SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2024, Vol. 67, Iss. 11, 212103:1–212103:15
https://doi.org/10.1007/s11432-023-3877-9

RCCA-SM9: securing SM9 on corrupted machines

Rongmao CHEN[1], Jinrong CHEN[1], Xinyi HUANG[2*] & Yi WANG[1]

[1]*College of Computer, National University of Defense Technology, Changsha* 410073*, China;*
[2]*Artificial Intelligence Thrust, Information Hub, Hong Kong University of Science and Technology (Guangzhou), Guangzhou* 510000*, China*

Received 7 June 2023/Revised 12 September 2023/Accepted 29 September 2023/Published online 11 October 2024

Abstract The SM9 identity-based encryption (IBE) scheme is a cryptographic standard used in China, and has been incorporated into the ISO/IEC standard in 2021. This work primarily proposes a countermeasure to secure the SM9 IBE scheme if its implementation is tampered with or deviated from the standard specification. Such attacks, known as subversion attacks, are feasible and powerful in real-world cryptographic application scenarios. Our goal is to design a subversion-resilient variant of the SM9 IBE scheme, primarily using the cryptographic reverse firewall (CRF) proposed by Mironov and Stephens-Davidowitz at EUROCRYPT 2015. A CRF can sanitize cryptographic transcripts to eliminate covert channels, necessitating that the underlying primitive be rerandomizable. Unfortunately, the rerandomizability of the SM9 IBE scheme is disabled for ensuring security against chosen ciphertext attack (CCA). Hence, we shift our focus to a relaxed version of CCA security called RCCA security, offering security guarantees comparable to CCA security while allowing for ciphertext rerandomization. For this purpose, we design an efficient and RCCA-secure variant of the SM9 IBE scheme with provable security that can integrate with CRFs to achieve subversion resilience.

Keywords SM9, subversion resilience, subversion attack, cryptographic reverse firewall, RCCA

1 Introduction

SM9 is a cryptographic standard widely used in China, playing a significant role in enhancing the security of numerous networks and information systems. It provides a comprehensive set of cryptographic primitives, including identity-based encryption (IBE), identity-based digital signature, and identity-based key exchange, all designed to meet stringent security requirements. Notably, the SM9 encryption scheme has gained international recognition and has been incorporated into the ISO/IEC standard[1)]. This standardization promotes the interoperability of SM9, allowing for the secure exchange of cryptographic keys and encrypted data across different systems and applications [1]. This recognition further highlights its relevance and effectiveness in ensuring secure communication and data protection on a global scale.

Although the SM9 IBE scheme has been theoretically proven to be secure, this work focuses on a specific and potent attack that is not currently addressed in the existing security model. Specifically, the real-world implementation of the SM9 IBE scheme may be vulnerable to subversion attacks, wherein attackers can covertly embed backdoors to gain unauthorized access to the system's secrets (e.g., secret keys). The concept of subversion attacks was initially explored by Young and Yung [2,3] in the 1990s and was further substantiated by the Snowden revelations in 2013, revealing their real-world implementation.

Subversion attacks possess such significant power that achieving meaningful security within a typical security model becomes impossible. In reality, a subverter controlling the cryptographic implementations can launch arbitrary attacks. For instance, a malicious cryptosystem implementer could modify the encryption procedure such that the algorithm always outputs the secret key, regardless of the messages intended for encryption. In such cases, security is entirely compromised unless additional assumptions are made. To this end, several approaches have been proposed to attain subversion resilience. These approaches aim to mitigate the threat of subversion attacks by introducing additional security measures and making suitable assumptions.

* Corresponding author (email: xinyi@ust.hk)

1) https://www.iso.org/standard/78751.html.

Given the increasing importance and popularity of SM9, we aim to design a subversion-resilient SM9 IBE variant with provable security. Our approach is based on a cryptographic primitive known as a cryptographic reverse firewall (CRF), proposed by Mironov and Stephens-Davidowitz [4]. This primitive has attracted considerable attention recently because of its ability to realize subversion-resilient cryptographic algorithms/protocols, including public-key encryption schemes, digital signature schemes, and key agreement protocols. Conceptually, a CRF can be considered similar to a traditional network firewall situated at the boundary of a private network. However, the key distinction between them lies in the capability of CRF to modify the incoming and outgoing messages of the party executing cryptographic algorithms. The primary function of the CRF is to sanitize cryptographic transcripts, thereby eliminating potential covert channels, while preserving the original functionality of the cryptographic algorithms. Moreover, we aim to fortify its resistance to subversion attacks by integrating it into the SM9 IBE scheme.

Designing CRF for the SM9 IBE scheme is challenging. The main challenge arose from the requirement that the modified ciphertexts produced by the CRF remain decryptable. This necessitates that the underlying encryption scheme be publicly rerandomizable. However, the SM9 IBE scheme provides strong security against chosen ciphertext attacks (CCA) [5–8], making the desirable property of rerandomizability unattainable.

To overcome this issue, inspired by the work of Dodis et al. [9], this work designs a variant of the SM9 IBE scheme that offers relaxed CCA (RCCA) security, as defined by Phan and Pointcheval [10]. RCCA security provides security guarantees comparable to CCA security from a practical perspective while allowing for ciphertext rerandomization, which is essential in the CRF setting. Based on this observation, new approaches for designing an efficient and RCCA-secure variant of the SM9 IBE scheme are explored. The primary objective for developing new approaches is to ensure that the ciphertexts remain rerandomizable to enable the application of CRFs, thereby achieving subversion resilience. By adopting RCCA security, a balance is attained between practical security guarantees and requirements for successful integration with CRFs.

1.1 Our contributions

For developing an RCCA-secure variant of the SM9 IBE scheme, careful analysis and new techniques are required. The aim is to maintain the core security properties of the original SM9 encryption scheme while introducing the necessary modifications for enabling rerandomizability. By leveraging existing research on RCCA security and drawing upon efficient cryptographic constructions, an enhanced SM9 IBE variant is designed that can achieve subversion resilience and efficient rerandomization of ciphertexts.

The main contributions of this work are summarized as follows.

• We introduce the notion of indistinguishability under identity-based RCCA (IND-ID-RCCA) and rerandomizability for IBE schemes. IND-ID-RCCA captures a relaxed version of the typical IND-ID-CCA security notion in IBE, while rerandomizability models the indistinguishable rerandomization of ciphertext.

• We design a variant of the SM9 IBE scheme that could realize IND-ID-RCCA security and ciphertext rerandomizability. Inspired by the optimal asymmetric encryption padding (OAEP) 3-round paradigm proposed by Phan and Pointcheval [10], necessary modifications are introduced to the SM9 IBE scheme to enable rerandomization.

• We propose a new hardness assumption, which can be reduced to the decisional q-bilinear Diffie-Hellman inversion (q-BDHI) assumption [11]. Based on this new assumption, the proposed scheme is proved to have satisfied the IND-ID-RCCA security and ciphertext rerandomizability in the random oracle model.

By defining the IND-ID-RCCA and rerandomizability notions, designing an enhanced SM9 IBE scheme, and establishing the security proof based on a new hardness assumption, our work contributes to the development of efficient and secure IBE encryption schemes compatible with CRFs.

1.2 Related work

The concept of RCCA security can be traced back to the work of An et al. [12] at EUROCRYPT'02, where they introduced the notion of "generalized CCA" security. In this notion, the adversary is constrained from making decryption queries for ciphertexts that are related to the challenge ciphertext. The relation between these ciphertexts must be an equivalence relation that is publicly and efficiently computable;

furthermore, decryption must preserve this relation, suggesting that if two ciphertexts are related, they necessarily encrypt identical plaintexts.

Phan and Pointcheval [10] proposed highly efficient asymmetric encryption schemes with IND-RCCA security, such as ElGamal and Paillier. Notably, their objective was different from ours. They primarily aimed to enhance the security reduction of the OAEP constructions, focusing on the intractability of partial domain one-wayness and restrictions to permutations. Moreover, they did not specifically address the issue of ciphertext rerandomizability, which is the main focus of this work. Chen et al. [13] designed a rerandomizable RCCA-secure SM2 encryption scheme, which is also a cryptographic standard used in China. However, to the best of our knowledge, there has been no prior construction of a rerandomizable RCCA-secure IBE scheme in the context of the notion proposed by Phan and Pointcheval [10]. Our design is the first rerandomizable IBE scheme that satisfies the security notion defined by Phan and Pointcheval [10].

