_{2,5}]_T) \coloneqq ([s\alpha_{\mathsf{ID}}], [s]_T, m \cdot [-sh_1]_T, [\sigma s^\dagger \vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma s^\ddagger \vec{\mu}\vec{h}_{4,5}^\top]_T)$
$\vec{Y} \coloneqq ([Y_1], [\vec{Y}_{2,5}]_T) \coloneqq ([t\alpha_{\mathsf{ID}}], [t]_T, [-th_1]_T, [\sigma t\vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma t\vec{\mu}\vec{h}_{4,5}^\top]_T)$
$\vec{U} \coloneqq ([U_1], [\vec{U}_{2,4}]_T) \coloneqq ([\hat{s}\alpha_{\mathsf{ID}}], [\hat{s}]_T, u \cdot [-\hat{s}h_6]_T, [\sigma\hat{s}h_7]_T)$
$\vec{V} \coloneqq ([V_1], [\vec{V}_{2,4}]_T) \coloneqq ([\hat{t}\alpha_{\mathsf{ID}}], [\hat{t}]_T, [-\hat{t}h_6]_T, [\sigma\hat{t}h_7]_T)$; **return** $\zeta \coloneqq (\vec{X}, \vec{Y}, \vec{U}, \vec{V})$

$\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \zeta)$

$\vec{K} \coloneqq (\vec{h}_{\mathsf{ID}}^\top, \vec{r}_{\mathsf{ID}}^\top)^\top$; $\vec{X}_{1,2}^\dagger \coloneqq \vec{X}_{1,2} + (z_0\alpha_{\mathsf{ID}}, z_0)$; $\vec{X}_{1,2}^\ddagger \coloneqq \vec{X}_{1,2} + (z_1\alpha_{\mathsf{ID}}, z_1)$
$m \coloneqq [X_3 + \vec{X}_{1,2}\vec{K}_1]_T$; $u \coloneqq [U_3 + \vec{U}_{1,2}\vec{K}_6]_T$; $\mu \coloneqq H(m)$; $\vec{\mu} \coloneqq (1, \mu)$; $\sigma \coloneqq H(u)$
$[\vec{V}'_{3,4}]_T \coloneqq ([-\vec{V}_{1,2}\vec{K}_6]_T, [\sigma\vec{V}_{1,2}\vec{K}_7]_T)$; $[U'_4]_T \coloneqq [\sigma\vec{U}_{1,2}\vec{K}_7]_T$
if $([\vec{V}'_{3,4}]_T, [U'_4]_T) \neq ([\vec{V}_{3,4}]_T, [U_4]_T)$, **return** $\perp$
$[\vec{X}'_{4,5}]_T \coloneqq ([\sigma\vec{X}_{1,2}^\dagger\vec{K}_{2,3}\vec{\mu}^\top]_T, [\sigma\vec{X}_{1,2}^\ddagger\vec{K}_{4,5}\vec{\mu}^\top]_T)$
$[\vec{Y}'_{4,5}]_T \coloneqq ([\sigma\vec{Y}_{1,2}\vec{K}_{2,3}\vec{\mu}^\top]_T, [\sigma\vec{Y}_{1,2}\vec{K}_{4,5}\vec{\mu}^\top]_T)$; $[Y'_3]_T \coloneqq [-\vec{Y}_{1,2}\vec{K}_1]_T$
if $([\vec{X}'_{4,5}]_T, [\vec{Y}'_{4,5}]_T, [Y'_3]_T) \neq ([\vec{X}_{4,5}]_T, [\vec{Y}_{4,5}]_T, [Y_3]_T)$, **return** $\perp$; **else** , **return** m

$\mathsf{Rerand}(\zeta)$

$s', t', \hat{s}', \hat{t}' \leftarrow\!\$\, \mathbb{Z}_p$
$\vec{X}' \coloneqq ([X_1 + s'Y_1], [\vec{X}_{2,5} + s'\vec{Y}_{2,5}]_T)$; $\vec{Y}' \coloneqq ([t'Y_1], [t'\vec{Y}_{2,5}]_T)$
$\vec{U}' \coloneqq ([U_1 + \hat{s}'V_1], [\vec{U}_{2,4} + \hat{s}'\vec{V}_{2,4}]_T)$; $\vec{V}' \coloneqq ([\hat{t}'V_1], [\hat{t}'\vec{V}_{2,4}]_T)$
return $\zeta' \coloneqq (\vec{X}', \vec{Y}', \vec{U}', \vec{V}')$

Figure 4: Our rerandomizable ANON-ID-RCCA secure IBE scheme.

Theorem 4.1 (Decryption Correctness)**.** *For* $(\mathsf{msk}, \mathsf{params}) \leftarrow\!\$\, \mathsf{Setup}(1^n)$*, any identity* $\mathsf{ID} \in \mathbb{Z}_p$ *and private key* $\mathsf{sk}_{\mathsf{ID}} = \mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$*, any* $m \in \mathcal{M}$*, we have*

$$\Pr[\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \mathsf{Enc}(\mathsf{ID}, m)) \neq m] \leq \mathsf{negl}(n)\,.$$

Proof. Assume that $\zeta = (\vec{X}, \vec{Y}, \vec{U}, \vec{V}) = \mathsf{Enc}(\mathsf{ID}, m)$. We consider the retrieval of plaintext m. That is, $[X_3 + \vec{X}_{1,2}\vec{K}_1]_T = [X_3 + s\alpha_{\mathsf{ID}}h_{\mathsf{ID},1} + sr_{\mathsf{ID},1}]_T = [X_3]_T \cdot [s(h_1 - r_{\mathsf{ID},1}) + sr_{\mathsf{ID},1}]_T = m$. Similarly, we have $[U_3 + \vec{U}_{1,2}\vec{K}_6]_T = u$. As for the validity checking part, we take $[\vec{X}_{4,5}]_T$ for example.

$$\begin{aligned}
& ([\sigma\vec{X}_{1,2}^\dagger\vec{K}_{2,3}\vec{\mu}^\top]_T, [\sigma\vec{X}_{1,2}^\ddagger\vec{K}_{4,5}\vec{\mu}^\top]_T) \\
= \; & ([\sigma((s+z_0)\alpha_{\mathsf{ID}}(h_{\mathsf{ID},2} + \mu h_{\mathsf{ID},3}) + (s+z_0)(r_{\mathsf{ID},2} + \mu r_{\mathsf{ID},3}))]_T, \\
& [\sigma((s+z_1)\alpha_{\mathsf{ID}}(h_{\mathsf{ID},4} + \mu h_{\mathsf{ID},5}) + (s+z_1)(r_{\mathsf{ID},4} + \mu r_{\mathsf{ID},5}))]_T) \\
= \; & ([\sigma(s+z_0)(h_2 + \mu h_3)]_T, [\sigma(s+z_1)(h_4 + \mu h_5)]_T) \\
= \; & ([\sigma s^\dagger\vec{\mu}\vec{h}_{2,3}^\top], [\sigma s^\ddagger\vec{\mu}\vec{h}_{4,5}^\top]) = [\vec{X}_{4,5}]_T.
\end{aligned}$$

One also can verify that checks on $[\vec{Y}_{4,5}]_T$, $[\vec{V}_{3,4}]_T$, $[Y_3]_T$, $[U_4]_T$ are valid. ∎

$\mathsf{AltSetup}(1^n, \mathcal{G})$	$\mathsf{AltExtract}(\mathsf{ID}, \mathcal{G})$
$z_0, z_1 \leftarrow\!\!\$\, \mathbb{Z}_p$	**if** $[\mathsf{ID}] = [\alpha]$, **return** $\perp$
$\vec{f}(x) \leftarrow\!\!\$\, (\mathbb{Z}_p[x])^7$; $[\vec{h}] := [\vec{f}(\alpha)]$	$\vec{r}_{\mathsf{ID}} := \vec{f}(\mathsf{ID})$; $[\vec{h}_{\mathsf{ID}}] := [\vec{F}_{\mathsf{ID}}(\alpha)]$
$\mathsf{params} := ([1], [\alpha], [\vec{h}], z_0, z_1)$	$\mathsf{sk}_{\mathsf{ID}} := (\vec{r}_{\mathsf{ID}}, [\vec{h}_{\mathsf{ID}}])$
return params	**return** $\mathsf{sk}_{\mathsf{ID}}$

Figure 5: Alternative setup algorithm AltSetup and extraction algorithm AltExtract.

Theorem 4.2 (ANON-ID-RCCA Security)**.** *Let q_{ID} be the times of extraction queries and $q = q_{\mathsf{ID}} + 2$. Assume that the truncated decision q-ABDHE assumption holds for $(\mathbb{G}, \mathbb{G}_T, e)$. The proposed $\mathcal{IBE}$ is ANON-ID-RCCA secure.*

Proof. We prove the ANON-ID-RCCA security of scheme $\mathcal{IBE}$ by constructing a serial of games G_0-G_4 and demonstrating the indistinguishability between them.

Game G_0: This is game $\mathbf{Exp}^{\mathsf{AIR}}_{\mathcal{A},\mathcal{IBE}}$. Let S_i denote the event that $(b, c) = (b', c')$ in game G_i, we have $\mathbf{Adv}^{\mathsf{AIR}}_{\mathcal{A},\mathcal{IBE}}(n) = |\Pr[S_0] - 1/4|$. We describe the modifications in each game G_1-G_4 as below.

Game G_1: This game is the same as G_0 except that the challenger runs AltSetup and AltExtract in Fig. 5 to generate system parameters and private key for adversary. Note that params is derived from tuple $\mathcal{G} = ([\beta], [\beta\alpha^{q+2}], [1], [\alpha], \cdots, [\alpha^q], Z)$ sampled from $\mathcal{R}_{ABDHE}$, which enables the challenger to compute the private keys without master key α. Particularly, $f_i(x)$ is a polynomial of degree q and $F_{\mathsf{ID},i}(x) = (f_i(x) - f_i(\mathsf{ID}))/(x - \mathsf{ID})$ is a $(q-1)$-degree polynomial. The values of $[f_i(\alpha)]$ and $[F_{\mathsf{ID},i}(\alpha)]$ could be derived from $[1], [\alpha], \cdots, [\alpha^q]$. The private key generated from AltExtract is valid, as $[h_{\mathsf{ID},i}] = [(f_i(\alpha) - f_i(\mathsf{ID}))/(\alpha - \mathsf{ID})] = [(h_i - r_{\mathsf{ID},i})/(\alpha - \mathsf{ID})]$.

Since tuple $\mathcal{G}$, randomness z_0, z_1 and polynomial $f_i(x)$ are uniformly picked at random, the distribution of params is identical to that in game G_0. Let $\mathcal{Q}$ denote all the identities queried by $\mathcal{A}$ and $\mathcal{I} = \{\alpha, \mathsf{ID}_b\} \cup \mathcal{Q}$. Since $f_i(x)$ is a uniformly random q-degree polynomial and $|\mathcal{I}| = q$, the values in $\{f_i(a)\}_{a \in \mathcal{I}}$ are uniformly random and independent in $\mathcal{A}$'s view. Thus, the distribution of private keys generated from AltExtract is identical to that in game G_0. Besides, $[\mathsf{ID}] = [\alpha]$ if and only if $\mathsf{ID} = \alpha$. So, game G_1 is actually identical to G_0.

We call a ciphertext ζ under identity ID bad if 1) it cannot pass the validity check of Dec or 2) $\mathsf{ID} \notin \mathcal{Q}$ and at least one tuple in $\{([X_1], [X_2]_T), ([Y_1], [Y_2]_T), ([U_1], [U_2]_T), ([V_1], [V_2]_T)\}$ is randomly sampled from $\mathbb{G} \times \mathbb{G}_T$ unless ζ is a rerandomization of challenge ciphertext ζ^*.

Lemma 4.3. *The decryption oracles $\mathcal{O}_{\mathsf{D}}$ and $\mathcal{O}'_{\mathsf{D}}$ in game G_1 reject all the bad ciphertexts except with negligible probability.*

Proof. Querying a valid ciphertext generated using Enc under identity ID or generated with $\mathsf{sk}_{\mathsf{ID}}$ does not reveal more information about master key α. Let ζ be the first bad ciphertext queried by the adversary.

If $([X_1], [X_2]_T), ([Y_1], [Y_2]_T), ([U_1], [U_2]_T)$ or $([V_1], [V_2]_T)$ is randomly sampled from $\mathbb{G} \times \mathbb{G}_T$ and underlying $\mathsf{ID} \notin \mathcal{Q}$, we assume that $([X_1], [X_2]_T) \leftarrow\!\!\$\, \mathbb{G} \times \mathbb{G}_T$. The probability of $X_1 = \alpha_{\mathsf{ID}} X_2$ is negligible. Recall that $h_{\mathsf{ID},1} = (h_1 - r_{\mathsf{ID},1})/\alpha_{\mathsf{ID}}$, then $[\vec{X}_{1,2}\vec{K}_1]_T = [(X_1/\alpha_{\mathsf{ID}})h_1 + (X_2 - X_1/\alpha_{\mathsf{ID}})r_{\mathsf{ID},1}]_T$. Since $f_1(x)$ is a q-degree polynomial, $r_{\mathsf{ID},1} = f_1(\mathsf{ID})$ is uniformly random in $\mathcal{A}$'s view. Thus, $[\vec{X}_{1,2}\vec{K}_1]_T$ is uniformly distributed in $\mathcal{A}$'s view. Similarly, $[\vec{Y}_{1,2}\vec{K}_1]_T$ (resp. $[\vec{U}_{1,2}\vec{K}_6]_T$, $[\vec{V}_{1,2}\vec{K}_6]_T$) is also uniformly random in $\mathcal{A}$'s view when $([Y_1], [Y_2]_T)$ (resp. $([U_1], [U_2]_T)$,

$\mathsf{AltEnc}(\mathsf{ID}, \mathsf{sk}_{\mathsf{ID}}, m \in \mathbb{G}_T)$

$([X_1], [X_2]_T), ([Y_1], [Y_2]_T), ([U_1], [U_2]_T), ([V_1], [V_2]_T) \leftarrow\!\!\$\ \mathbb{G} \times \mathbb{G}_T$

$u \leftarrow\!\!\$\ \mathbb{G}_T;\ \mu := H(m);\ \vec{\mu} := (1, \mu);\ \sigma := H(u)$

$\vec{X} := ([X_1], [X_2]_T, m \cdot [-\vec{X}_{1,2}\vec{K}_1]_T, [\sigma \vec{X}_{1,2}^{\dagger}\vec{K}_{2,3}\vec{\mu}^{\top}]_T, [\sigma \vec{X}_{1,2}^{\ddagger}\vec{K}_{4,5}\vec{\mu}^{\top}]_T)$

$\vec{Y} := ([Y_1], [Y_2]_T, [-\vec{Y}_{1,2}\vec{K}_1]_T, [\sigma \vec{Y}_{1,2}\vec{K}_{2,3}\vec{\mu}^{\top}]_T, [\sigma \vec{Y}_{1,2}\vec{K}_{4,5}\vec{\mu}^{\top}])$

$\vec{U} := ([U_1], [U_2]_T, u \cdot [-\vec{U}_{1,2}\vec{K}_6]_T, [\sigma \vec{U}_{1,2}\vec{K}_7]_T)$

$\vec{V} := ([V_1], [V_2]_T, [-\vec{V}_{1,2}\vec{K}_6]_T, [\sigma \vec{V}_{1,2}\vec{K}_7]_T);$ **return** $\zeta := (\vec{X}, \vec{Y}, \vec{U}, \vec{V})$

Figure 6: Alternative encryption algorithm AltEnc.