Another relaxation of CCA security, known as replayable CCA security, was introduced by Canette et al. at the International Cryptology Conference (CRYPTO) 2003 [14]. This notion restricts the relation in "generalized CCA" security [12] to the (possibly non-computable) equality of plaintexts. Although an RCCA-secure scheme is trivially secure in the "replayable CCA" scenario, it may not necessarily provide security in the "generalized CCA" or traditional CCA scenarios. Moreover, several researches have focused on replayable CCA-secure constructions [15–21]. For instance, Wang et al. [21] proposed the first anonymous rerandomizable replayable CCA-secure public-key encryption scheme in the standard model.

In the context of IBE, Wang et al. [22] first considered rerandomizable replayable CCA security for IBE in the standard model at International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2021. They proposed the first rerandomizable replayable CCA-secure IBE scheme, which can be considered as a double strand of Gentry-IBE [23]. Golle et al. [15] initially proposed the idea of using a double strand, and it was later employed by Prabhakaran and Rosulek [17] at CRYPTO 2007 to construct a replayable CCA-secure encryption scheme in the standard model. However, this approach is not applicable to the SM9 IBE scheme because of its dissimilarity in the ciphertext structure from that used by ElGamal or Cramer-Shoup schemes [5]. Additionally, the scheme proposed by Wang et al. [22] is quite inefficient because of the double encryption paradigm. Our construction, while achieving a different RCCA security notion, is more efficient than the scheme proposed by Wang et al. [22].

2 Preliminaries

2.1 Notations

Let $\lambda \in \mathbb{N}$ denote the security parameter and $\mathsf{negl}(\lambda)$ denote the negligible function. An asymmetric bilinear group is a tuple $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, P_1, P_2)$ where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are groups of prime order p, P_1 is a generator of $\mathbb{G}_1$, P_2 is a generator of $\mathbb{G}_2$. $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable, non-degenerate bilinear map. For any non-empty set $\mathcal{X}$, $x \leftarrow\$\, \mathcal{X}$ denotes sampling x from $\mathcal{X}$ uniformly at random. For any randomized algorithm $\mathsf{Alg}(x)$, $y \leftarrow\$\, \mathsf{Alg}(x)$ denotes the random output of $\mathsf{Alg}(x)$. For any deterministic algorithm $\mathsf{Alg}(x)$, $y \leftarrow \mathsf{Alg}(x)$ denotes the deterministic output of $\mathsf{Alg}(x)$.

2.2 IBE

An IBE scheme is specified by four algorithms: Setup, Ext, Enc, and Dec.

- Setup takes as input 1^λ where λ is the security parameter, and returns the master public key mpk and the master secret key msk, including message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.
- Ext takes as input mpk, msk and an arbitrary ID $\mathsf{id} \in \{0,1\}^*$, and returns a private key $\mathsf{sk}_{\mathsf{id}}$.
- Enc takes as input mpk, id and $m \in \mathcal{M}$, and returns a ciphertext $C \in \mathcal{C}$.
- Dec takes as input mpk, $\mathsf{sk}_{\mathsf{id}}$ and $C \in \mathcal{C}$, and returns $m \in \mathcal{M}$ or $\perp$.

The scheme is correct if for $(\mathsf{mpk}, \mathsf{msk}) \leftarrow\$\, \mathsf{Setup}(1^\lambda)$, any $m \in \mathcal{M}$, any $\mathsf{id} \in \{0,1\}^*$ and $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$,

$$\Pr[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{Enc}(\mathsf{id}, m)) \neq m] \leqslant \mathsf{negl}(\lambda).$$

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

1 : $s \leftarrow\!\$\ [1, p-1]$
2 : $P_{\text{pub}} \leftarrow [s]P_1$
3 : $g \leftarrow \hat{e}(P_{\text{pub}}, P_2)$
4 : $\mathsf{mpk} \leftarrow (P_{\text{pub}}, g)$
5 : $\mathsf{msk} \leftarrow s$
6 : **return** $(\mathsf{mpk}, \mathsf{msk})$

$\mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$

1 : $s \leftarrow \mathsf{msk}$
2 : **if** $s + \mathsf{H}_1(\mathsf{id}) \equiv 0 \bmod p$ **then**
3 : **return** $\perp$
4 : **endif**
5 : $\mathsf{sk}_{\mathsf{id}} \leftarrow [\frac{s}{s + \mathsf{H}_1(\mathsf{id})}]P_2$
6 : **return** $\mathsf{sk}_{\mathsf{id}}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$

1 : $(P_{\text{pub}}, g) \leftarrow \mathsf{mpk}$
2 : $h_1 \leftarrow \mathsf{H}_1(\mathsf{id})$
3 : $Q \leftarrow [h_1]P_1 + P_{\text{pub}}$
4 : $x \leftarrow\!\$\ [1, p-1]$
5 : $C_1 \leftarrow [x]Q$
6 : $t \leftarrow g^x$
7 : $K_1 \| K_2 \leftarrow \mathsf{KDF}(C_1, t, m)$
8 : $C_2 \leftarrow K_1 \oplus m$
9 : $C_3 \leftarrow \mathsf{H}(C_2 \| K_2)$
10 : $C = C_1 \| C_2 \| C_3$
11 : **return** C

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, C)$

1 : $C_1 \| C_2 \| C_3 \leftarrow C$
2 : **if** $C_1 \notin \mathbb{G}_1^*$ **then**
3 : **return** $\perp$
4 : **endif**
5 : $t \leftarrow \hat{e}(C_1, \mathsf{sk}_{\mathsf{id}})$
6 : $K_1 \| K_2 \leftarrow \mathsf{KDF}(C_1, t, m)$
7 : $C_3' = \mathsf{H}(C_2 \| K_2)$
8 : **if** $C_3' \neq C_3$ **then**
9 : **return** $\perp$
10 : **endif**
11 : **return** $m \leftarrow K_1 \oplus C_2$

Figure 1 SM9 encryption scheme $\Pi_{\mathtt{SM9}}$.

$\text{IND-RCCA}_{\Pi}^{\mathcal{A}}(1^\lambda)$

1 : $(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\$\ \mathsf{Setup}(1^\lambda)$
2 : $(m^*, r^*) \leftarrow \perp$
3 : $(m_0, m_1) \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk}.\mathsf{id}^*)$
4 : $b \leftarrow\!\$\ \{0,1\},\ r \leftarrow\!\$\ \mathcal{R}$
5 : $c^* \leftarrow\!\$\ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, m_b; r)$
6 : $(m^*, r^*) \leftarrow (m_b, r)$
7 : $b' \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk}, \mathsf{id}^*, c^*)$
8 : **return** $[b = b']$

Oracle $O_{\mathsf{Dec}}(c_i)$

1 : $\mathsf{sk}_{\mathsf{id}^*} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}^*)$
2 : $(m, r) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}^*}, c_i)$
3 : **if** $(m, r) = (m^*, r^*)$ **then**
4 : **return** test
5 : **endif**
6 : **return** m

Figure 2 Attack game for the RCCA security [10].

The SM9 encryption scheme, called $\Pi_{\mathtt{SM9}}$ for short, is shown in Figure 1. As for the parameters, $\Pi_{\mathtt{SM9}}$ requires an asymmetric bilinear map $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, P_1, P_2)$, and three collision-resistant hash functions: $\mathsf{H}_1 : \mathcal{ID} \to \mathbb{Z}_p$, $\mathsf{KDF} : \mathbb{G}_1 \times \mathbb{G}_T \times \mathcal{M} \to \{0,1\}^{\ell_1}$, and $\mathsf{H} : \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$.

3 Defining RCCA security for IBE

We extend the definition of IND-RCCA by Phan and Pointcheval [10] as shown in Figure 2, to the identity-based setting. Our new security notion, called indistinguishability under adaptive identity-based relaxed chosen-ciphertext attack (IND-ID-RCCA), is defined within the security game depicted in Figure 3.

The decryption algorithm Dec described in Figure 3 is slightly from a typical one as it additionally outputs some partial randomness. This is because that in this work, we mainly follow the 3-round generic paradigm of RCCA construction by Phan and Pointcheval [10]. As we will show later, such an additional output is essential to achieve RCCA security as the adversary is unable to produce a ciphertext with the same randomness without querying it. More details will be given when we describe our construction later.

Definition 1 (IND-ID-RCCA security)**.** We say an IBE scheme Π is IND-ID-RCCA-secure, if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$ in Figure 3,

$$\mathsf{Adv}_{\mathcal{A},\Pi}^{\text{IND-ID-RCCA}}(\lambda) = |\Pr[b = b'] - 1/2| \leqslant \mathsf{negl}(\lambda).$$

$\text{IND-ID-RCCA}_{\Pi}^{\mathcal{A}}(1^\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\$\ \mathsf{Setup}(1^\lambda)$
$(m^*, r^*, \mathsf{id}^*) \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset$
$(m_0, m_1, \mathsf{id}^*) \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Ext}}, O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk})$
if $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **then**
  return $\perp$
endif
$b \leftarrow\!\$\ \{0,1\}$
$c^* \leftarrow\!\$\ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, m_b)$
$\mathsf{sk}_{\mathsf{id}^*} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}^*)$
$(m_b, r) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}^*}, c^*)$
$(m^*, r^*) \leftarrow (m_b, r)$
$b' \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Ext}}, O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk}, c^*)$
return $[b = b']$

Oracle $O_{\mathsf{Ext}}(\mathsf{id}_i)$

if $\mathsf{id}_i = \mathsf{id}^*$ **then**
  return $\perp$
endif
$\mathrm{List}^{\mathsf{id}}.\mathrm{append}(\mathsf{id}_i)$
return $\mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$

Oracle $O_{\mathsf{Dec}}(\mathsf{id}_i, c_i)$

$\mathsf{sk}_{\mathsf{id}_i} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$
$(m, r) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}_i}, c_i)$
if $(m, r) = (m^*, r^*)$ **then**
  return test
endif
return m

Figure 3 Attack game for the IND-ID-RCCA security.

$\text{IND-ID-RR}_{\Pi}^{\mathcal{A}}(1^\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\$\ \mathsf{Setup}(1^\lambda)$
$\mathsf{id}^* \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset$
$(c^*, \mathsf{id}^*) \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Ext}}, O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk})$
$\mathsf{sk}_{\mathsf{id}^*} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}^*)$
$(m^*, r^*) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}^*}, c^*)$
if $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **or** $m^* = \perp$ **then**
  return $\perp$
endif
$b \leftarrow\!\$\ \{0,1\}$
$c_0 \leftarrow\!\$\ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, m^*)$
$c_1 \leftarrow\!\$\ \mathsf{Rerand}(\mathsf{mpk}, \mathsf{id}^*, c^*)$
$b' \leftarrow\!\$\ \mathcal{A}^{O_{\mathsf{Ext}}, O_{\mathsf{Dec}}}(1^\lambda, \mathsf{mpk}, c_b)$
return $[b = b']$

Oracle $O_{\mathsf{Ext}}(\mathsf{id}_i)$

if $\mathsf{id}_i = \mathsf{id}^*$ **then**
  return $\perp$
endif
$\mathrm{List}^{\mathsf{id}}.\mathrm{append}(\mathsf{id}_i)$
return $\mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$

Oracle $O_{\mathsf{Dec}}(\mathsf{id}_i, c_i)$

if $\mathsf{id}_i = \mathsf{id}^*$ **then**
  return $\perp$
endif
$\mathsf{sk}_{\mathsf{id}_i} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$
$(m, r) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}_i}, c_i)$
return m

Figure 4 Security game of rerandomizability.

Definition 2 (Rerandomizability)**.** An IBE scheme Π is called rerandomizable if the following conditions are satisfied.

- **(Correctness)** There exists a PPT algorithm Rerand that takes as input ciphertext C and outputs a new ciphertext C'; and for $(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\$\, \mathsf{Setup}(1^\lambda)$, any $\mathsf{id} \in \{0,1\}^*$, $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$, any ciphertext C,

$$\Pr[\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, C') \neq \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, C) : C' \leftarrow\!\$\, \mathsf{Rerand}(C)] \leqslant \mathsf{negl}(\lambda);$$

- **(Indistinguishability)** For any PPT adversary $\mathcal{A}$ depicted in Figure 4,

$$\mathsf{Adv}_{\mathcal{A},\Pi}^{\text{IND-ID-RR}}(\lambda) = |\Pr[b = b'] - 1/2| \leqslant \mathsf{negl}(\lambda).$$

4 The proposed IBE scheme

The proposed scheme, called $\Pi_{\texttt{RCCA-SM9}}$, is depicted in Figure 5. As for the public parameters, $\Pi_{\texttt{RCCA-SM9}}$ also requires an asymmetric bilinear map $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, P_1, P_2)$. Let $\mathsf{F}, \mathsf{G}, \mathsf{H} : \mathbb{G}_T \to \mathbb{G}_T, \mathsf{H}_1, \mathsf{H}_1' : \mathcal{ID} \to \mathbb{Z}_p$ be collision-resistant hash functions.

- The correctness of decryption algorithm Dec: for any $(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\$\, \mathsf{Setup}(1^\lambda), \mathsf{id} \in \mathcal{ID}, m \in \mathcal{M}, C \leftarrow\!\$\, \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$ and $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$, in $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, C)$, we can verify the correctness

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

1 : $s_A \leftarrow\$ [1, p-1]$
2 : $s_B \leftarrow\$ [1, p-1]$
3 : $P_A \leftarrow [s_A]P_1$
4 : $P_B \leftarrow [s_B]P_1$
5 : $g_A \leftarrow \hat{e}(P_A, P_2)$
6 : $g_B \leftarrow \hat{e}(P_B, P_2)$
7 : $\mathsf{mpk} \leftarrow (P_A, P_B, g_A, g_B)$
8 : $\mathsf{msk} \leftarrow (s_A, s_B)$
9 : **return** $(\mathsf{mpk}, \mathsf{msk})$

$\mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$

1 : $(s_A, s_B) \leftarrow \mathsf{msk}$
2 : **if** $s_A + \mathsf{H}_1(\mathsf{id}) \equiv 0 \bmod p$ **then**
3 : **return** $\perp$
4 : **elseif** $s_B + \mathsf{H}_1'(\mathsf{id}) \equiv 0 \bmod p$ **then**
5 : **return** $\perp$
6 : **endif**
7 : $\mathsf{sk}_A \leftarrow [\frac{s_A}{s_A + \mathsf{H}_1(\mathsf{id})}]P_2,\ \mathsf{sk}_B \leftarrow [\frac{s_B}{s_B + \mathsf{H}_1'(\mathsf{id})}]P_2$
8 : **return** $\mathsf{sk}_{\mathsf{id}} \leftarrow (\mathsf{sk}_A, \mathsf{sk}_B)$

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

1 : $r \leftarrow\$ \mathbb{G}_T,\ s \leftarrow \mathsf{F}(r) \cdot m$
2 : $t \leftarrow \mathsf{G}(s) \cdot r,\ u \leftarrow \mathsf{H}(t) \cdot s$
3 : $(P_A, P_B, g_A, g_B) \leftarrow \mathsf{mpk}$
4 : $h_1 \leftarrow \mathsf{H}_1(\mathsf{id})$
5 : $h_2 \leftarrow \mathsf{H}_1'(\mathsf{id})$
6 : $Q_A \leftarrow [h_1]P_1 + P_A$
7 : $Q_B \leftarrow [h_2]P_1 + P_B$
8 : $x_A, x_B \leftarrow\$ [1, p-1]$
9 : $C_1 \leftarrow [x_A]Q_A,\ C_2 \leftarrow [x_B]Q_B$
10 : $C_3 \leftarrow g_A^{x_A} \cdot u,\ C_4 \leftarrow g_B^{x_B} \cdot t$
11 : $C = C_1 \| C_2 \| C_3 \| C_4$
12 : **return** C