$([V_1], [V_2]_T))$ is randomly sampled from $\mathbb{G} \times \mathbb{G}_T$. In this case, the probability that ciphertext ζ is valid is negligible.

If ζ cannot pass the validity check of Dec, the oracles reject it, which rules out one possible value of master key α. Note that the number of decryption query is polynomial, while the size of master key space is superpolynomial, the probability of generating a valid bad ciphertext is negligible. ■

Game G_2: This game is the same as G_1 except that challenge ciphertext ζ^* is generated by alternative encryption algorithm AltEnc as shown in Fig. 6. Comparing to Enc, algorithm AltEnc picks random elements from $\mathbb{G} \times \mathbb{G}_T$ for $([X_1], [X_2]_T), ([Y_1], [Y_2]_T), ([U_1], [U_2]_T)$ and $([V_1], [V_2]_T)$, and uses private key $\mathsf{sk}_{\mathsf{ID}}$ to compute corresponding values.

Lemma 4.4. *Games* G_1 *and* G_2 *are computationally indistinguishable if truncated decision* q*-ABDHE assumption holds for* $(\mathbb{G}, \mathbb{G}_T, e)$.

Proof. Let $\mathsf{G}_{1,0}$ denote the game that generates challenge ciphertext ζ^* using private key $\mathsf{sk}_{\mathsf{ID}_b^*}$. Game $\mathsf{G}_{1,1}$ is the same as $\mathsf{G}_{1,0}$ except that $([X_1^*], [X_2^*]_T)$ in ζ^* is randomly sampled from $\mathbb{G} \times \mathbb{G}_T$. Game $\mathsf{G}_{1,2}$ is the same as $\mathsf{G}_{1,1}$ except that $([Y_1^*], [Y_2^*]_T)$ is randomly sampled. Game $\mathsf{G}_{1,3}$ is the same as $\mathsf{G}_{1,2}$ except that $([U_1^*], [U_2^*]_T)$ is randomly sampled. Game $\mathsf{G}_{1,4}$ is the same as $\mathsf{G}_{1,3}$ except that $([V_1^*], [V_2^*]_T)$ is randomly sampled. Obviously, game $\mathsf{G}_{1,0}$ is identical to G_1 by the decryption correctness, and game $\mathsf{G}_{1,4}$ is identical to G_2.

Next, we prove that game $\mathsf{G}_{1,0}$ is computationally indistinguishable from $\mathsf{G}_{1,1}$. Consider a random instance $([\beta], [\beta\alpha^{q+2}], [1], [\alpha], \cdots, [\alpha^q], Z)$ of truncated decision q-ABDHE assumption. The challenger simulates the Setup phase, decryption and extraction oracles as in game $\mathsf{G}_{1,0}$. In Challenge phase, only the computation of $[X_1^*]$ and $[X_2^*]_T$ in ζ^* is different from that in $\mathsf{G}_{1,0}$. Specifically, let $f'(x) = x^{q+2}$ and $F'_{\mathsf{ID}_b^*}(x) = (f'(x) - f'(\mathsf{ID}_b^*))/(x - \mathsf{ID}_b^*)$, the challenger sets

$$[X_1^*] = [\beta(f'(\alpha) - f'(\mathsf{ID}_b^*))] \qquad [X_2^*]_T = Z \cdot \left[\beta \textstyle\sum_{i=0}^{q} F'_{\mathsf{ID}_b^*,i}\alpha^i\right]_T$$

where $F'_{\mathsf{ID}_b^*,i}$ is the coefficient of x^i in $F'_{\mathsf{ID}_b^*}(x)$. Let $s = \beta F'_{\mathsf{ID}_b^*}(\alpha)$, we have $[X_1^*] = [s(\alpha - \mathsf{ID}_b^*)]$. Since β is uniformly distributed over $\mathbb{Z}_p$, s and $[X_1^*]$ are uniformly distributed over $\mathbb{Z}_p$ and $\mathbb{G}$ respectively. If $Z = [\beta\alpha^{q+1}]_T$, then $[X_2^*]_T = [s]_T$. The simulation is actually game $\mathsf{G}_{1,0}$. If Z is a random element uniformly sampled from $\mathbb{G}_T$, $[X_2^*]_T$ is uniformly distributed over $\mathbb{G}_T$. The simulation is game $\mathsf{G}_{1,1}$. Then, the indistinguishability between game $\mathsf{G}_{1,0}$ and $\mathsf{G}_{1,1}$ is reduced to the hardness of truncated decision q-ABDHE problem. Similarly, game $\mathsf{G}_{1,1}$(resp. $\mathsf{G}_{1,2}, \mathsf{G}_{1,3}$) is computationally indistinguishable from $\mathsf{G}_{1,2}$(resp. $\mathsf{G}_{1,3}, \mathsf{G}_{1,4}$). Finally, game G_1 is computationally indistinguishable from G_2. ■

Lemma 4.5. *Given system parameters* params *and set of private keys* $\{\mathsf{sk}_{\mathsf{ID}_i}\}_{\mathsf{ID}_i\in\mathcal{Q}}$ *in game* G_2*, for* $([X_1],[X_2]_T),([Y_1],[Y_2]_T)\leftarrow_{\$}\mathbb{G}\times\mathbb{G}_T$*, any* $\mathsf{ID}\notin\mathcal{Q}$*, any* $\mu,\sigma\in\mathbb{Z}_p$ *and any PPT adversary* $\mathcal{A}$*,* $([\vec{X}_{1,2}\vec{K}_1]_T,\ [\vec{Y}_{1,2}\vec{K}_1]_T)$ *and* $([\vec{X}_{4,5}]_T,\ [\vec{Y}_{4,5}]_T)$ *in algorithm* AltEnc *are uniformly distributed in* $\mathcal{A}$*'s view.*

Proof. Recall that $h_{\mathsf{ID},1}=(h_1-r_{\mathsf{ID},1})/\alpha_{\mathsf{ID}}$, then we rewrite $[\vec{X}_{1,2}\vec{K}_1]_T$ and $[\vec{Y}_{1,2}\vec{K}_1]_T$ as follows.

$$[\vec{X}_{1,2}\vec{K}_1]_T=[(X_1/\alpha_{\mathsf{ID}})h_1+(X_2-X_1/\alpha_{\mathsf{ID}})r_{\mathsf{ID},1}]_T$$
$$[\vec{Y}_{1,2}\vec{K}_1]_T=[(Y_1/\alpha_{\mathsf{ID}})h_1+(Y_2-Y_1/\alpha_{\mathsf{ID}})r_{\mathsf{ID},1}]_T$$

Since $f_1(x)$ is a q-degree polynomial and $|\{\alpha,\mathsf{ID}\}\cup\mathcal{Q}|=q$, then $r_{\mathsf{ID},1}=f_1(\mathsf{ID})$ is uniformly random in $\mathcal{A}$'s view. Thus, $([\vec{X}_{1,2}\vec{K}_1]_T,[\vec{Y}_{1,2}\vec{K}_1]_T)$ is uniformly distributed in $\mathcal{A}$'s view.

Let $\bar{\Theta}=\Theta_1/\alpha_{\mathsf{ID}}$, $\bar{\Theta}^{\dagger}=\bar{\Theta}_1+z_0$, $\bar{\Theta}^{\ddagger}=\bar{\Theta}_1+z_1$, $\hat{\Theta}=\Theta_2-\bar{\Theta}_1$ for $\Theta\in\{X,Y\}$ and $\vec{\mu}=(1,\mu)$. We rewrite $[\vec{X}_{4,5}]_T$ and $[\vec{Y}_{4,5}]_T$ as follows.

$$[\vec{X}_{4,5}]_T=([\sigma\bar{X}^{\dagger}\vec{\mu}\vec{h}_{2,3}^{\top}+\sigma\hat{X}\vec{\mu}\vec{r}_{\mathsf{ID},2,3}^{\top}]_T,[\sigma\bar{X}^{\ddagger}\vec{\mu}\vec{h}_{4,5}^{\top}+\sigma\hat{X}\vec{\mu}\vec{r}_{\mathsf{ID},4,5}^{\top}]_T)$$
$$[\vec{Y}_{4,5}]_T=([\sigma\bar{Y}\vec{\mu}\vec{h}_{2,3}^{\top}+\sigma\hat{Y}\vec{\mu}\vec{r}_{\mathsf{ID},2,3}^{\top}]_T,[\sigma\bar{Y}\vec{\mu}\vec{h}_{4,5}^{\top}+\sigma\hat{Y}\vec{\mu}\vec{r}_{\mathsf{ID},4,5}^{\top}]_T)$$

Consider that $\vec{\mu}\vec{r}_{\mathsf{ID},2,3}^{\top}=\vec{\mu}\vec{f}_{2,3}^{\top}(\mathsf{ID})$, $\vec{\mu}\vec{r}_{\mathsf{ID},4,5}^{\top}=\vec{\mu}\vec{f}_{4,5}^{\top}(\mathsf{ID})$ and $\mathcal{A}$ knows $[\vec{h}_{2,5}]=[\vec{f}_{2,5}(\alpha)]$ and $\{\vec{f}_{2,5}(\mathsf{ID}_i)\}_{\mathsf{ID}_i\in\mathcal{Q}}$, we represent these values as matrix product.

$$[\vec{c}_2\quad\vec{c}_3\quad\vec{c}_4\quad\vec{c}_5]\underbrace{\begin{bmatrix}\mathbf{V}&0&0&0&\vec{\gamma}_{\mathsf{ID}}&0\\0&\mathbf{V}&0&0&\mu\vec{\gamma}_{\mathsf{ID}}&0\\0&0&\mathbf{V}&0&0&\vec{\gamma}_{\mathsf{ID}}\\0&0&0&\mathbf{V}&0&\mu\vec{\gamma}_{\mathsf{ID}}\end{bmatrix}}_{:=\mathbf{P}},$$

where $\mathbf{V}=\begin{bmatrix}\vec{\gamma}_{\mathsf{ID}_1}&\vec{\gamma}_{\mathsf{ID}_2}&\cdots&\vec{\gamma}_{\mathsf{ID}_{q-2}}&\vec{\gamma}_{\alpha}\end{bmatrix}$, $\vec{\gamma}_x=(1,x,\cdots,x^q)^{\top}$ for $x\in\mathcal{Q}\cup\{\alpha,\mathsf{ID}\}$, $\vec{c}_i=(c_{i,0},c_{i,1},\cdots,c_{i,q})$ and $c_{i,j}$ is the coefficient of x^j in $f_i(x)$. Note that matrix $\mathbf{P}$ contains four $(q+1)\times(q-1)$ Vandermonde matrices whose columns are linearly independent. Since $\mathsf{ID}\notin\mathcal{Q}\cup\{\alpha\}$, $\vec{\gamma}_{\mathsf{ID}}$ is linearly independent of columns in $\mathbf{V}$. The columns of $\mathbf{P}$ are linearly independent. Thus, $([\vec{X}_{4,5}]_T,[\vec{Y}_{4,5}]_T)$ is uniformly distributed over $\mathbb{G}_T^2$ in $\mathcal{A}$'s view, as $\vec{\mu}\vec{r}_{\mathsf{ID},2,3}^{\top}$ and $\vec{\mu}\vec{r}_{\mathsf{ID},4,5}^{\top}$ are uniformly distributed in $\mathcal{A}$'s view. ■

Lemma 4.6. *If the decryption oracles in game* G_2 *reject all the bad ciphertexts except with negligible probability, given system parameters* params *and set of private keys* $\{\mathsf{sk}_{\mathsf{ID}_i}\}_{\mathsf{ID}_i\in\mathcal{Q}}$*, challenge ciphertext* ζ^* *in game* G_2 *is distributed independently of* ID_b^**,* m_c *and* u*.*

Proof. Since $([X_1^*],[X_2^*]_T),([Y_1^*],[Y_2^*]_T),([U_1^*],[U_2^*]_T)$ and $([V_1^*],[V_2^*]_T)$ are uniformly sampled from $\mathbb{G}\times\mathbb{G}_T$, by Lemma 4.5, $([X_3^*]_T/m_c,\ [Y_3^*]_T)$, $([U_3^*]_T/u,\ [V_3^*]_T)$, $([\vec{X}_{4,5}^*]_T,\ [\vec{Y}_{4,5}^*]_T)$ and $([U_4^*]_T,\ [V_4^*]_T)$ are uniformly distributed over appropriate domains in $\mathcal{A}$'s view, from which the lemma follows. ■

Game G_3: This game is the same as G_2 except that the challenger handles all the decryption queries with alternative decryption algorithm AltDec, as shown in Fig. 7, that only uses system parameters params, identity ID, challenge ciphertext $\zeta^*=(\vec{X}^*,\vec{Y}^*,\vec{U}^*,\vec{V}^*)$ and underlying identity ID_b^* to decrypt ciphertext. We now prove that G_2 and G_3 are statistically indistinguishable. In this case, AltDec in game G_3 is allowed to run in unbounded time, which is also the reason why AltDec could decrypt ciphertext with params, ID, ID_b^* and ζ^*.