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, C)$

1 : $C_1 \| C_2 \| C_3 \| C_4 \leftarrow C$
2 : $(\mathsf{sk}_A, \mathsf{sk}_B) \leftarrow \mathsf{sk}_{\mathsf{id}}$
3 : **if** $C_1 \notin \mathbb{G}_1^*$ **or** $C_2 \notin \mathbb{G}_1^*$ **then**
4 : **return** $\perp$
5 : **endif**
6 : $u \leftarrow C_3 / \hat{e}(C_1, \mathsf{sk}_A)$
7 : $t \leftarrow C_4 / \hat{e}(C_2, \mathsf{sk}_B)$
8 : $s \leftarrow u / \mathsf{H}(t)$
9 : $r \leftarrow t / \mathsf{G}(s)$
10 : $m \leftarrow s / \mathsf{F}(r)$
11 : **return** m

$\mathsf{Rerand}(\mathsf{mpk}, \mathsf{id}, C)$

1 : $(P_A, P_B, g_A, g_B) \leftarrow \mathsf{mpk}$
2 : $C_1 \| C_2 \| C_3 \| C_4 \leftarrow C$
3 : $x_A', x_B' \leftarrow\$ [1, p-1]$
4 : $h_1 \leftarrow \mathsf{H}_1(\mathsf{id})$
5 : $h_2 \leftarrow \mathsf{H}_1'(\mathsf{id})$
6 : $Q_A \leftarrow [h_1]P_1 + P_A$
7 : $Q_B \leftarrow [h_2]P_1 + P_B$
8 : $C_1' \leftarrow C_1 + [x_A']Q_A$
9 : $C_2' \leftarrow C_2 + [x_B']Q_B$
10 : $C_3' \leftarrow g_A^{x_A'} \cdot C_3$
11 : $C_4' \leftarrow g_B^{x_B'} \cdot C_4$
12 : **return** $C' \leftarrow C_1' \| C_2' \| C_3' \| C_4'$

Figure 5 Proposed IBE scheme $\Pi_{\text{RCCA-SM9}}$.

of steps 6 and 7 as follows:

$$\begin{aligned} C_3/\hat{e}(C_1, \mathsf{sk}_A) &= \frac{g_A^x \cdot u}{\hat{e}([x]Q_A, [\frac{s_A}{s_A + \mathsf{H}_1(\mathsf{id})}]P_2)} = \frac{\hat{e}(P_1, P_2)^{xs_A} \cdot u}{\hat{e}([x](\mathsf{H}_1(\mathsf{id}) + [s_A])P_1, [\frac{s_A}{s_A + \mathsf{H}_1(\mathsf{id})}]P_2)} \\ &= \frac{\hat{e}(P_1, P_2)^{xs_A} \cdot u}{\hat{e}([x]P_1, [s_A]P_2)} = \frac{\hat{e}(P_1, P_2)^{xs_A} \cdot u}{\hat{e}(P_1, P_2)^{xs_A}} = u, \\ C_4/\hat{e}(C_2, \mathsf{sk}_B) &= \frac{g_B^x \cdot t}{\hat{e}([x]Q_B, [\frac{s_B}{s_B + \mathsf{H}_1(\mathsf{id})}]P_2)} = \frac{\hat{e}(P_1, P_2)^{xs_B} \cdot t}{\hat{e}([x](\mathsf{H}_1(\mathsf{id}) + [s_B])P_1, [\frac{s_B}{s_B + \mathsf{H}_1(\mathsf{id})}]P_2)} \\ &= \frac{\hat{e}(P_1, P_2)^{xs_B} \cdot t}{\hat{e}([x]P_1, [s_B]P_2)} = \frac{\hat{e}(P_1, P_2)^{xs_B} \cdot t}{\hat{e}(P_1, P_2)^{xs_B}} = t. \end{aligned}$$

Steps 8–10 are just the inverse operations of the steps 2–4 of Enc, therefore

$$\Pr\left[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, C) = m \,\middle|\, \begin{array}{c} (\mathsf{mpk}, \mathsf{msk}) \leftarrow\$ \mathsf{Setup}(1^\lambda) \\ \mathsf{id} \in \mathcal{ID},\ \mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}) \\ m \in \mathcal{M},\ C \leftarrow\$ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m) \end{array}\right] = 1.$$

- The correctness of rerandomizability: for any $x' \leftarrow\$ [1, p-1]$, we have

$$\begin{aligned} C_1' &= C_1 + [x']Q_A \\ &= [x]Q_A + [x']Q_A \\ &= [x + x']Q_A, \end{aligned} \quad \begin{aligned} C_2' &= C_2 + [x']Q_B \\ &= [x]Q_B + [x']Q_B \\ &= [x + x']Q_B, \end{aligned} \quad \begin{aligned} C_3' &= g_A^{x'} \cdot C_3 \\ &= g_A^{x'} \cdot g_A^x \cdot u \\ &= g_A^{x+x'} \cdot u, \end{aligned} \quad \begin{aligned} C_4' &= g_B^{x'} \cdot C_3 \\ &= g_B^{x'} \cdot g_B^x \cdot t \\ &= g_B^{x+x'} \cdot t, \end{aligned}$$

therefore the output $C' = C_1' \| C_2' \| C_3' \| C_4'$ of $\mathsf{Rerand}(\mathsf{mpk}, \mathsf{id}, C)$ is the same as its input $C = C_1 \| C_2 \| C_3 \| C_4$ except that the underlying randomness x is replaced by $x + x'$ where x' is randomly sampled from $[1, p-1]$.

5 Security analysis

5.1 A new hardness assumption

Definition 3 (q-decision-BDHI (q-DBDHI) assumption [11]). Let $\hat{e}:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ be a bilinear pairing, where $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ are cyclic groups of prime order p generated by $P_1\in\mathbb{G}_1, P_2\in\mathbb{G}_2, P_T\in\mathbb{G}_T$ respectively. For any $\alpha\in\mathbb{Z}_p$ and $R\in\mathbb{G}_T$, given $(P_1,[\alpha]P_1,P_2,[\alpha]P_2,\ldots,[\alpha^q]P_2,R)$, there is no efficient algorithm that can determine whether R is equal to $\hat{e}(P_1,P_2)^{1/\alpha}$ or not. That is, for any efficient algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ with respective to the q-DBDHI problem $\mathsf{Adv}^{q\text{-}\mathsf{DBDHI}}_{\mathcal{A},\hat{e}}(\lambda)$ is negligible.

Lemma 1 (q-decision-BDHI* (q-DBDHI*) assumption). Let $\hat{e}:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ be a bilinear pairing, where $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ are cyclic groups of prime order p generated by $P_1\in\mathbb{G}_1, P_2\in\mathbb{G}_2, P_T\in\mathbb{G}_T$ respectively. If the decisional q-BDHI assumption holds in $\hat{e}$, then for any $\alpha,\beta\in\mathbb{Z}_p$ and $R\in\mathbb{G}_T$, given $(P_1,[\alpha]P_1,(h_0,[\beta(h_0+\alpha)]P_1),P_2,(h_1,[\frac{\alpha}{\alpha+h_1}]P_2),\ldots,(h_q,[\frac{\alpha}{\alpha+h_q}]P_2),R)$ where $h_i\in\mathbb{Z}_p,\alpha+h_i\neq 0$ and h_i are different from each other for $i=0,\ldots,q$, there is no efficient algorithm can determine whether R is equal to $\hat{e}(P_1,P_2)^{\alpha\beta}$ or not.

Proof. (Proof of Lemma 1) In this proof, we will show that if there is an adversary $\mathcal{A}$ who can solve the problem defined in Lemma 1 with advantage ε, then we can construct an adversary $\mathcal{B}$ who can solve the q-DBDHI problem (defined in Definition 3) with advantage $\varepsilon'\geqslant\varepsilon$.

When $\mathcal{B}$ obtains the decisional q-DBDHI problem instance $(P_1,[\alpha]P_1,P_2,[\alpha]P_2,\ldots,[\alpha^q]P_2,R)$ from its challenger, then it can play the role of challenger to $\mathcal{A}$ as follows:

(1) Randomly choose different $h_0,\ldots,h_q\in\mathbb{Z}_p$ where $[h_i]P_1+[\alpha]P_1\neq P_1$.

(2) Set $P_1'\leftarrow P_1$.

(3) Let $f(x):=(x-h_0+h_1)\cdot(x-h_0+h_2)\cdots(x-h_0+h_q)=x^q+w_{q-1}x^{q-1}+\cdots+w_1x+x$, where w_i is the coefficient of x^i for $i=0,\ldots,q-1$ in

$$(x-h_0+h_1)\cdot(x-h_0+h_2)\cdots(x-h_0+h_q)=x^q+w_{q-1}x^{q-1}+\cdots+w_1x+w_0.$$

(4) Set

$$\begin{aligned}P_2'\leftarrow[f(\alpha)]P_2&=[(\alpha-h_0+h_1)\cdot(\alpha-h_0+h_2)\cdots(\alpha-h_0+h_q)]P_2\\&=[\alpha^q+w_{q-1}\alpha^{q-1}+\cdots+w_1\alpha+w_0]P_2\\&=[\alpha^q]P_2+[w_{q-1}]\cdot[\alpha^{q-1}]P_2+\cdots+[w_1]\cdot[\alpha]P_2+[w_0]P_2.\end{aligned}$$

It is easy to see that P_2' can be computed with the problem instance.

(5) Let $\alpha'\leftarrow\alpha-h_0$ and $\beta'\leftarrow r/\alpha$ with a random number $r\in\mathbb{Z}_p$.

(6) Compute $[\alpha']P_1':=[\alpha-h_0]P_1=[\alpha]P_1-[h_0]P_1$ and $[\beta'(h_0+\alpha')]P_1':=\left[\frac{r}{\alpha}[h_0+(\alpha-h_0)]\right]P_1=[r]P_1$.

(7) For $i=1,\ldots,q$, compute

$$\begin{aligned}\left[\frac{\alpha'}{\alpha'+h_i}\right]P_2'&:=\left[\frac{\alpha-h_0}{\alpha-h_0+h_i}\right]\cdot[(\alpha-h_0+h_1)\cdot(\alpha-h_0+h_2)\cdots(\alpha-h_0+h_q)]P_2\\&=\left[(\alpha-h_0)\cdot\prod_{j=1,j\neq i}^{q}(\alpha-h_0+h_j)\right]P_2\\&=[\alpha^q+w'_{i,q-1}\alpha^{q-1}+\cdots+w'_{i,1}\alpha+w'_{i,0}]P_2\\&=[\alpha^q]P_2+[w'_{i,q-1}]\cdot[\alpha^{q-1}]P_2+\cdots+[w'_{i,1}]\cdot[\alpha]P_2+[w'_{i,0}]P_2,\end{aligned}$$

where $w'_{i,j}$ is the coefficient of α^j for $j=0,\ldots,q-1$ in

$$(\alpha-h_0)\cdot\prod_{j=1,j\neq i}^{q}(\alpha-h_0+h_j)=\alpha^q+w'_{i,q-1}\alpha^{q-1}+\cdots+w'_{i,1}\alpha+w'_{i,0}.$$

(8) Then

$$\hat{e}(P_1',P_2')^{\alpha'\beta'}=\hat{e}\left(P_1,[f(\alpha)]P_2\right)^{(\alpha-h_0)\cdot\frac{r}{\alpha}}=\hat{e}(P_1,P_2)^{\frac{r(\alpha-h_0)f(\alpha)}{\alpha}}=\hat{e}(P_1,P_2)^{r\cdot\frac{\alpha^{q+1}+\sum_{i=0}^{q}w_i''\alpha^i}{\alpha}}$$

$$= \left(\hat{e}(P_1, [\alpha^q]P_2) + \sum_{i=1}^{q} \hat{e}(P_1, [w_i'']\cdot[\alpha^{i-1}]P_1) + (\hat{e}(P_1,P_2)^{\frac{1}{\alpha}})^{w_0''} \right)^r,$$

where w_i'' is the coefficient of α^i for $i = 0, \ldots, q$ in $(\alpha - h_0)f(\alpha) = \alpha^{q+1} + \sum_{i=0}^{q} w_i''\alpha^i$. Therefore, if we set $R' \leftarrow (\hat{e}(P_1, [\alpha^q]P_2) + \sum_{i=1}^{q} \hat{e}(P_1, [w_i'']\cdot[\alpha^{i-1}]P_1) + R^{w_0''})^r$, where R is from the problem instance, we can note that $R = \hat{e}(P_1,P_2)^{\frac{1}{\alpha}}$ *iff.* $R' = \hat{e}(P_1', P_2')^{\alpha'\beta'}$.

(9) Send $(P_1', [\alpha']P_1', (h_0, [\beta'(h_0+\alpha')]P_1'), P_2', (h_1, [\frac{\alpha'}{\alpha'+h_1}]P_2'), \ldots, (h_q, [\frac{\alpha'}{\alpha'+h_q}]P_2'), R')$ to $\mathcal{A}$. Note that all the elements can be computed with the problem instance as shown in the above steps.

Since $R = \hat{e}(P_1,P_2)^{\frac{1}{\alpha}}$ iff. $R' = \hat{e}(P_1', P_2')^{\alpha'\beta'}$, if $\mathcal{A}$ can determine whether R' is equal to $\hat{e}(P_1', P_2')^{\alpha'\beta'}$ or not with advantage ε, then our $\mathcal{B}$ can determine whether R is equal to $\hat{e}(P_1,P_2)^{1/\alpha}$ by using the output of $\mathcal{A}$. Thus, the advantage that $\mathcal{B}$ solves the q-DBDHI problem is $\varepsilon' \geqslant \varepsilon$.

Definition 4 (q-gap-BDHI* (q-GBDHI*) assumption)**.** Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear pairing, where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of prime order p generated by $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2, P_T \in \mathbb{G}_T$ respectively. We say that the gap q-GBDHI* assumption holds in $\hat{e}$, if for any efficient adversary $\mathcal{A}$,

$$\Pr\left[\mathcal{A}^{O_{q\text{-}\mathsf{DBDHI}*}(\cdot)}\begin{pmatrix} P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), \\ P_2, (h_1, [\frac{\alpha}{\alpha+h_1}]P_2), \ldots, (h_q, [\frac{\alpha}{\alpha+h_q}]P_2)\end{pmatrix} = \hat{e}(P_1,P_2)^{\alpha\beta} : \alpha, \beta \leftarrow\$\, \mathbb{Z}_p\right] \leqslant \mathsf{negl}(\lambda),$$

where $O_{q\text{-}\mathsf{DBDHI}*}(\cdot)$ is a q-DBDHI* oracle, which takes as input $(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2, (h_1, [\frac{\alpha}{\alpha+h_1}]P_2), \ldots, (h_q, [\frac{\alpha}{\alpha+h_q}]P_2), R)$ and returns 1 if $R = \hat{e}(P_1,P_2)^{\alpha\beta}$ or 0 otherwise.

5.2 IND-ID-RCCA Security

Theorem 1. Assume $\mathsf{H}_1, \mathsf{H}_1' : \mathcal{ID} \to \mathbb{Z}_p$ are modeled as random oracles. If the q_{H_1}-GBDHI* assumption holds in $\hat{e}$ (q_{H_1} is the number of queries to H_1), then our proposed IBE $\Pi_{\mathtt{RCCA\text{-}SM9}}$ is IND-ID-RCCA secure.