Alternative Decryption Algorithm $\mathsf{AltDec}(\mathsf{ID}, \zeta, \mathsf{ID}_b^*, \zeta^*)$

(i) Check that there exist $\hat{s}, \hat{t} \in \mathbb{Z}_p$ such that $[U_2]_T = [\hat{s}]_T$, $[V_2] = [\hat{t}]_T$, $[U_1] = [\hat{s}\alpha_{\mathsf{ID}}]$ and $[V_1] = [\hat{t}\alpha_{\mathsf{ID}}]$. If not, go to (ii). Otherwise, compute $u = [U_3 + \hat{s}h_6]_T$, $\sigma = H(u)$ and check that $[\vec{V}_{3,4}]_T = ([-\hat{t}h_6]_T, [\sigma\hat{t}h_7]_T)$ and $[U_4]_T = [\sigma\hat{s}h_7]_T$ holds. If not, output $\perp$. Otherwise, check that there exist plaintext m, randomness $s, t \in \mathbb{Z}_p$ such that

$$\vec{X} = ([s\alpha_{\mathsf{ID}}], [s]_T, m \cdot [-sh_1]_T, [\sigma s^\dagger \vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma s^\ddagger \vec{\mu}\vec{h}_{4,5}^\top]_T)$$
$$\vec{Y} = ([t\alpha_{\mathsf{ID}}], [t]_T, [-th_1]_T, [\sigma t\vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma t\vec{\mu}\vec{h}_{4,5}^\top]_T),$$

where $\vec{\mu} = (1, H(m))$. If not, output $\perp$. If $m \notin \{m_0, m_1\}$, output m; otherwise output `replay`.

(ii) If AltDec is called in Phase 1, output $\perp$. Otherwise, check that there exist $\hat{s}', \hat{t}', s', t' \in \mathbb{Z}_p$ such that

$$\vec{U} = ([U_1^* + \hat{s}'V_1^*], [\vec{U}_{2,4}^* + \hat{s}'\vec{V}_{2,4}^*]_T);\ \vec{V} = ([\hat{t}'V_1^*], [\hat{t}'\vec{V}_{2,4}^*]_T)$$
$$\vec{X} = ([X_1^* + s'Y_1^*], [\vec{X}_{2,5}^* + s'\vec{Y}_{2,5}^*]_T);\ \vec{Y} = ([t'Y_1^*], [t'\vec{Y}_{2,5}^*]_T).$$

If not, output $\perp$. Otherwise, check that $\mathsf{ID} = \mathsf{ID}_b^*$. If not, output $\perp$; otherwise, output `replay`.

Figure 7: The alternative decryption algorithm AltDec.

Lemma 4.7. *Given system parameters* params*, set of private keys* $\{\mathsf{sk}_{\mathsf{ID}_i}\}_{\mathsf{ID}_i \in \mathcal{Q}}$*,* $([X_1^*], [X_2^*]_T)$*,* $([Y_1^*], [Y_2^*]_T) \in \mathbb{G} \times \mathbb{G}_T$ *and* $[\vec{X}_{4,5}^*]_T$*,* $[\vec{Y}_{4,5}^*]_T$ *with* $\mathsf{ID}^* \notin \mathcal{Q}$ *and* $\mu^*, \sigma^* \in \mathbb{Z}_p$ *in game* G_3*, for any* $([X_1], [X_2]_T) \in \mathbb{G} \times \mathbb{G}_T$*, any* $\mu, \sigma \in \mathbb{Z}_p$ *with* $([X_1], [X_2]_T) \notin \{([X_1^* + s'Y_1^*], [X_2^* + s'Y_2^*]_T)\}_{s' \in \mathbb{Z}_p}$*,* $\mu \neq \mu^*$ *or* $\sigma \notin \{\sigma'\sigma^*\}_{\sigma' \in \mathbb{Z}_p}$ *and any PPT adversary* $\mathcal{A}$*,* $[\vec{X}_{4,5}]_T$ *with* ID^**,* μ *and* σ *is uniformly distributed in* $\mathcal{A}$*'s view with overwhelming probability.*

Proof. Let $\bar{\Theta} = \Theta_1/\alpha_{\mathsf{ID}^*}$, $\bar{\Theta}^\dagger = \bar{\Theta}_1 + z_0$, $\bar{\Theta}^\ddagger = \bar{\Theta}_1 + z_1$ and $\hat{\Theta} = \Theta_2 - \bar{\Theta}_1$ for $\Theta \in \{X^*, Y^*, X\}$. We rewrite $[\vec{X}_{4,5}^*]_T$, $[\vec{Y}_{4,5}^*]_T$ and $[\vec{X}_{4,5}]_T$ as follows.

$$\begin{aligned}
[\vec{X}_{4,5}^*]_T = \ & ([\sigma^*(\bar{X}^*)^\dagger \vec{\mu}^* \vec{h}_{2,3}^\top + \sigma^* \hat{X}^* \vec{\mu}^* \vec{r}_{\mathsf{ID}^*,2,3}^\top]_T, [\sigma^*(\bar{X}^*)^\ddagger \vec{\mu}^* \vec{h}_{4,5}^\top + \sigma^* \hat{X}^* \vec{\mu}^* \vec{r}_{\mathsf{ID}^*,4,5}^\top]_T) \\
[\vec{Y}_{4,5}^*]_T = \ & ([\sigma^* \bar{Y}^* \vec{\mu}^* \vec{h}_{2,3}^\top + \sigma^* \hat{Y}^* \vec{\mu}^* \vec{r}_{\mathsf{ID}^*,2,3}^\top]_T, [\sigma^* \bar{Y}^* \vec{\mu}^* \vec{h}_{4,5}^\top + \sigma^* \hat{Y}^* \vec{\mu}^* \vec{r}_{\mathsf{ID}^*,4,5}^\top]_T) \\
[\vec{X}_{4,5}]_T = \ & ([\sigma \bar{X}^\dagger \vec{\mu} \vec{h}_{2,3}^\top + \sigma \hat{X} \vec{\mu} \vec{r}_{\mathsf{ID}^*,2,3}^\top]_T, [\sigma \bar{X}^\ddagger \vec{\mu} \vec{h}_{4,5}^\top + \sigma \hat{X} \vec{\mu} \vec{r}_{\mathsf{ID}^*,4,5}^\top]_T
\end{aligned}$$

Besides, $\mathcal{A}$ also knows $[\vec{h}_{2,5}] = [\vec{f}_{2,5}(\alpha)]$ and $\{\vec{f}_{2,5}(\mathsf{ID}_i) : \mathsf{ID}_i \in \mathcal{Q}\}$. We represent these values as following matrix product.

$$\vec{c} \underbrace{\begin{bmatrix}
\mathbf{V} & 0 & 0 & 0 & \sigma^*\vec{\Gamma}^\dagger_{X^*} & 0 & \sigma^*\vec{\Gamma}_{Y^*} & 0 & \sigma\vec{\Gamma}^\dagger_X & 0 \\
0 & \mathbf{V} & 0 & 0 & \mu^*\sigma^*\vec{\Gamma}^\dagger_{X^*} & 0 & \mu^*\sigma^*\vec{\Gamma}_{Y^*} & 0 & \mu\sigma\vec{\Gamma}^\dagger_X & 0 \\
0 & 0 & \mathbf{V} & 0 & 0 & \sigma^*\vec{\Gamma}^\ddagger_{X^*} & 0 & \sigma^*\vec{\Gamma}_{Y^*} & 0 & \sigma\vec{\Gamma}^\ddagger_X \\
0 & 0 & 0 & \mathbf{V} & 0 & \mu^*\sigma^*\vec{\Gamma}^\ddagger_{X^*} & 0 & \mu^*\sigma^*\vec{\Gamma}_{Y^*} & 0 & \mu\sigma\vec{\Gamma}^\ddagger_X
\end{bmatrix}}_{:=\mathbf{P}},$$

where $\vec{c} = [\vec{c}_2\ \vec{c}_3\ \vec{c}_4\ \vec{c}_5]$, $\vec{c}_i = (c_{i,0}, c_{i,1}, \cdots, c_{i,q})$ and $c_{i,j}$ is the coefficient of x^j in $f_i(x)$, $\mathbf{V} = \begin{bmatrix}\vec{\gamma}_{\mathsf{ID}_1} & \vec{\gamma}_{\mathsf{ID}_2} & \cdots & \vec{\gamma}_{\mathsf{ID}_{q-2}} & \vec{\gamma}_\alpha\end{bmatrix}$, $\vec{\gamma}_x = (1, x, \cdots, x^q)^\top$ for $x \in \mathcal{Q} \cup \{\alpha, \mathsf{ID}^*\}$, $\vec{\Gamma}^\dagger_\Theta = \bar{\Theta}^\dagger\vec{\gamma}_\alpha + \hat{\Theta}\vec{\gamma}_{\mathsf{ID}^*}$, $\vec{\Gamma}^\ddagger_\Theta = \bar{\Theta}^\ddagger\vec{\gamma}_\alpha + \hat{\Theta}\vec{\gamma}_{\mathsf{ID}^*}$ for $\Theta \in \{X^*, X\}$ and $\vec{\Gamma}_{Y^*} = \bar{Y}^*\vec{\gamma}_\alpha + \hat{Y}^*\vec{\gamma}_{\mathsf{ID}^*}$. Next, we discuss the linear independence of columns in matrix $\mathbf{P}$ as follows.

- If $\mu \neq \mu^*$, it is obvious that columns in $\mathbf{P}$ are linearly independent.

- If $\mu = \mu^*$ and $\sigma \notin \{\sigma'\sigma^*\}_{\sigma' \in \mathbb{Z}_p}$. Assume that columns in $\mathbf{P}$ are linearly dependent. Recall that $\vec{\gamma}_{\mathsf{ID}^*}$ is not a linear combination of columns in $\mathbf{V}$, then there must exist $\sigma' \in \mathbb{Z}_p$ such that $\sigma = \sigma'\sigma^*$, which is contradict to current case. Thus, $\mathbf{P}$ is non-singular.
- If $\mu = \mu^*$, $\exists \sigma' \in \mathbb{Z}_p$ *s.t.* $\sigma = \sigma'\sigma^*$ and $([X_1], [X_2]_T) \notin \{([X_1^* + s'Y_1^*], [X_2^* + s'Y_2^*]_T)\}_{s' \in \mathbb{Z}_p}$. Assume that $([X_1], [X_2]_T) = ([aX_1^* + bY_1^* + (\alpha - \mathsf{ID}^*)s], [aX_2^* + bY_2^* + s]_T)$ with $a \neq 1$ or $s \neq 0$, we have
$$\sigma\vec{\Gamma}_X^{\dagger} = a\sigma'\sigma^*\vec{\Gamma}_{X^*}^{\dagger} + b\sigma'\sigma^*\vec{\Gamma}_{Y^*} + \sigma(s + (1-a)z_0)\vec{\gamma}_\alpha$$
$$\sigma\vec{\Gamma}_X^{\ddagger} = a\sigma'\sigma^*\vec{\Gamma}_{X^*}^{\ddagger} + b\sigma'\sigma^*\vec{\Gamma}_{Y^*} + \sigma(s + (1-a)z_1)\vec{\gamma}_\alpha$$
Note that σ^* is uniformly distributed in $\mathcal{A}$'s view. Coefficients $(s + (1-a)z_0)$ and $(s + (1-a)z_1)$ should equal to 0 simultaneously, which is contradict to $a \neq 1$ or $s \neq 0$. In this case, columns in $\mathbf{P}$ are linearly independent

■

Lemma 4.8. *Given system parameters* params*, set of private keys* $\{\mathsf{sk}_{\mathsf{ID}_i}\}_{\mathsf{ID}_i \in \mathcal{Q}}$*,* $([Y_1^*], [Y_2^*]_T) \in \mathbb{G} \times \mathbb{G}_T$ *and* $[\vec{Y}_{4,5}^*]_T$ *with* $\mathsf{ID}^* \notin \mathcal{Q}$ *and* $\mu^*, \sigma^* \in \mathbb{Z}_p$*, for any* $([Y_1], [Y_2]_T) \in \mathbb{G} \times \mathbb{G}_T$*, any* $\mu, \sigma \in \mathbb{Z}_p$ *with* $([Y_1], [Y_2]_T) \notin \{([t'Y_1^*], [t'Y_2^*]_T)\}_{t' \in \mathbb{Z}_p}$*,* $\mu \neq \mu^*$ *or* $\sigma \notin \{\sigma'\sigma^*\}_{\sigma' \in \mathbb{Z}_p}$ *and any PPT adversary* $\mathcal{A}$*,* $[\vec{Y}_{4,5}]_T$ *with* ID^**,* μ *and* σ *is uniformly distributed in* $\mathcal{A}$*'s view with overwhelming probability.*

Proof. Let $\bar{\Theta} = \Theta_1/\alpha_{\mathsf{ID}^*}$ and $\hat{\Theta} = \Theta_2 - \bar{\Theta}_1$ for $\Theta \in \{Y^*, Y\}$. We rewrite $[\vec{Y}_{4,5}^*]_T$ and $[\vec{Y}_{4,5}]_T$ as follows.

$$\begin{aligned}
[\vec{Y}_{4,5}^*]_T = \;& ([\sigma^*\bar{Y}^*\vec{\mu}^*\vec{h}_{2,3}^{\top} + \sigma^*\hat{Y}^*\vec{\mu}^*\vec{r}_{\mathsf{ID}^*,2,3}^{\top}]_T, [\sigma^*\bar{Y}^*\vec{\mu}^*\vec{h}_{4,5}^{\top} + \sigma^*\hat{Y}^*\vec{\mu}^*\vec{r}_{\mathsf{ID}^*,4,5}^{\top}]_T) \\
[\vec{Y}_{4,5}]_T = \;& ([\sigma\bar{Y}\vec{\mu}\vec{h}_{2,3}^{\top} + \sigma\hat{Y}\vec{\mu}\vec{r}_{\mathsf{ID}^*,2,3}^{\top}]_T, [\sigma\bar{Y}\vec{\mu}\vec{h}_{4,5}^{\top} + \sigma\hat{Y}\vec{\mu}\vec{r}_{\mathsf{ID}^*,4,5}^{\top}]_T)
\end{aligned}$$

Besides, $\mathcal{A}$ also knows $[\vec{h}_{2,5}] = [\vec{f}_{2,5}(\alpha)]$ and $\{\vec{f}_{2,5}(\mathsf{ID}_i)\}_{\mathsf{ID}_i \in \mathcal{Q}}$. We represent these values as following matrix product.

$$\begin{bmatrix} \vec{c}_2 & \vec{c}_3 & \vec{c}_4 & \vec{c}_5 \end{bmatrix} \underbrace{\begin{bmatrix} \mathbf{V} & 0 & 0 & 0 & \sigma^*\vec{\Gamma}_{Y^*} & 0 & \sigma\vec{\Gamma}_Y^{\dagger} & 0 \\ 0 & \mathbf{V} & 0 & 0 & \mu^*\sigma^*\vec{\Gamma}_{Y^*} & 0 & \mu\sigma\vec{\Gamma}_Y^{\dagger} & 0 \\ 0 & 0 & \mathbf{V} & 0 & 0 & \sigma^*\vec{\Gamma}_{Y^*} & 0 & \sigma\vec{\Gamma}_Y^{\ddagger} \\ 0 & 0 & 0 & \mathbf{V} & 0 & \mu^*\sigma^*\vec{\Gamma}_{Y^*} & 0 & \mu\sigma\vec{\Gamma}_Y^{\ddagger} \end{bmatrix}}_{:=\mathbf{P}},$$

where $\vec{c}_i = (c_{i,0}, c_{i,1}, \cdots, c_{i,q})$ and $c_{i,j}$ is the coefficient of x^j in $f_i(x)$, $\vec{V} = \begin{bmatrix} \vec{\gamma}_{\mathsf{ID}_1} & \vec{\gamma}_{\mathsf{ID}_2} & \cdots & \vec{\gamma}_{\mathsf{ID}_{q-2}} & \vec{\gamma}_\alpha \end{bmatrix}$, $\vec{\gamma}_x = (1, x, \cdots, x^q)^{\top}$ for $x \in \mathcal{Q} \cup \{\alpha, \mathsf{ID}^*\}$ and $\vec{\Gamma}_\Theta = \bar{\Theta}\vec{\gamma}_\alpha + \hat{\Theta}\vec{\gamma}_{\mathsf{ID}^*}$ for $\Theta \in \{Y^*, Y\}$. Next, we discuss the linear independence of columns in matrix $\mathbf{P}$ as follows.

- If $\mu \neq \mu^*$, it is obvious that columns in $\mathbf{P}$ are linearly independent.
- If $\mu = \mu^*$ and $\sigma \notin \{\sigma'\sigma^*\}_{\sigma' \in \mathbb{Z}_p}$. Assume that columns in $\mathbf{P}$ are linearly dependent. Recall that $\vec{\gamma}_{\mathsf{ID}^*}$ is not a linear combination of columns in $\mathbf{V}$, then there must exist $\sigma' \in \mathbb{Z}_p$ such that $\sigma = \sigma'\sigma^*$, which is contradict to current case. Thus, $\mathbf{P}$ is non-singular.
- If $\mu = \mu^*$, $\exists \sigma' \in \mathbb{Z}_p$ *s.t.* $\sigma = \sigma'\sigma^*$ and $([Y_1], [Y_2]_T) \notin \{([t'Y_1^*], [t'Y_2^*]_T)\}_{t' \in \mathbb{Z}_p}$. Assume that $([Y_1], [Y_2]_T) = ([aY_1^* + s\alpha_{\mathsf{ID}}^*], [aY_2^* + s]_T)$ with $s \neq 0$, we have $\sigma\vec{\Gamma}_Y = a\sigma'\sigma^*\vec{\Gamma}_{Y^*} + \sigma s\vec{\gamma}_\alpha$. Note that σ^* is uniformly distributed in $\mathcal{A}$'s view, so is coefficient σs. In this case, columns in $\mathbf{P}$ are linearly independent in $\mathcal{A}$'s view.

■

Lemma 4.9. *The response of challenger to decryption query in game* G_3 *agrees with the response to decryption query in game* G_2*.*

Proof. In the cases where the response to decryption query in G_3 is plaintext m, the response in G_2 is also m by the correctness of decryption. Analogously, in the cases where the response to decryption query in G_3 is `replay`, the response in G_2 is also `replay` by the correctness of decryption and rerandomization.

We now prove that when challenger answers decryption query in G_3 with special symbol $\perp$, challenger in G_2 would also return $\perp$ with overwhelming probability. That is, when AltDec outputs $\perp$, Dec would also output $\perp$ with overwhelming probability. Let $\zeta^* = (\vec{X}^*, \vec{Y}^*, \vec{U}^*, \vec{V}^*)$ denote the challenge ciphertext under identity ID_b^* and $\langle \mathsf{ID}, \zeta = (\vec{X}, \vec{Y}, \vec{U}, \vec{V}) \rangle$ denote the decryption query input. We consider all the possible cases where AltDec outputs $\perp$ as follows.

In step (i), there are four cases where AltDec rejects ζ under ID.

- Checks on $[\vec{V}_{3,4}]_T$ and $[U_4]_T$ do not hold. Obviously, Dec would reject ζ.
- $(X_1, Y_1) \neq (X_2\alpha_{\mathsf{ID}}, Y_2\alpha_{\mathsf{ID}})$ in Phase 1. By Lemma 4.5, $[\vec{X}_{4,5}]_T$ or $[\vec{Y}_{4,5}]_T$ is uniformly distributed in $\mathcal{A}$'s view.
- $(X_1, Y_1) \neq (X_2\alpha_{\mathsf{ID}}, Y_2\alpha_{\mathsf{ID}})$ in Phase 2. If there exist $s', t' \in \mathbb{Z}_p$ such that $([X_1], [X_2]_T) = ([X_1^* + s'Y_1^*], [X_2^* + s'Y_2^*]_T)$ and $([Y_1], [Y_2]_T) = ([t'Y_1^*], [t'Y_2^*]_T)$, then the underlying u of ζ would be related to u^* in ζ^*. However, u^* is uniformly distributed over $\mathbb{G}_T$. The correct value of u is unknown to $\mathcal{A}$. Thus, the validity check on ζ would fail. Otherwise, given $[\vec{X}_{4,5}^*]_T$, $[\vec{Y}_{4,5}^*]_T$, the value of $[\vec{X}_{4,5}]_T$ is uniformly distributed over $\mathbb{G}_T^2$ in $\mathcal{A}$'s view by Lemma 4.7.
- $(X_1, Y_1) = (X_2\alpha_{\mathsf{ID}}, Y_2\alpha_{\mathsf{ID}})$ but checks on $[\vec{X}_{4,5}]_T$, $[\vec{Y}_{4,5}]_T$ and $[Y_3]_T$ do not hold in Phase 1 and 2 for any $m \in \mathbb{G}_T$. The validity check on ζ in Dec fails.

In step (ii), there are following cases where AltDec rejects ζ under ID.

- $(U_1, V_1) \neq (U_2\alpha_{\mathsf{ID}}, V_2\alpha_{\mathsf{ID}})$ in Phase 1. By Lemma 4.5, $[U_3]_T/u$ or $[V_3]_T$ is uniformly distributed over $\mathbb{G}_T$ in $\mathcal{A}$'s view.
- $([U_1], [U_2]_T) \neq ([aU_1^* + bV_1^* + \alpha_{\mathsf{ID}^*}s], [aU_2^* + bV_2^* + s]_T)$ or $([V_1], [V_2]_T) \neq ([aV_1^* + \alpha_{\mathsf{ID}^*}s], [aV_2^* + s]_T)$ for any $a, b, s \in \mathbb{Z}_p$. By Lemma 4.5, $[U_3]_T/u$, $[U_4]_T$ or $[\vec{V}_{3,4}]_T$ is uniformly distributed in $\mathcal{A}$'s view.
- $([U_1], [U_2]_T) = ([aU_1^* + bV_1^* + \alpha_{\mathsf{ID}^*}s], [aU_2^* + bV_2^* + s]_T)$ with $a \neq 1$ or $s \neq 0$. If $a \neq 1$, then $[U_3]_T = [aU_3^* + bV_3^* - sh_6]_T/(u^*)^{a-1}$ is uniformly distributed in $\mathcal{A}$'s view, as u^* is uniformly distributed over $\mathbb{G}_T$. If $a = 1$ and $s \neq 0$, then $[U_4]_T = [\sigma'(U_4^* + bV_4^* + \sigma^* sh_7)]_T$ is also uniformly distributed in $\mathcal{A}$'s view, as $\sigma^* = H(u^*)$ is uniformly distributed over $\mathbb{Z}_p$.
- $([V_1], [V_2]_T) = ([aV_1^* + \alpha_{\mathsf{ID}^*}s], [aV_2^* + s]_T)$ with $s \neq 0$. Similarly, $[V_4]_T = [aV_4^* + \sigma^* sh_7]_T$ is uniformly distributed in $\mathcal{A}$'s view, as σ^* is uniformly distributed over $\mathbb{Z}_p$.
- $[\vec{U}_{3,4}]_T$, $[V_4]_T$ do not hold for any $u' \in \mathbb{G}_T$. In this case, Dec would reject ζ.
- s' or $t' \in \mathbb{Z}_p$ does not exist. By Lemma 4.7 and 4.8, $[\vec{X}_{4,5}]_T$ or $[\vec{Y}_{4,5}]_T$ is uniformly distributed in $\mathcal{A}$'s view.
- $\mathsf{ID} \neq \mathsf{ID}_b^*$. Obviously, Dec would reject ζ.

In conclusion, the output of AltDec in G_3 is the same as that of Dec in G_2 in every case with overwhelming probability. ∎

Lemma 4.10. $\Pr[S_3] = 1/4$.

Proof. Note that $\mathsf{AltExtract}$ does not use the master key to generate the private key and AltDec does not use the private key to perform the decryption. The extraction and decryption queries do not provide extra information about master key and private keys to adversary $\mathcal{A}$. Lemma 4.6 shows that ζ^* is distributed independently of bits b, c, from which the lemma follows. ■

Putting it all together, the theorem follows. ■

Below we analyse the rerandomizability of $\mathcal{IBE}$.

Theorem 4.11 (Rerandomizability)**.** *Let q_{ID} be the times of extraction queries in game $\mathbf{Exp}^{\mathsf{Re}}_{\mathcal{A},\mathcal{IBE}}$, as shown in Fig. 3, and $q = q_{\mathsf{ID}} + 2$. If the truncated decision q-ABDHE assumption holds for $(\mathbb{G}, \mathbb{G}_T, e)$, the proposed $\mathcal{IBE}$ is rerandomizable.*

Proof. Below we prove the three conditions specified in Definition 4.3.

(Correctness) For $(\mathsf{msk}, \mathsf{params}) \leftarrow\!\!\$\ \mathsf{Setup}(1^n)$, any $\mathsf{ID} \in \mathbb{Z}_p$ and $\mathsf{sk}_{\mathsf{ID}} = \mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$, any ciphertext $\zeta = (\vec{X}, \vec{Y}, \vec{U}, \vec{V})$, $\zeta' = (\vec{X}', \vec{Y}', \vec{U}', \vec{V}') = \mathsf{Rerand}(\zeta)$ and $m = \mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \zeta)$, if $m \neq \perp$, then ζ passes the validity check in Dec. Also, we have $m = [X_3 + \vec{X}_{1,2}\vec{K}_1]_T$ and $u = [U_3 + \vec{U}_{1,2}\vec{K}_6]_T$. One can verify that $m = [X'_3 + \vec{X}'_{1,2}\vec{K}_1]_T$ and $u = [U'_3 + \vec{U}'_{1,2}\vec{K}_6]_T$. ζ' also can pass the validity check and $\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \zeta') = m$. If $m = \perp$, ζ fails the validity check. One can verify that ζ' also would not pass the validity check. Thus, $\mathsf{Dec}(\mathsf{sk}_{\mathsf{ID}}, \zeta') = \perp$.

(Tightness of Decryption) The proof of Lemma 4.3 shows that conditioned on system parameters, the probability of adversary $\mathcal{A}$ generating a valid bad ciphertext is negligible, from which the tightness of decryption follows.

(Indistinguishability) We construct a serial of games to prove that the advantage of adversary $\mathcal{A}$ winning game $\mathbf{Exp}^{\mathsf{Re}}_{\mathcal{A},\mathcal{IBE}}$ is negligible. Let S_i denote the event that $b = b'$ in game G_i.

Game G_0: This is the game $\mathbf{Exp}^{\mathsf{Re}}_{\mathcal{A},\mathcal{IBE}}$. Let S_i denote the event that $b = b'$ in game G_1. In game G_0, the advantage of PPT adversary $\mathcal{A}$ is $|\Pr[S_0] - 1/2|$.