Proof. (Proof of Theorem 1) We define a series of games, Game j for $j = 0, 1$, where Game 0 is the IND-ID-RCCA game played by $\mathcal{A}$ with respect to $\Pi_{\mathtt{RCCA\text{-}SM9}}$. In each game, b is the random bit chosen by the challenger, while b' is the bit output by $\mathcal{A}$ at the end of the game. For $j = 0, 1$, we use W_j to define the event that $b = b'$ in Game j.

$\mathsf{Game}_0(\lambda)$. The logic of the challenger in this game is shown in Figure 6.

The adversary $\mathcal{A}$ can make the extraction query, decryption query, H_1 random oracle query and H_1' random oracle query for multiple times, but can only make the encryption query for one time. In the initialization step, the challenger computes the master public/secret key pair $(\mathsf{mpk}, \mathsf{msk})$, sets $(m^*, r^*, \mathsf{id}^*) \leftarrow \perp$ and prepares an empty list $\mathrm{List}^{\mathsf{id}}$ as the actual game; it also initializes two empty associative arrays $\mathrm{Map}, \mathrm{Map}' : \mathcal{ID} \to \mathbb{Z}_p$ to record the responds in the random oracle queries. When $\mathcal{A}$ makes the extraction and decryption query, the challenger behaves as in the actual game, except that when the challenger needs to evaluate H_1 and H_1', random oracles are invoked instead. In each new random oracle query, the challenger responds with a random number sampled from $\mathbb{Z}_p$, and uses an associative array to record it. Note that except for extra bookkeeping, it is clear that the challenger behaves exactly as in the actual attack game. Therefore, we have

$$|\Pr[W_0] - 1/2| = \mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{A},\Pi_{\mathtt{RCCA\text{-}SM9}}}(\lambda). \tag{1}$$

$\mathsf{Game}_1(\lambda)$. In this game, we change the initialization and random oracle query steps as shown in Figure 7, where $q_{\mathsf{H}_1}, q_{\mathsf{H}_1'}$ are the total number of random oracle queries to $\mathsf{H}_1, \mathsf{H}_1'$ respectively.

The main purpose of such a change is that we want the challenger to decide the hash values in the initialization step. As for the challenge identity id^*, the challenger needs to ask random oracles to get h_1^* and h_2^*, but it does not know the exact index in the query. Therefore in lines (1) and (2) the challenger needs to guess the index i_1^*, i_2^* in H_1 and H_1' random oracles respectively (the corresponding responds are in lines (5) and (7)). From now on, the challenger behaves exactly as in Game 0. For consistency, an extra abort rule (line (8)) is added in the encryption query step as shown in Figure 8.

Therefore,

$$|\Pr[W_1] - \Pr[W_0]| \leqslant \frac{1}{q_{\mathsf{H}_1}\cdot q_{\mathsf{H}_1'}}. \tag{2}$$

Initialization:

$s_A \leftarrow\$ [1, p-1],\ s_B \leftarrow\$ [1, p-1],\ P_A \leftarrow [s_A]P_1,\ P_B \leftarrow [s_B]P_1$

$g_A \leftarrow \hat{e}(P_A, P_2),\ g_B \leftarrow \hat{e}(P_B, P_2),\ \mathsf{mpk} \leftarrow (P_A, P_B, g_A, g_B),\ \mathsf{msk} \leftarrow (s_A, s_B)$

$(m^*, r^*, \mathsf{id}^*) \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset,\ b \leftarrow\$ \{0,1\},$

initialize two empty associative arrays: $\mathsf{Map}, \mathsf{Map}' : \mathcal{ID} \to \mathbb{Z}_p$, send mpk to $\mathcal{A}$

Upon receiving an encryption query $(m_0, m_1, \mathsf{id}^*) \in \mathcal{M}^2 \times \mathcal{ID}$:

if $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **then return** $\perp$ **endif**

$h_1^* \leftarrow \mathsf{H}_1(\mathsf{id}^*),\ h_2^* \leftarrow \mathsf{H}_1'(\mathsf{id}^*)$

if $s_A + h_1^* \equiv 0 \bmod p$ **or** $s_B + h_2^* \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\mathsf{sk}_A^* \leftarrow [\frac{s_A}{s_A + h_1^*}]P_2,\ \mathsf{sk}_B^* \leftarrow [\frac{s_B}{s_B + h_2^*}]P_2$

$b \leftarrow\$ \{0,1\}, m^* \leftarrow m_b$

$r^* \leftarrow\$ \mathbb{G}_T,\ s^* \leftarrow \mathsf{F}(r^*) \cdot m^*,\ t^* \leftarrow \mathsf{G}(s^*) \cdot r^*,\ u^* \leftarrow \mathsf{H}(t^*) \cdot s^*$

$Q_A^* \leftarrow [h_1^*]P_1 + P_A,\ Q_B^* \leftarrow [h_2^*]P_1 + P_B, x_A^*, x_B^* \leftarrow\$ [1, p-1]$

$C_1^* \leftarrow [x_A^*]Q_A^*,\ C_2^* \leftarrow [x_B^*]Q_B^*,\ C_3^* \leftarrow g_A^{x_A^*} \cdot u^*,\ C_4^* \leftarrow g_B^{x_B^*} \cdot t^*,\ c^* \leftarrow C_1^* \| C_2^* \| C_3^* \| C_4^*$

send the challenger ciphertext c^* to $\mathcal{A}$

Upon receiving an extraction query $\mathsf{id}_i \in \mathcal{ID}$, where $\mathsf{id}_i \neq \mathsf{id}^*$:

$\mathrm{List}^{\mathsf{id}}.\mathrm{append}(\mathsf{id}_i),\ h_{i,1} \leftarrow \mathsf{H}_1(\mathsf{id}_i), h_{i,2} \leftarrow \mathsf{H}_1'(\mathsf{id}_i)$

if $s_A + h_{i,1} \equiv 0 \bmod p$ **or** $s_B + h_{i,2} \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\mathsf{sk}_{i,A} \leftarrow [\frac{s_A}{s_A + h_{i,1}}]P_2,\ \mathsf{sk}_{i,B} \leftarrow [\frac{s_B}{s_B + h_{i,2}}]P_2,\ \mathsf{sk}_{\mathsf{id}_i} \leftarrow (\mathsf{sk}_{i,A}, \mathsf{sk}_{i,B})$

send the secret key $\mathsf{sk}_{\mathsf{id}_i}$ to $\mathcal{A}$

Upon receiving a decryption query $(\mathsf{id}_i, c_i) \in \mathcal{ID} \times \mathcal{C}$:

$\mathsf{sk}_{\mathsf{id}_i} \leftarrow\$ \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$

$(m, r) \leftarrow \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}_i}, c_i)$

if $(m, r) = (m^*, r^*)$ **then return** test **endif**

return m

Upon receiving a H_1 random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

if $\mathsf{id}_i \notin \mathrm{Domain}(\mathsf{Map})$ **then** $\mathsf{Map}[\mathsf{id}_i] \leftarrow\$ \mathbb{Z}_p$ **endif**

send $\mathsf{Map}[\mathsf{id}_i]$ to $\mathcal{A}$

Upon receiving a H_1' random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

if $\mathsf{id}_i \notin \mathrm{Domain}(\mathsf{Map}')$ **then** $\mathsf{Map}'[\mathsf{id}_i] \leftarrow\$ \mathbb{Z}_p$ **endif**

send $\mathsf{Map}'[\mathsf{id}_i]$ to $\mathcal{A}$

Figure 6 Game 0 challenger in the proof of Theorem 1.

Then we will show that if the q_{H_1}-GBDHI* assumption holds in $\hat{e}$, $\Pr[W_1]$ is negligible.

Upon receiving the problem instance $(P_1, [\alpha]P_1, (h_0, [\beta(h_0 + \alpha)]P_1), P_2, (h_1, [\frac{\alpha}{\alpha + h_1}]P_2), \ldots, (h_{q_{\mathsf{H}_1}}, [\frac{\alpha}{\alpha + h_{q_{\mathsf{H}_1}}}]P_2))$, we set $s_A \leftarrow \alpha$, $(h_1^*, h_{1,1}, \ldots, h_{q_{\mathsf{H}_1},1}) \leftarrow (h_0, h_1, \ldots, h_{q_{\mathsf{H}_1}})$. One can see that the challenger is able to answer the extraction query, the decryption query, and the hash query. Thus, this game is equal to the RCCA attack game for the challenge identity id^*. It means that if there is no efficient adversary that wins this RCCA attack game [10], then $\Pr[W_1]$ is negligible. To show this, we need to rely on the following theorem from [10].