Game G_1: This game is the same as G_0 except that the challenger runs $\mathsf{AltSetup}$ and $\mathsf{AltExtract}$ in Fig. 5 to generate system parameters and private key for $\mathcal{A}$. According to the analysis in Theorem 4.2, game G_1 is identical to G_0.

Game G_2: This game is the same as G_1 except that ciphertext ζ_0 is generated using AltEnc in Fig. 6. By Lemma 4.4 in Theorem 4.2, games G_1 and G_2 are computationally indistinguishable if truncated decision q-ABDHE assumption holds for $(\mathbb{G}, \mathbb{G}_T, e)$.

Game G_3: This game is the same as G_2 except that ciphertext ζ_0 is generated by AltEnc^*. The only difference between AltEnc and AltEnc^* is the choice of mask u. Specifically, u in AltEnc is randomly sampled from $\mathbb{G}_T$, while u in AltEnc^* equals to the underlying mask of ζ generated by $\mathcal{A}$. That is, u in AltEnc^* is determined by $\mathcal{A}$. By Lemma 4.6, we have ζ_0 in G_2 is distributed independently of underlying ID, m and u, which implies that $\mathcal{A}$'s choice of u would not affect the distribution of ζ_0 in G_3. Thus, game G_3 is identical to G_2.

Game G_4: This game is the same as G_3 except that the challenger handles all the decryption queries with AltDec^* that only uses system parameter params, identity ID_i and challenge ciphertext ζ_b under identity ID to decrypt ciphertext. In this case, AltDec^* in G_4 is allowed to run in unbounded time, which is also the reason why AltDec^* could decrypt ciphertext ζ_i with params and ID_i. Let m denote the underlying plaintext of ζ. For any decryption query ID_i and ζ_i, we describe algorithm AltDec^* as shown in Fig. 8.

Alternative Decryption Algorithm $\mathsf{AltDec}^*(\mathsf{ID}_i, \zeta_i := (\vec{X}, \vec{Y}, \vec{U}, \vec{V}))$

Check that there exist $\hat{s}, \hat{t} \in \mathbb{Z}_p$ such that $[U_2]_T = [\hat{s}]_T$, $[V_2] = [\hat{t}]_T$, $[U_1] = [\hat{s}\alpha_{\mathsf{ID}_i}]$ and $[V_1] = [\hat{t}\alpha_{\mathsf{ID}_i}]$. If not, output $\perp$. Otherwise, compute $u = [U_3 + \hat{s}h_6]_T$, $\sigma = H(u)$ and check that $[\vec{V}_{3,4}]_T = ([-\hat{t}h_6]_T, [\sigma\hat{t}h_7]_T)$ and $[U_4]_T = [\sigma\hat{s}h_7]_T$ holds. If not, output $\perp$. Otherwise, check that there exist plaintext m', randomness $s, t \in \mathbb{Z}_p$ such that

$$\vec{X} = ([s\alpha_{\mathsf{ID}_i}], [s]_T, m' \cdot [-sh_1]_T, [\sigma s^\dagger \vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma s^\ddagger \vec{\mu}\vec{h}_{4,5}^\top]_T)$$
$$\vec{Y} = ([t\alpha_{\mathsf{ID}_i}], [t]_T, [-th_1]_T, [\sigma t\vec{\mu}\vec{h}_{2,3}^\top]_T, [\sigma t\vec{\mu}\vec{h}_{4,5}^\top]_T),$$

where $\vec{\mu} = (1, H(m'))$. If not, output $\perp$. If $m' \neq m^*$, output m'; otherwise output $\perp$.

Figure 8: The alternative decryption algorithm AltDec^*.

Lemma 4.12. *The output of alternative decryption algorithm* AltDec^* *in game* G_4 *agrees with the output of decryption oracles* $\mathcal{O}_\mathsf{D}$ *and* $\mathcal{O}'_\mathsf{D}$ *in game* G_3.

Proof. In the cases where the output of AltDec^* in game G_4 is plaintext $m'(m' \neq m^*)$, the output of oracle $\mathcal{O}_\mathsf{D}(\mathcal{O}'_\mathsf{D})$ is also m' by the correctness of decryption. Now we prove that when the output of AltDec^* in game G_4 is special symbol $\perp$, decryption oracle in G_3 would also return $\perp$ with overwhelming probability.

Let $\zeta_b = (\vec{X}^*, \vec{Y}^*, \vec{U}^*, \vec{V}^*)$ denote the challenge ciphertext under identity ID and $\langle \mathsf{ID}_i, \zeta_i = (\vec{X}, \vec{Y}, \vec{U}, \vec{V})\rangle$ denote the decryption query input. We consider all the possible cases where AltDec^* outputs $\perp$ as follows.

- Validity checking failed. In this case, decryption oracle in G_3 also outputs $\perp$.
- Decryption result equals to m^*. Obviously, oracle in G_3 also outputs $\perp$.
- $s, t, \hat{s}$ or $\hat{t}$ does not exist. That is, $([X_1], [Y_1], [U_1], [V_1]) \neq ([X_2\alpha_{\mathsf{ID}_i}], [Y_2\alpha_{\mathsf{ID}_i}], [U_2\alpha_{\mathsf{ID}_i}], [V_2\alpha_{\mathsf{ID}_i}])$.
  - If $b = 0$, then $([X_1^*], [Y_1^*], [U_1^*], [V_1^*]) \neq ([X_2^*\alpha_\mathsf{ID}], [Y_2^*\alpha_\mathsf{ID}], [U_2^*\alpha_\mathsf{ID}], [V_2^*\alpha_\mathsf{ID}])$, as ζ_b is generated using AltEnc^*.
    - If $([X_1], [X_2]_T) \neq ([aX_1^* + bY_1^* + \alpha_\mathsf{ID}s], [aX_2^* + bY_2^* + s]_T)$, $([Y_1], [Y_2]_T) \neq ([aY_1^* + \alpha_\mathsf{ID}s], [aY_2^* + s]_T)$, $([U_1], [U_2]_T) \neq ([cU_1^* + dV_1^* + \alpha_\mathsf{ID}t], [cU_2^* + dV_2^* + t]_T)$ or $([V_1], [V_2]_T) \neq ([cV_1^* + \alpha_\mathsf{ID}t], [cV_2^* + t]_T)$ for any $a, b, c, d, s, t \in \mathbb{Z}_p$. By Lemma 4.5, $[X_3]_T/m'$, $[\vec{X}_{4,5}]_T$, $[\vec{Y}_{3,5}]_T$, $[U_3]_T/u$, $[U_4]_T$ or $[\vec{V}_{3,4}]_T$ is uniformly distributed in $\mathcal{A}$'s view.
    - Otherwise, ζ_i is derived from ζ_b and the underlying plaintext of ζ_i must be m^*.
  - If $b = 1$, then ζ_b is a rerandomization of ζ^* generated by $\mathcal{A}$. Since $m^* = \mathsf{Dec}(\mathsf{sk}_\mathsf{ID}, \zeta^*) \neq \perp$, we have $([X_1^*], [Y_1^*], [U_1^*], [V_1^*]) = ([X_2^*\alpha_\mathsf{ID}], [Y_2^*\alpha_\mathsf{ID}], [U_2^*\alpha_\mathsf{ID}], [V_2^*\alpha_\mathsf{ID}])$, otherwise, $[\vec{X}_{4,5}^*]_T$, $[\vec{Y}_{3,5}^*]_T$, $[U_4^*]_T$ or $[\vec{V}_{3,4}^*]_T$ is uniformly distributed over appropriate domains by Lemma 4.5. Again, since $s, t, \hat{s}$ or $\hat{t}$ does not exist, $[\vec{X}_{4,5}]_T$, $[\vec{Y}_{3,5}]_T$, $[U_4]_T$ or $[\vec{V}_{3,4}]_T$ is uniformly distributed in $\mathcal{A}$'s view from Lemma 4.5.

In conclusion, the output of AltDec^* in G_4 is the same as that of decryption oracles in G_3 in every case with overwhelming probability. ■

Lemma 4.13. $\Pr[S_4] = 1/2$.

Proof. Note that $\mathsf{AltExtract}$ does not use master key to generate private key and AltDec does not use private key to perform decryption. The extraction and decryption queries do not provide extra information about master key and private keys to adversary $\mathcal{A}$. The distribution of the encryptions of particular message is determined by randomnesses $s, t, \hat{s}, \hat{t}$ and mask u. One can note that in algorithms Rerand, randomnesses are rerandomized to $s + s't$, $t't$, $\hat{s} + \hat{s}'\hat{t}$, $\hat{t}'\hat{t}$ respectively. Since $s', t', \hat{s}', \hat{t}'$ are uniformly picked from appropriate domains and ζ_0, ζ_1 share same mask u, the distribution of ζ_1 is identical to that of ζ_0, from which the lemma follows. ■

Put it all together, the theorem follows. ■

5 An Application: Identity-based Universal Mixnet

In this section, we show that rerandomizable ANON-ID-RCCA secure IBE scheme could be useful in practice by presenting an application example.

5.1 Definitions

Universal mixnet is usually constructed for providing externally anonymous communications among parties [13, 14, 17]. That is, a set of senders intends to communicate with their recipients in such a way that nobody could identify a particular communication except the sender and recipient of this communication.

Here we consider an ID-based universal mix network with ℓ mix-servers $\{M_i\}_{i=1}^{\ell}$, n senders $\{S_i\}_{i=1}^{n}$ and n receivers $\{R_i\}_{i=1}^{n}$. We abuse notations and denote both party itself and its identity as M_i, S_i or R_i. All the parties share a bulletin board to upload/download ciphertexts in turn. We assume that every sender knows the identities of his receiver and all the mix-servers, and there is a trusted key generator center (KGC) responsible for generating private key for every user and mix-server.

Definition 5.1 (Identity-based Universal Mixnet)**.** An identity-based universal mixnet Ω with ℓ mix-servers $\{M_i\}_{i=1}^{\ell}$, n senders $\{S_i\}_{i=1}^{n}$ and n receivers $\{R_i\}_{i=1}^{n}$ consists of following algorithms.

- $\mathsf{Init}\,(1^n, ID)$ takes as input security parameter n and the identities of all the parties $ID := \{M_i\}_{i=1}^{\ell} \cup \{S_i, R_i\}_{i=1}^{n}$, and outputs master key msk, system parameters params and a set of private keys $\mathsf{SK} := \{\mathsf{sk}_{\mathsf{ID}}\}_{\mathsf{ID} \in ID}$;
- $\mathsf{PktGen}\left(\{(R_{\phi(i)}, m_i)\}_{i=1}^{n}\right)$ takes as input a set of (recipient, message) tuples $\{(R_{\phi(i)}, m_i)\}_{i=1}^{n}$, where ϕ is a permutation of $\{1, \cdots, n\}$, and outputs a packet set $\{P_{1,i}\}_{i=1}^{n}$;
- $\mathsf{Mix}\left(\{P_{j,i}\}_{i=1}^{n}, \mathsf{sk}_{M_j}\right)$ takes as input the packet set $\{P_{j,i}\}_{i=1}^{n}$ and mix-server M_j's private key sk_{M_j}, and outputs a set of new packet $\{P_{j+1,i}\}_{i=1}^{n}$;
- $\mathsf{PktDec}\left(\{P_{\ell+1,i}\}_{i=1}^{n}, \{\mathsf{sk}_{R_j}\}_{j=1}^{n}\right)$ takes as input the packet set $\{P_{\ell+1,i}\}_{i=1}^{n}$ and all the recipients' private keys $\{\mathsf{sk}_{R_j}\}_{j=1}^{n}$, and outputs a set of (recipient, message) tuples $\{(R_j, m_{\phi^{-1}(j)})\}_{j=1}^{n}$.

Definition 5.2 (Correctness)**.** Let $\Omega = (\mathsf{Init}, \mathsf{PktGen}, \mathsf{Mix}, \mathsf{PktDec})$ be an identity-based universal mixnet. We say Ω is correct if for $(\mathsf{params}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Init}(1^n, ID)$, any permutation $\phi \in \Phi$, any $m_i \in \mathcal{M}$, $\{P_{1,i}\}_{i=1}^{n} \leftarrow_{\$} \mathsf{PktGen}\left(\{(R_{\phi(i)}, m_i)\}_{i=1}^{n}\right)$, $\{P_{\ell+1,i}\}_{i=1}^{n} \leftarrow_{\$} \mathsf{Mix}(\cdots \mathsf{Mix}(\mathsf{Mix}(\{P_{1,i}\}_{i=1}^{n}, \mathsf{sk}_{M_1}), \mathsf{sk}_{M_2}) \cdots, \mathsf{sk}_{M_\ell})$, we have

$$\Pr\left[\mathsf{PktDec}\left(\{P_{\ell+1,i}\}_{i=1}^{n}, \{\mathsf{sk}_{R_j}\}_{j=1}^{n}\right) \neq \{(R_{\phi(i)}, m_i)\}_{i=1}^{n}\right] \leq \mathsf{negl}(n)\,,$$

where Φ includes all the permutation of $\{1, \cdots, n\}$ and $\mathcal{M}$ is the message space.

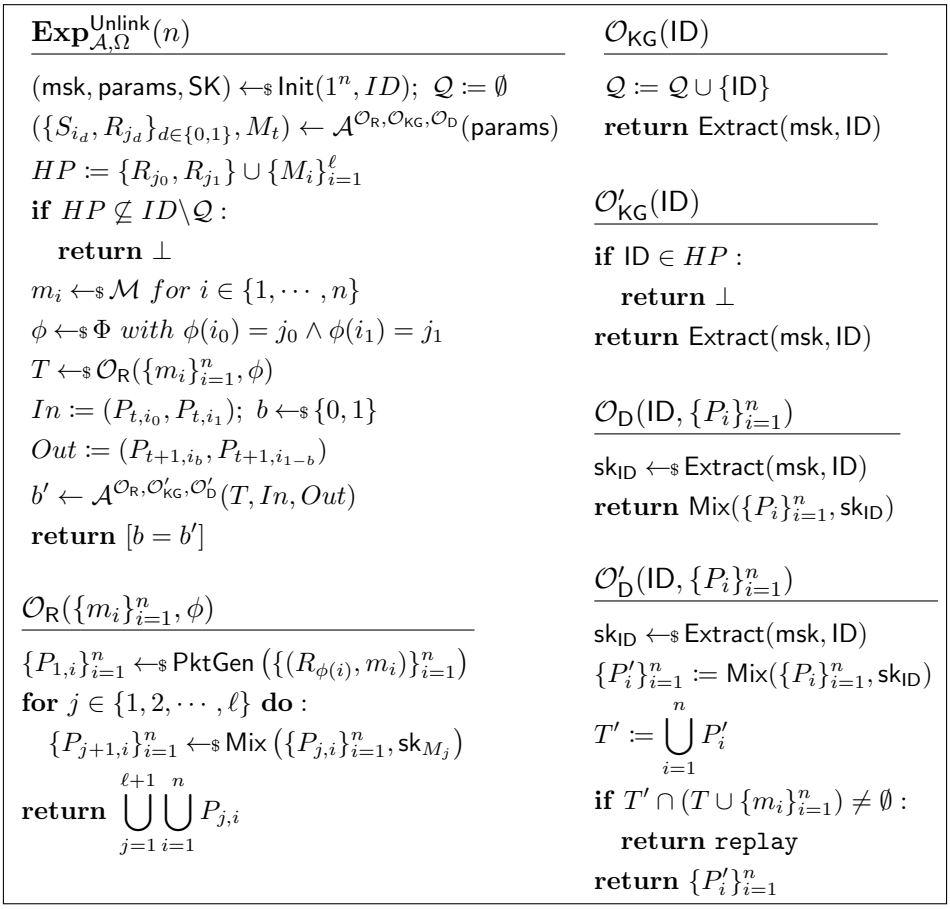

Figure 9: The security game of unlinkability.

Definition 5.3 (Unlinkability)**.** Let $\Omega = (\mathsf{Init}, \mathsf{PktGen}, \mathsf{Mix}, \mathsf{PktDec})$ be an identity-based universal mixnet. We say Ω provides unlinkability if for any PPT adversary $\mathcal{A}$ in game $\mathbf{Exp}^{\mathsf{Unlink}}_{\mathcal{A},\Omega}$ as shown in Fig. 9,

$$\mathbf{Adv}^{\mathsf{Unlink}}_{\mathcal{A},\Omega}(n) \coloneqq \left|\Pr\left[\mathbf{Exp}^{\mathsf{Unlink}}_{\mathcal{A},\Omega}(n) - 1/2\right]\right| \leq \mathsf{negl}(n)\,.$$

5.2 The Proposed Mixnet

Here we first give the definition of symmetric encryption and thereafter present the proposed ID-based universal mixnet.

Definition 5.4 (Semantically Secure Symmetric Encryption)**.** A symmetric encryption scheme $\mathcal{SE} = (\mathsf{K}, \mathsf{E}, \mathsf{D})$ is semantically secure if for any PPT adversary $\mathcal{A}$ there exists a PPT algorithm $\mathcal{A}'$ such that for every efficiently-sampleable distribution X and all efficient functions f and h,

$$\left|\Pr\left[\mathcal{A}(1^n, \mathsf{E}(k, m), h(m)) = f(m)\right] - \Pr\left[\mathcal{A}'(1^n, h(m)) = f(m)\right]\right| \leq \mathsf{negl}(n)\,,$$

where m is chosen according to the distribution X.

Let $\mathcal{SE} = (\mathsf{K}, \mathsf{E}, \mathsf{D})$ be a semantically secure symmetric encryption, and $\epsilon_k(m)$ denote the encryption of message m under symmetric key k. Let $\mathcal{IBE} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Rerand})$

be the proposed IBE scheme and $E_{\mathsf{ID}}(m)$ denote the encryption of m under identity ID using $\mathcal{IBE}$. We present a concrete identity-based universal mixnet Ω as follows.

- $\mathsf{Init}\,(1^n, ID)$: The KGC first generates master key and system parameters $(\mathsf{msk}, \mathsf{params}) \leftarrow_{\$} \mathsf{Setup}(1^n)$, and then computes and distributes private key $\mathsf{sk}_{\mathsf{ID}} \leftarrow_{\$} \mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$ to every party via secure channel.

- $\mathsf{PktGen}\left(\{(R_{\phi(i)}, m_i)\}_{i=1}^n\right)$: For $i = 1$ to n, sender S_i chooses a recipient $R_{\phi(i)}$ and then generates a packet of message m_i as follows.

$$P_{1,i} \coloneqq \left\{\epsilon_{k_{1,i}}(\cdots \epsilon_{k_{\ell,i}}(\epsilon_{k_i}(m_i))\cdots), E_{M_1}(k_{1,i}), \cdots, E_{M_\ell}(k_{\ell,i}), E_{R_{\phi(i)}}(k_i)\right\}$$

  where symmetric keys $k_{1,i}, \cdots, k_{\ell,i}$ and k_i are generated by sender S_i using K. Finally, n packets are sent to the bulletin board.

- $\mathsf{Mix}\left(\{P_{j,i}\}_{i=1}^n, \mathsf{sk}_{M_j}\right)$: Let $P_{j,i} = \{\xi_{j,i}, \zeta_{j,i}, \cdots, \zeta_{\ell,i}, \zeta_{\ell+1,i}\}$, the mix-server M_j downloads all the packets on the bulletin board and generates a set of new packets $\{P_{j+1,i}\}_{i=1}^n$ as follows.
  For $i = 1$ to n:

  - Decrypt the IBE ciphertext $\zeta_{j,i}$ and obtains $k_{j,i} \coloneqq \mathsf{Dec}(\mathsf{sk}_{M_j}, \zeta_{j,i})$;
  - Decrypt the symmetric ciphertext $\xi_{j,i}$ with $k_{j,i}$ and the new ciphertext is $\xi_{j+1,i} \coloneqq \epsilon_{k_{j+1,i}}(\cdots \epsilon_{k_{\ell,i}}(\epsilon_{k_i}(m_i))\cdots)$;
  - Compute new IBE ciphertext $\zeta'_{s,i} \leftarrow_{\$} \mathsf{Rerand}(\zeta_{s,i})$ for $s = j+1$ to $\ell+1$, and the new packet is $P_{j+1,i} \coloneqq \{\xi_{j+1,i}, \zeta'_{j+1,i}, \cdots, \zeta'_{\ell,i}, \zeta'_{\ell+1,i}\}$.

  In the end, the mix-server M_j updates the bulletin board with new packets.

- $\mathsf{PktDec}\left(\{P_{\ell+1,i}\}_{i=1}^n, \{\mathsf{sk}_{R_j}\}_{j=1}^n\right)$: For $j = 1$ to n, the recipient R_j downloads the packet set $\{P_{\ell+1,i}\}_{i=1}^n$ from the bulletin board, decrypts every IBE ciphertext in the packet set to retrieve the symmetric key $k_{\phi^{-1}(j)}$, and decrypts the corresponding symmetric ciphertext to retrieve the message $m_{\phi^{-1}(j)}$.

By the correctness of $\mathcal{SE}$ and $\mathcal{IBE}$, one can verify that Ω is correct. The unlinkability of Ω is formally proved as follows.

Theorem 5.1. *If $\mathcal{SE}$ is of semantic security and $\mathcal{IBE}$ is of rerandomizable ANON-ID-RCCA security, the mixnet Ω above provides unlinkability.*

Proof. We use a sequence of games to prove the unlinkability of Ω as follows.

Game G_0: This is the game $\mathbf{Exp}^{\mathsf{Unlink}}_{\mathcal{A},\Omega}$. Let S_i denote the event that $b = b'$ in game G_i. In game G_0, the advantage of PPT adversary $\mathcal{A}$ is $|\Pr[S_0] - 1/2|$.

Game G_1: This game is the same as G_0 except that all the IBE ciphertexts $\{\zeta_{j,i_0}, \zeta_{j,i_1}\}_{j=t+1}^{\ell+1}$ in P_{t+1,i_0} and P_{t+1,i_1} are generated using Enc instead of Rerand. To show the gap between G_0 and G_1, we consider game $\mathsf{G}_{0,s}$ $(s = 1, \cdots, \ell - t + 1)$ that is the same as G_0 except that $\{\zeta_{j,i_0}\}_{j=t+1}^{t+s}$ in P_{t+1,i_0} are generated using Enc, and game $\mathsf{G}^*_{0,s}(s = 1, \cdots, \ell - t + 1)$ that is the same as $\mathsf{G}_{0,\ell-t+1}$ except that $\{\zeta_{j,i_1}\}_{j=t+1}^{t+s}$ in P_{t+1,i_1} are generated using Enc. Game $\mathsf{G}^*_{0,\ell-t+1}$ is identical to G_1.

Lemma 5.2. *Let $\mathsf{G}_{0,0} = \mathsf{G}_0$. Game $\mathsf{G}_{0,i}$ (resp. $\mathsf{G}^*_{0,i}$, $\mathsf{G}_{0,\ell-t+1}$) is computationally indistinguishable from $\mathsf{G}_{0,i+1}$ (resp. $\mathsf{G}^*_{0,i+1}$, $\mathsf{G}^*_{0,1}$) for $i = 0, \cdots, \ell - t$.*

Proof. If there exists a PPT adversary $\mathcal{A}$ can distinguish game $\mathsf{G}_{0,i}$ and $\mathsf{G}_{0,i+1}$ with non-negligible advantage, we show how to break the rerandomizability of $\mathcal{IBE}$ with $\mathcal{A}$ as follows.

Let $\mathcal{C}_{\mathsf{Re}}$ be the challenger in the game $\mathbf{Exp}^{\mathsf{Re}}_{\mathcal{A}',\mathcal{IBE}}$, and the adversary $\mathcal{A}'$ has to simulate the game $\mathsf{G}_{0,i}$ or $\mathsf{G}_{0,i+1}$ for $\mathcal{A}$. $\mathcal{A}'$ first forwards params generated by $\mathcal{C}_{\mathsf{Re}}$ to $\mathcal{A}$. Although $\mathcal{A}'$ does not know the master key chosen by $\mathcal{C}_{\mathsf{Re}}$, it can response the extraction and decryption queries from $\mathcal{A}$ with the answers provided by $\mathcal{C}_{\mathsf{Re}}$. Then, $\mathcal{A}'$ follows the description of $\mathsf{G}_{0,i}$ to generate T, In and Out, sends ζ_{t+i+1,i_0} in P_{t,i_0} and M_{t+i+1} to $\mathcal{C}_{\mathsf{Re}}$, and replaces ζ_{t+i+1,i_0} in P_{t+1,i_0} to the challenge ciphertext ζ_b. If $b = 1$, then ζ_{t+i+1,i_0} in P_{t+1,i_0} is a rerandomization of that in P_{t,i_0} and the simulation is $\mathsf{G}_{0,i}$; otherwise, it is $\mathsf{G}_{0,i+1}$. ■

Game G_2: This game is the same as G_1 except that the underlying plaintexts of all the IBE ciphertexts $\{\zeta_{j,i_0}, \zeta_{j,i_1}\}_{j=t+1}^{\ell+1}$ in P_{t+1,i_0} and P_{t+1,i_1} are changed into randomly picked symmetric keys $\{k'_{j,i_0}, k'_{j,i_1}\}_{j=t+1}^{\ell+1}$. Similarly, we consider game $\mathsf{G}_{1,s}$ $(s = 1, \cdots, \ell - t + 1)$ that is the same as G_1 except that the underlying plaintexts of $\{\zeta_{j,i_0}\}_{j=t+1}^{t+s}$ in P_{t+1,i_0} are changed into random keys $\{k'_{j,i_0}\}_{j=t+1}^{t+s}$, and game $\mathsf{G}^*_{1,s}(s = 1, \cdots, \ell - t + 1)$ that is the same as $\mathsf{G}_{1,\ell-t+1}$ except that the underlying plaintexts of $\{\zeta_{j,i_1}\}_{j=t+1}^{t+s}$ in P_{t+1,i_1} are changed into random keys $\{k'_{j,i_1}\}_{j=t+1}^{t+s}$. Game $\mathsf{G}^*_{1,\ell-t+1}$ is identical to G_2.

Lemma 5.3. *Let* $\mathsf{G}_{1,0} = \mathsf{G}_1$. *Game* $\mathsf{G}_{1,i}$ *(resp.* $\mathsf{G}^*_{1,i}$, $\mathsf{G}_{1,\ell-t+1}$*) is computationally indistinguishable from* $\mathsf{G}_{1,i+1}$ *(resp.* $\mathsf{G}^*_{1,i+1}$, $\mathsf{G}^*_{1,1}$*) for* $i = 0, \cdots, \ell - t$.

Proof. We show how to break the ID-RCCA security of $\mathcal{IBE}$ with a PPT adversary $\mathcal{A}$ who can distinguish game $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i+1}$ with non-negligible advantage.