Theorem 2. Let $\mathcal{A}$ be an IND-ID-RCCA adversary against the OAEP 3-round construction with any trapdoor one-way probabilistic function family $(\varphi_{\mathsf{pk}})_{\mathsf{pk}}$, within time τ. Assume that after q_f, q_g, q_h and q_d queries to random oracles $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$, and the decryption oracle respectively, its advantage $\mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{A},\mathsf{oaep\text{-}3}}(\tau)$ is greater than ϵ. Then, $\mathsf{Succ}^{\mathsf{gap}}_{\varphi}(\tau', q_d(q_g q_h + q_d))$ is upper-bounded by

$$\frac{\varepsilon}{2} - q_d^2 \times \left(\frac{1}{2^l} + \frac{6}{2^k}\right) - (4q_d + 1) \times \left(\frac{q_g}{2^l} + \frac{q_f}{2^k}\right) - q_d \times \frac{q_f + 1}{2^k},$$

Initialization:

$s_A \leftarrow\$ [1, p-1],\ s_B \leftarrow\$ [1, p-1],\ P_A \leftarrow [s_A]P_1,\ P_B \leftarrow [s_B]P_1$

$g_A \leftarrow \hat{e}(P_A, P_2),\ g_B \leftarrow \hat{e}(P_B, P_2),\ \mathsf{mpk} \leftarrow (P_A, P_B, g_A, g_B),\ \mathsf{msk} \leftarrow (s_A, s_B)$

(1) $i_1^* \leftarrow\$ [1, q_{\mathsf{H}_1}], h_1^*, h_{1,1}, \cdots, h_{q_{\mathsf{H}_1},1} \leftarrow\$ \mathbb{Z}_p$

(2) $i_2^* \leftarrow\$ [1, q_{\mathsf{H}_1'}], h_2^*, h_{1,2}, \cdots, h_{q_{\mathsf{H}_1'},2} \leftarrow\$ \mathbb{Z}_p$

(3) $x'_A, x'_B, x''_A, x''_B \leftarrow\$ [1, p-1]$

$\mathsf{id}^* \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset,\ b \leftarrow\$ \{0,1\}$,

initialize two empty associative arrays: $\mathrm{Map}, \mathrm{Map}' : \mathcal{ID} \to \mathbb{Z}_p$, send mpk to $\mathcal{A}$

Upon receiving a H_1 random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

(4) **if** $\mathsf{id}_i \notin \mathrm{Domain}(\mathrm{Map})$ **then** $\mathrm{Map}[\mathsf{id}_i] \leftarrow h_{i,1}$ **endif**

(5) **if** $i = i_1^*$ **then** $\mathrm{Map}[\mathsf{id}_i] \leftarrow h_1^*$ **endif**

send $\mathrm{Map}[\mathsf{id}_i]$ to $\mathcal{A}$

Upon receiving a H_1' random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

(6) **if** $\mathsf{id}_i \notin \mathrm{Domain}(\mathrm{Map}')$ **then** $\mathrm{Map}'[\mathsf{id}_i] \leftarrow h_{i,2}$ **endif**

(7) **if** $i = i_2^*$ **then** $\mathrm{Map}'[\mathsf{id}_i] \leftarrow h_2^*$ **endif**

send $\mathrm{Map}'[\mathsf{id}_i]$ to $\mathcal{A}$

Figure 7 Initialization and random oracle query steps of Game 1 challenger in the proof of Theorem 1.

Upon receiving an encryption query $(m_0, m_1, \mathsf{id}^*) \in \mathcal{M}^2 \times \mathcal{ID}$:

if $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **then return** $\perp$ **endif**

$h_1^* \leftarrow \mathsf{H}_1(\mathsf{id}^*),\ h_2^* \leftarrow \mathsf{H}_1'(\mathsf{id}^*)$

(8) **if** $\mathsf{id}^* \neq \mathsf{id}_{i_1^*}$ **and** $\mathsf{id}^* \neq \mathsf{id}_{i_2^*}$ **then return** $\perp$ **endif**

if $s_A + h_1^* \equiv 0 \bmod p$ **or** $s_B + h_2^* \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\cdots$

send the challenger ciphertext c^* to $\mathcal{A}$

Figure 8 Encryption query step of Game 1 challenger in the proof of Theorem 1.

with $\tau' \leqslant \tau + (q_f + q_g + q_h + q_d)T_{\mathrm{lu}} + q_d^2 T_{\mathsf{Same}} + (q_d+1)q_g q_h(T_\varphi + T_{\mathsf{Same}})$, where T_φ is the time complexity for evaluating any function φ_{pk}, T_{Same} is the time for the decisional oracle $\mathsf{Same}_{\varphi_{\mathsf{pk}}}$ to give its answer, and T_{lu} is the time complexity for a look up in a list.

Note that the procedure from line 1 to line 4 in the encryption algorithm is indeed an implementation of OAEP 3-round construction. Then Theorem 2 implies that if the implementation from line 5 to line 13 could be viewed as a trapdoor one-way probabilistic function[2)], then there is no efficient adversary that can win the IND-ID-RCCA game for id^* described above.

Consider a function f as follows which is constructed from line 5 to line 13 of our proposed encryption algorithm:

$$f_{\mathsf{mpk},\mathsf{id}}((M_A, M_B), (x_A, x_B)) = C_1 \| C_2 \| C_3 \| C_4 = ([x_A]Q_A) \| ([x_B]Q_B) \| (g_A^{x_A} \cdot M_A) \| (g_B^{x_B} \cdot M_B),$$

where $\mathsf{mpk} = (P_A, P_B, g_A, g_B) = (P_A, P_B, \hat{e}(P_A, P_2), \hat{e}(P_B, P_2)) = ([s_A]P_1, [s_B]P_2, \hat{e}(P_1, P_2)^{s_A}, \hat{e}(P_1, P_2)^{s_B})$, $M_A, M_B \in \mathbb{G}_T$, $Q_A = [s_A + \mathsf{H}_1(\mathsf{id})]P_1$, $Q_B = [s_B + \mathsf{H}_1'(\mathsf{id})]P_1$ and $x_A, x_B \leftarrow\$ [1, p-1]$. The trapdoor $\mathsf{msk} = (s_A, s_B)$, and

$$f_{\mathsf{mpk},\mathsf{id}}^{-1}(C_1 \| C_2 \| C_3 \| C_4) = \left(\frac{C_3}{\hat{e}(C_1, [\frac{s_A}{s_A + \mathsf{H}_1(\mathsf{id})}]P_2)}, \frac{C_4}{\hat{e}(C_2, [\frac{s_B}{s_B + \mathsf{H}_1'(\mathsf{id})}])} \right).$$

2) A trapdoor one-way probabilistic function f is: 1. $f : E \times R \to F$ is a bijection; 2. without knowing the trapdoor. It is intractable to invert f in E, even for an adversary which has access to the decisional oracle $\mathsf{Same}_f(y, y')$ which answers whether $g(y) = g(y')$ (see [10] for more details).

Now we will prove that $f_{\mathsf{mpk},\mathsf{id}^*}$ is a trapdoor one-way probabilistic function.

One could see that $f_{\mathsf{mpk},\mathsf{id}} : \mathbb{G}_T^2 \times \mathbb{Z}_p^2 \to \mathbb{G}_1 \| \mathbb{G}_1 \| G_T \| G_T$ is a bijection.