Let $\mathcal{C}_{\mathsf{IR}}$ be the challenger in the game $\mathbf{Exp}^{\mathsf{IR}}_{\mathcal{A}',\mathcal{IBE}}$, and the adversary $\mathcal{A}'$ has to simulate the game $\mathsf{G}_{1,i}$ or $\mathsf{G}_{1,i+1}$ for $\mathcal{A}$. $\mathcal{A}'$ first forwards params generated by $\mathcal{C}_{\mathsf{IR}}$ to $\mathcal{A}$. $\mathcal{A}'$ can response the extraction and decryption queries from $\mathcal{A}$ with the answers provided by $\mathcal{C}_{\mathsf{IR}}$. Then, $\mathcal{A}'$ follows the description of $\mathsf{G}_{1,i}$ to generate T, In and Out, where k_{t+i+1,i_0} is picked by $\mathcal{A}'$. Now, $\mathcal{A}'$ samples a new key k'_{t+i+1,i_0}, sends tuple $(k_{t+i+1,i_0}, k'_{t+i+1,i_0}, M_{t+i+1})$ to $\mathcal{C}_{\mathsf{IR}}$, and replaces ζ_{t+i+1,i_0} in P_{t+1,i_0} to the challenge ciphertext ζ_b. If $b = 0$, the underlying plaintext of ζ_{t+i+1,i_0} does not change and the simulation is $\mathsf{G}_{1,i}$; otherwise, it is $\mathsf{G}_{1,i+1}$. ■

Game G_3: This game is the same as G_2 except that the underlying identity of IBE ciphertext $\zeta_{\ell+1,i_0}$ in P_{t+1,i_0} are changed into randomly picked identity R'_0.

Game G_4: This game is the same as G_3 except that the underlying identity of IBE ciphertext $\zeta_{\ell+1,i_1}$ in P_{t+1,i_1} are changed into randomly picked identity R'_1.

Lemma 5.4. *Game* G_3 *(resp.* G_4*) is computationally indistinguishable from* G_2 *(resp.* G_3*).*

Proof. Here we consider a variant of game $\mathbf{Exp}^{\mathsf{AIR}}_{\mathcal{A}',\mathcal{IBE}}$ where $m_0 = m_1$ and adversary $\mathcal{A}'$ only has to guess the underlying identity of challenge ciphertext. The advantage of $\mathcal{A}'$ in this game is also negligible when $\mathcal{IBE}$ is of ANON-ID-RCCA security. Below we show how to break this game with a PPT $\mathcal{A}$ who can distinguish game G_2 and G_3 with non-negligible advantage.

Let $\mathcal{C}$ be the challenger in this variant, and the adversary $\mathcal{A}'$ has to simulate game G_2 or G_3 for $\mathcal{A}$. Analogous to previous analysis, $\mathcal{A}'$ is able to response the queries from $\mathcal{A}$ correctly. $\mathcal{A}'$ then follows the description of G_2 to generate T, In and Out. Now, $\mathcal{A}'$ picks a random identity R'_0, sends (k_{i_0}, R_{j_0}, R'_0) to $\mathcal{C}$ and replaces $\zeta_{\ell+1,i_0}$ in P_{t+1,i_0} to the challenge ciphertext ζ_b. If $b = 0$, the simulation is G_2; otherwise, it is G_3. ■

Lemma 5.5. $\Pr[S_4] = 1/2$.

Proof. All the IBE ciphertexts in P_{t+1,i_0} and P_{t+1,i_1} are independent of those in P_{t,i_0} and P_{t,i_1}. As for symmetric ciphertext, since the underlying keys of ξ_{t+1,i_0} and ξ_{t+1,i_1} are completely changed, by the semantic security of $\mathcal{SE}$, they are also independent of ξ_{t,i_0} and ξ_{t,i_1}. ■

Put it all together, the theorem follows. ■

Comparison with Golle et al.'s Work [13]. Golle et al. [13] proposed a mixnet which is only secure against passive adversary. In contrast, due to the ID-RCCA security of the underlying $\mathcal{IBE}$, our mixnet is secure against active adversaries. In terms of system deployment, our ID-based mixnet enjoys more flexibility, as IBE scheme inherently dispenses with the issue of key distribution among servers and the universal rerandomizability of $\mathcal{IBE}$ permits server to rerandomize all the ciphertexts without public keys. Consequently, the ad-hoc enter or leave of a server (that does not locate in any mixing path) does not need complex configuration or affect the running of other servers in mix network, as mix operation on each server only requires the private key. Also, our ID-based mixnet supports fair anonymity as the trusted authority could upon abuse reveal the receiver identity.

6 Conclusions

In this work, we propose a new security notion called ANON-ID-RCCA security for rerandomizable IBE, and design a concrete IBE satisfying this security and universal rerandomizability. To illustrate the usefulness of this notion, we also present an ID-based universal mixnet where the proposed IBE plays as the core building block. With the ANON-ID-RCCA security of underlying IBE, this universal mixnet achieves both fair anonymity and strong unlinkability.

As this is the first work studying RCCA security in the identity-based setting, it naturally raises some interesting problems that deserve further investigation. Regarding the construction, reducing the ciphertext size of proposed IBE will be the top priority, as it is four times greater than the Gentry-IBE. This may require a completely new design of the ciphertext structure allowing constrained rerandomization. Also, it might be interesting to achieve perfect rerandomizability where the distribution of the rerandomization of a fixed ciphertext is identical to that of the fresh encryption of same plaintext.

As for the applications, we believe that our new notion could be also applicable to most existing rerandomizable RCCA-secure applications to eliminate the need for public key distribution infrastructure. For example, an application of rerandomizable ANON-ID-RCCA-secure IBE is achieving the first exfiltration-resilient one-round ID-based message transmission with reverse firewall [9].

Acknowledgement. We thank all the anonymous reviewers for their insightful comments and suggestions on this manuscript. Rongmao Chen is support by National Natural Science Foundation of China (Grant No. 62122092, 62032005). Xinyi Huang and Jianting Ning are supported by Natural Science Foundation of China (Grant No. 61972094, 62032005), and the young talent promotion project of Fujian Science and Technology Association, and Science Foundation of Fujian Provincial Science and Technology Agency (2020J02016).

References

[1] Badertscher, C., Maurer, U., Portmann, C., Rito, G.: Revisiting (R)CCA security and replay protection. In: Garay, J. (ed.) PKC 2021. LNCS, vol. 12711, pp. 173202. Springer, Heidelberg (May 2021). https://doi.org/10.1007/978-3-030-75248-4_7

[2] Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (Aug 2001). https://doi.org/10.1007/3-540-44647-8_13

[3] Camenisch, J., Lysyanskaya, A.: A formal treatment of onion routing. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 169–187. Springer, Heidelberg (Aug 2005). https://doi.org/10.1007/11535218_11

[4] Canetti, R., Krawczyk, H., Nielsen, J.B.: Relaxing chosen-ciphertext security. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 565–582. Springer, Heidelberg (Aug 2003). https://doi.org/10.1007/978-3-540-45146-4_33

[5] Chase, M., Kohlweiss, M., Lysyanskaya, A., Meiklejohn, S.: Malleable proof systems and applications. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 281–300. Springer, Heidelberg (Apr 2012). https://doi.org/10.1007/978-3-642-29011-4_18

[6] Chen, R., Mu, Y., Yang, G., Susilo, W., Guo, F., Zhang, M.: Cryptographic reverse firewall via malleable smooth projective hash functions. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 844–876. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_31

[7] Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_4

[8] David, C., Eugne, v.H.: Group Signatures. In: Donald, W.D.(ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (May 1991).https://doi.org/10.1007/3-540-46416-6_22

[9] Dodis, Y., Mironov, I., Stephens-Davidowitz, N.: Message transmission with reverse firewalls—secure communication on corrupted machines. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 341–372. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_13

[10] Faonio, A., Fiore, D.: Improving the efficiency of re-randomizable and replayable cca secure public key encryption. In: International Conference on Applied Cryptography and Network Security. pp. 271–291. Springer (2020)

[11] Faonio, A., Fiore, D., Herranz, J., Ràfols, C.: Structure-preserving and re-randomizable RCCA-secure public key encryption and its applications. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 159–190. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34618-8_6

[12] Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (May / Jun 2006). https://doi.org/10.1007/11761679_27

[13] Golle, P., Jakobsson, M., Juels, A., Syverson, P.F.: Universal re-encryption for mixnets. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 163–178. Springer, Heidelberg (Feb 2004). https://doi.org/10.1007/978-3-540-24660-2_14

[14] Gomulkiewicz, M., Klonowski, M., Kutylowski, M.: Onions based on universal re-encryption - anonymous communication immune against repetitive attack. In: Lim, C.H., Yung, M. (eds.) WISA 04. LNCS, vol. 3325, pp. 400–410. Springer, Heidelberg (Aug 2004)

[15] Groth, J.: Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 152–170. Springer, Heidelberg (Feb 2004). https://doi.org/10.1007/978-3-540-24638-1_9

[16] Habib, A.Y., Javad, M., Mahmoud, S.: Identity-based universal re-encryption for mixnets. In: Secur. Commun. Networks (2015). vol. 8, pp. 2992–3001. https://doi.org/10.1002/sec.1226

[17] Klonowski, M., Kutyłowski, M., Zagórski, F.: Anonymous communication with on-line and off-line onion encoding. In: International Conference on Current Trends in Theory and Practice of Computer Science. pp. 229–238. Springer (2005)

[18] Libert, B., Peters, T., Qian, C.: Structure-preserving chosen-ciphertext security with shorter verifiable ciphertexts. In: Fehr, S. (ed.) PKC 2017, Part I. LNCS, vol. 10174, pp. 247–276. Springer, Heidelberg (Mar 2017). https://doi.org/10.1007/978-3-662-54365-8_11

[19] Maurer, U.: Constructive cryptography-a new paradigm for security definitions and proofs. In: TOSCA 2011. LNCS, vol. 6993, pp. 3356. Springer (2012). https://doi.org/10.1007/978-3-642-27375-9_3

[20] Mironov, I., Stephens-Davidowitz, N.: Cryptographic reverse firewalls. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 657–686. Springer, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46803-6_22

[21] Naveed, M., Agrawal, S., Prabhakaran, M., Wang, X., Ayday, E., Hubaux, J.P., Gunter, C.A.: Controlled functional encryption. In: Ahn, G.J., Yung, M., Li, N. (eds.) ACM CCS 2014. pp. 1280–1291. ACM Press (Nov 2014). https://doi.org/10.1145/2660267.2660291

[22] Pereira, O., Rivest, R.L.: Marked mix-nets. In: Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P.Y.A., Teague, V., Bracciali, A., Sala, M., Pintore, F., Jakobsson, M. (eds.) FC 2017 Workshops. LNCS, vol. 10323, pp. 353–369. Springer, Heidelberg (Apr 2017)

[23] Phan, D.H., Pointcheval, D.: OAEP 3-round: A generic and secure asymmetric encryption padding. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 63–77. Springer, Heidelberg (Dec 2004). https://doi.org/10.1007/978-3-540-30539-2_5

[24] Prabhakaran, M., Rosulek, M.: Rerandomizable RCCA encryption. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 517–534. Springer, Heidelberg (Aug 2007). https://doi.org/10.1007/978-3-540-74143-5_29

[25] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO'84. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (Aug 1984)

[26] Syverson, P., Dingledine, R., Mathewson, N.: Tor: The second generation onion router. In: Usenix Security (2004)

[27] Wang, Y., Chen, R., Yang, G., Huang, X., Wang, B., Yung, M.: Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021. LNCS, vol. 12828, pp. 270–300. Springer, Heidelberg (Aug 2021). https://doi.org/10.1007/978-3-030-84259-8_10

A Another Application: Exfiltration-Resilient ID-based Message Transmission

A.1 ID-Based Message Transmission Protocols

An ID-based message transmission (MT) protocol is a two-party protocol where one party, Alice, is able to communicate a message to the other one, Bob, by using his identity. Below is the formal definition of this notion which is a slight adaption of MT protocol in [9].

Definition A.1 (ID-based MT protocol)**.** An ID-based MT protocol consists of a tuple of algorithms $\mathcal{P} = (\mathsf{setup}, \mathsf{extract}, \mathsf{next}_A, \mathsf{next}_B, \mathsf{return}_B)$ as follows.

- setup takes as input 1^n, where n is the security parameter, and outputs the master secret key msk and initial states for each party, S_A, S_B, which consist of private input σ_A, σ_B respectively and public input π.
- $\mathsf{extract}$ takes as input master secret key msk and identity $\mathsf{ID} \in \{0,1\}^*$, and returns the private key corresponding to ID.
- next takes as input session id sid and an incoming message, updates the state of party and outputs an outgoing message.
- return_B takes as input Bob's state S_B and session id sid and returns Bob's final output.

Alice receives as input a plaintext m, identities $\mathsf{ID}_A, \mathsf{ID}_B$ and private key sk_A corresponding to ID_A. Bob receives as input identities $\mathsf{ID}_A, \mathsf{ID}_B$ and private key sk_B corresponding to ID_B. The protocol is correct if for any input m, identities ID_A and ID_B, Bob always outputs m.

We consider a game described in Fig. 10. The adversary first calls Initialize, then makes calls to other procedures, finally guesses the challenge bit and calls Finalize. If the output of Finalize is 1, then adversary wins the game.

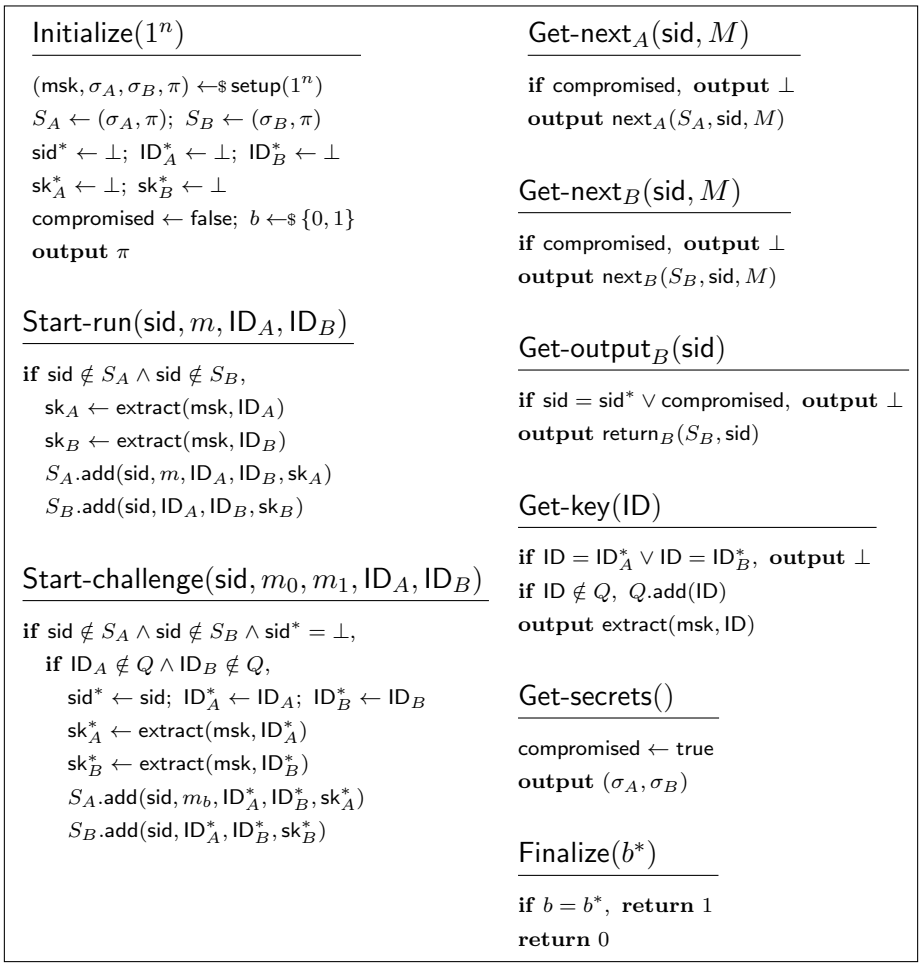

Figure 10: Procedures used to define security for ID-based MT protocol.

Definition A.2 (ID-based MT security)**.** An ID-based MT protocol is

- chosen-plaintext secure (ID-CPA-secure) if no PPT adversary has non-negligible advantage in the game in Fig. 10 when $\mathsf{Get\text{-}next}_A(\mathsf{sid}, M)$ and $\mathsf{Get\text{-}next}_B(\mathsf{sid}, M)$ output $\perp$ unless this is the first Get-next call with this sid or M is the output from the previous $\mathsf{Get\text{-}next}_A$ call with the same sid or the previous $\mathsf{Get\text{-}next}_B$ with the same sid respectively; and
- chosen-ciphertext secure (ID-CCA-secure) if no PPT adversary has non-negligible advantage in the game presented in Fig. 10 with access to all oracles.

A.2 Reverse Firewalls

A cryptographic protocol $\mathcal{P}$ defines the interactions between parties $(P_1, \ldots, P_\ell)$ and satisfies certain functionality requirements $\mathcal{F}$ and security requirements $\mathcal{S}$. For any party A, we use $\bar{A}$ to denote arbitrary adversarial implementation of party A and $\widetilde{A}$ to denote functionality-maintaining implementation of A. For any protocol $\mathcal{P}$ with party A, the protocol where party A is replaced by $\widetilde{A}$ is represented as $\mathcal{P}_{A\to\widetilde{A}}$.

Definition A.3 (Reverse firewalls [20])**.** A reverse firewall (RF) is a stateful algorithm $\mathcal{W}$ that takes as input its state and a message and outputs an updated state and message. For simplicity, the state of $\mathcal{W}$ is not written explicitly.

For party A and reverse firewall $\mathcal{W}$, a composed party is denoted by $\mathcal{W} \circ A$. When the composed party engages in a protocol $\mathcal{P}$, the state of $\mathcal{W}$ is initialized to public parameters. If $\mathcal{W}$ is meant to be composed with party A, we call it a reverse firewall for A.

A functionality-maintaining reverse firewall would not break the correctness of protocol. The functionality requirements of $\mathcal{P}_{A\to\mathcal{W}\circ A}$ and $\mathcal{P}$ is identical.

Definition A.4 (Security preservation)**.** For any protocol $\mathcal{P}$ that satisfies security requirement $\mathcal{S}$ and functionality requirement $\mathcal{F}$, and any reverse firewall $\mathcal{W}$, we say that $\mathcal{W}$ strongly preserves $\mathcal{S}$ for party A if for any polynomial-time algorithm $\bar{A}$, protocol $\mathcal{P}_{A\to\mathcal{W}\circ\bar{A}}$ satisfies $\mathcal{S}$. Reverse firewall $\mathcal{W}$ preserves $\mathcal{S}$ for party A if for any polynomial-time algorithm $\widetilde{A}$ such that $\mathcal{P}_{A\to\widetilde{A}}$ satisfies $\mathcal{F}$, protocol $\mathcal{P}_{A\to\mathcal{W}\circ\widetilde{A}}$ satisfies $\mathcal{S}$.

A reverse firewall is exfiltration-resistant if no adversarial implementation of Alice can leak information through it. Game LEAK in Fig. 11 is adopted to define this property.

$\mathsf{LEAK}(\mathcal{P}, A, B, \mathcal{W}, n)$

$(\bar{A}, \bar{B}, I) \leftarrow \mathcal{A}(1^n)$; $b \leftarrow\!\!\$\ \{0,1\}$
if $b = 1$, $A^* \leftarrow \mathcal{W} \circ \bar{A}$; **else** $A^* \leftarrow \mathcal{W} \circ A$
$\mathcal{T}^* \leftarrow \mathcal{P}_{A\to A^*, B\to\bar{B}}(I)$; $b^* \leftarrow \mathcal{A}(\mathcal{T}^*, \mathsf{st}_{\bar{B}})$
return $(b = b^*)$

Figure 11: Definition of game $\mathsf{LEAK}(\mathcal{P}, A, B, \mathcal{W}, n)$. I is a valid input for $\mathcal{P}$; $\mathcal{T}^*$ is the transcript of running $\mathcal{P}_{A\to A^*, B\to\bar{B}}(I)$; $\mathsf{st}_{\bar{B}}$ is the state of $\bar{B}$ after the run of protocol.

Definition A.5 (Exfiltration resistance)**.** For any protocol $\mathcal{P}$ that satisfies functionality $\mathcal{F}$, and any reverse firewall $\mathcal{W}$, we say $\mathcal{W}$ is strongly exfiltration-resistant for A against B in $\mathcal{P}$ if no PPT adversary $\mathcal{A}$ has non-negligible advantage in $\mathsf{LEAK}(\mathcal{P}, A, B, \mathcal{W}, n)$. If B is empty, then $\mathcal{W}$ is strongly exfiltration-resistant. $\mathcal{W}$ is exfiltration-resistant for A against B in $\mathcal{P}$ satisfying functionality $\mathcal{F}$ if no PPT adversary $\mathcal{A}$ with output circuits $\widetilde{A}$ and $\widetilde{B}$ such that $\mathcal{P}_{A\to\widetilde{A}}$ and $\mathcal{P}_{B\to\widetilde{B}}$ satisfy $\mathcal{F}$ has non-negligible advantage in $\mathsf{LEAK}(\mathcal{P}, A, B, \mathcal{W}, n)$. If B is empty, then $\mathcal{W}$ is exfiltration-resistant.

A.3 Exfiltration-Resilient ID-based Message Transmission Protocol

In [9], Dodis et al. presented a one-round message transmission protocol that is exfiltration-resilient which means no secret information could be stealthily leaked from the possibly corrupted machines during the message transmission. At the core of their protocol is a Rand-RCCA-secure PKE scheme equipped with cryptographic reverse firewall (CRF) [20], which could be viewed as a machine sitting between the party and the outside, preserving the security of protocol and resisting the exfiltration by modifying the incoming and outgoing messages of the party (See A.2 for more details).

Here we extend Dodis et al.'s protocol into the identity-based setting by using a rerandomizable ANON-ID-RCCA secure IBE and consequently obtain the first exfiltration-resilient ID-based (one-round) message transmission protocol. The protocol is somewhat simple as shown in Fig. 12, where the only message is an encryption of Alice's plaintext under Bob's identity. The formal definitions of this notion and its security are provided in A.1.

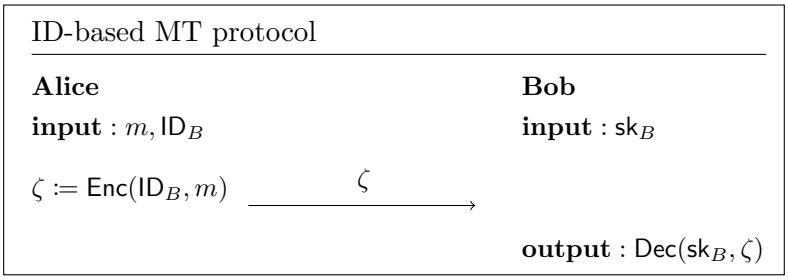

Figure 12: ID-based MT protocol using IBE scheme $(\mathsf{Setup}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ where private key $\mathsf{sk}_B := \mathsf{Extract}(\mathsf{msk}, \mathsf{ID}_B)$ and master key msk is generated from Setup.

Definition A.6 (ID-based encryption)**.** An ID-based encryption (IBE) scheme is specified by four algorithms: Setup, $\mathsf{Extract}$, Enc and Dec.

- Setup takes as input 1^n where n is the security parameter and returns master secret key msk and system parameters params including message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.
- $\mathsf{Extract}$ takes as input params, msk and arbitrary $\mathsf{ID} \in \{0,1\}^*$, and returns a private key sk.
- Enc takes as input params, $m \in \mathcal{M}$ and ID, and returns a ciphertext $c \in \mathcal{C}$.
- Dec takes as input params, private key sk and $c \in \mathcal{C}$, and returns $m \in \mathcal{M}$.

We omit the system parameters from the input to $\mathsf{Extract}$, Enc and Dec. The scheme is correct if $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(m, \mathsf{ID})) = m$ for any $m \in \mathcal{M}$, $\mathsf{ID} \in \{0,1\}^*$ and $\mathsf{sk} = \mathsf{Extract}(\mathsf{msk}, \mathsf{ID})$. The IBE scheme is ID-CPA-secure if for any adaptively chosen pair of plaintexts (m_0, m_1) and ID^*, $\mathsf{Enc}(m_0, \mathsf{ID}^*)$ and $\mathsf{Enc}(m_1, \mathsf{ID}^*)$ are computationally indistinguishable.

Definition A.7 (Rerandomizable ID-based encryption)**.** An ID-based encryption scheme is *rerandomizable* if 1) there exists an efficient algorithm Rerand that takes as input ciphertext c and ID and outputs a new ciphertext c'; 2) for any ID and corresponding private key sk, and any ciphertext c under ID such that $\mathsf{Dec}(\mathsf{sk}, c) \neq \perp$, we have $\mathsf{Dec}(\mathsf{sk}, \mathsf{Rerand}(c, \mathsf{ID})) = \mathsf{Dec}(\mathsf{sk}, c)$ and $(c, \mathsf{Rerand}(c, \mathsf{ID}))$ is computationally indistinguishable from $(c, \mathsf{Rerand}(\mathsf{Enc}(0, \mathsf{ID}), \mathsf{ID}))$. We say that it is *stongly rerandomizable* if the rerandomizability also holds when $\mathsf{Dec}(\mathsf{sk}, c) = \perp$.

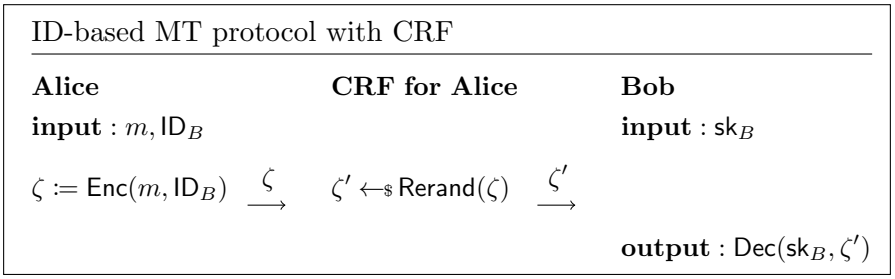

Figure 13: Reverse firewall for Alice in ID-based MT protocol. Rerand is the rerandomization algorithm of IBE scheme.

The protocol with reverse firewall is shown in Fig. 13. The encryption sent from Alice is "sanitized" by reverse firewall performing rerandomization.

Theorem A.1. *The ID-based MT protocol shown in Fig. 12 is ID-CCA-secure if the underlying IBE scheme is ID-RCCA-secure. If this IBE scheme is also rerandomizable, then the reverse firewall shown in Fig. 13 preserves security for Alice and resists exfiltration for Alice.*

Proof. It is clear that protocol shown in Fig. 12 is ID-CCA-secure. By the correctness of rerandomization, the firewall for Alice maintains functionality. Let $\widetilde{A}$ denote a compromised implementation of Alice maintaining functionality and ζ be the encryption sent by $\widetilde{A}$. Since $\widetilde{A}$ maintains functionality, we have $m = \mathsf{Dec}(\mathsf{sk}_B, \zeta) \neq \perp$. By the definition of rerandomizability, the output of $\mathsf{Rerand}(\zeta)$ is computationally indistinguishable from $\mathsf{Enc}(\mathsf{ID}_B, m)$, from which the security preservation and exfiltration resistance of firewall follows. ■

The usage of IBE scheme makes protocol in Fig. 12 unsuitable to transmit very long plaintext in practice, as operations in IBE scheme can be quite time-consuming and inefficient. One common solution is *hybrid encryption* where plaintext is encrypted using symmetric-key encryption and the symmetric key (much shorter than plaintext) is encrypted using IBE scheme. When we consider the reverse firewall for this protocol, the symmetric-key encryption must be "key malleable". Roughly speaking, key malleability means that an encryption in symmetric-key scheme can be converted into an encryption with same plaintext under new key by reverse firewall. The reason behind this requirement is that the symmetric key chosen by compromised Alice might be "malicious" and needs the sanitization of reverse firewall (i.e., modification on symmetric key). Unfortunately, according to the conclusion in [9], such a "key malleable" symmetric-key encryption implies public-key encryption which is still inefficient when the plaintext is very long. Therefore, it seems hybrid encryption fails to settle the issue of efficiency.