Now consider a variant of the q-GBDHI* assumption: for any efficient adversary $\mathcal{A}$,

$$\Pr[\mathcal{A}^{O_{\mathsf{DBDHI}*}(\cdot)}(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2) = \hat{e}(P_1,P_2)^{\alpha\beta} : \alpha, \beta \leftarrow\$\, \mathbb{Z}_p] \leqslant \mathsf{negl}(\lambda),$$

where $O_{\mathsf{DBDHI}*}(\cdot)$ is a DBDHI* oracle, which takes as input $(P_1,\ [\alpha]P_1,\ (h_0, [\beta(h_0+\alpha)]P_1),\ P_2, R)$ and returns 1 if $R = \hat{e}(P_1,P_2)^{\alpha\beta}$ or 0 otherwise.

It is obvious that if the q-GBDHI* assumption holds in $\hat{e}$, then the variant also holds. Suppose there exists an adversary $\mathcal{A}$ who can invert $f_{\mathsf{mpk},\mathsf{id}^*}$ with the help of the decisional oracle $\mathsf{Same}_f(y, y')$, then we can construct an adversary $\mathcal{B}$ that breaks the variant problem as follows:

(1) Upon receiving the problem instance $(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2)$, $\mathcal{B}$ lets $\mathsf{H}_1(\mathsf{id}) \leftarrow h_0$, computes $h_B \leftarrow \mathsf{H}_1'(\mathsf{id})$, sets $s_B, x_B \leftarrow\$\, [1, p-1], R, M_B \leftarrow\$\, \mathbb{G}_T$,

$$C_1^* \| C_2^* \| C_3^* \| C_4^* \leftarrow ([\beta(h_0+\alpha)]P_1) \| ([x_B h_B]P_1 + [x_B] \cdot [\alpha]P_1) \| R \| (\hat{e}(P_1,P_2)^{s_B x_B} \cdot M_B),$$

and sends $C_1^* \| C_2^* \| C_3^* \| C_4^*$ to $\mathcal{A}$.

(2) Upon receiving a decisional oracle query $\mathsf{Same}_f(C_1 \| C_2 \| C_3 \| C_4, C_1' \| C_2' \| C_3' \| C_4')$, $\mathcal{B}$ responds with

$$O_{\mathsf{O}_{\mathsf{DBDHI}*}}(P_1, [\alpha]P_1, (h_0, C_1' - C_1), P_2, C_3'/C_3) \wedge O_{\mathsf{O}_{\mathsf{DBDHI}*}}(P_1, [s_B]P_1, (h_B, C_2' - C_2), P_2, C_4'/C_4).$$

(3) When $\mathcal{A}$ outputs the right image (M_1, M_2) of $C_1^* \| C_2^* \| C_3^* \| C_4^*$, then C_3^*/M_1 is the solution of the GBDHI* problem.

Therefore, there is no efficient adversary that can win the RCCA attack game for id^* described above. Thus, $\Pr[W_1]$ is negligible.

Putting all the above together, we conclude that $\mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{A},\Pi_{\mathtt{RCCA-SM9}}}(\lambda)$ is negligible.

5.3 Rerandomizability

Theorem 3. Assume $\mathsf{H}_1, \mathsf{H}_1' : \mathcal{ID} \to \mathbb{Z}_p$ are modeled as random oracles. If the q-DBDHI* assumption holds in $\hat{e}$ (where $q = \max(q_{\mathsf{H}_1}, q_{\mathsf{H}_1'})$), then our proposed IBE $\Pi_{\mathtt{RCCA-SM9}}$ is rerandomizable. In particular, for any efficient IND-ID-RR adversary $\mathcal{A}$ that attacks $\Pi_{\mathtt{RCCA-SM9}}$ as in Figure 4, and makes at most $q_{\mathsf{H}_1}, q_{\mathsf{H}_1'}$ queries to $\mathsf{H}_1, \mathsf{H}_1'$ random oracles respectively, there exist an IND-ID-RCCA adversary $\mathcal{B}$ with $\mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{B}_{\text{RCCA}},\Pi_{\mathtt{RCCA-SM9}}}(\lambda)$, a q_{H_1}-DBDHI* adversary $\mathcal{B}_1'$ with $\mathsf{Adv}^{q_{\mathsf{H}_1}\text{-DBDHI}*}_{\mathcal{B}_1',\hat{e}}(\lambda)$ and a $q_{\mathsf{H}_1'}$-DBDHI* adversary $\mathcal{B}_2'$ with $\mathsf{Adv}^{q_{\mathsf{H}_1'}\text{-DBDHI}*}_{\mathcal{B}_2',\hat{e}}(\lambda)$ such that

$$\mathsf{Adv}^{\text{IND-ID-RR}}_{\mathcal{A},\Pi_{\mathtt{RCCA-SM9}}}(\lambda) \leqslant \frac{1}{q_{\mathsf{H}_1} \cdot q_{\mathsf{H}_1'}} + \mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{B},\Pi_{\mathtt{RCCA-SM9}}}(\lambda) + 2 \cdot \mathsf{Adv}^{q_{\mathsf{H}_1}\text{-DBDHI}*}_{\mathcal{B}_1',\hat{e}}(\lambda) + 2 \cdot \mathsf{Adv}^{q_{\mathsf{H}_1'}\text{-DBDHI}*}_{\mathcal{B}_2',\hat{e}}(\lambda).$$

Proof. (Proof of Theorem 3) We define Game 0 to Game 7. In each game, b is the random bit chosen by the challenger, while b' is the bit output by $\mathcal{A}$ in the end of the game. For $j = 0, \ldots, 7$, we use W_j to define the event that $b = b'$ in Game j.

$\mathsf{Game}_0(\lambda)$. The logic of the challenger in this game is shown in Figure 9.

The adversary $\mathcal{A}$ can make the extraction query, decryption query, H_1 random oracle query and H_1' random oracle query for multiple times, but can only make the rerandomization/re-encryption query for one time. In the initialization step, the challenger computes $(\mathsf{mpk}, \mathsf{msk})$, sets $\mathsf{id}^* \leftarrow \perp$, prepares an empty list $\text{List}^{\mathsf{id}}$, and initializes two empty associative arrays $\text{Map}, \text{Map}' : \mathcal{ID} \to \mathbb{Z}_p$ to record the responds in the random oracle queries. When $\mathcal{A}$ makes extraction and decryption queries, the challenger behaves the same as in the actual game, except that when needs to evaluate H_1 and H_1', the challenger invokes random oracles. For each new random oracle query, the challenger responds with a random number sampled from $\mathbb{Z}_p$, and uses an associative array to record it. Note that except for extra bookkeeping, it is clear that the challenger behaves exactly as in the actual attack game. Therefore, we have

$$|\Pr[W_0] - 1/2| = \mathsf{Adv}^{\text{IND-ID-RR}}_{\mathcal{A},\Pi_{\mathtt{RCCA-SM9}}}(\lambda). \tag{3}$$

$\mathsf{Game}_1(\lambda)$. This game changes the initialization and random oracle query steps as shown in Figure 10, where $q_{\mathsf{H}_1}, q_{\mathsf{H}_1'}$ are the total numbers of random oracle queries to $\mathsf{H}_1, \mathsf{H}_1'$ respectively, and deletes the codes highlighted in the rerandomization/re-encryption query step in Game 0.

Initialization:

$s_A \leftarrow\$ [1, p-1],\ s_B \leftarrow\$ [1, p-1],\ P_A \leftarrow [s_A]P_1,\ P_B \leftarrow [s_B]P_1$

$g_A \leftarrow \hat{e}(P_A, P_2),\ g_B \leftarrow \hat{e}(P_B, P_2),\ \mathsf{mpk} \leftarrow (P_A, P_B, g_A, g_B),\ \mathsf{msk} \leftarrow (s_A, s_B)$

$\mathsf{id}^* \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset,\ b \leftarrow\$ \{0,1\},$ initialize two empty associative arrays: $\mathrm{Map}, \mathrm{Map}' : \mathcal{ID} \to \mathbb{Z}_p$

send the master public key mpk to $\mathcal{A}$

Upon receiving a rerandomization/re-encryption query $(c^*, \mathsf{id}^*) \in \mathcal{C} \times \mathcal{ID}$:

$h_1^* \leftarrow \mathsf{H}_1(\mathsf{id}^*),\ h_2^* \leftarrow \mathsf{H}_1'(\mathsf{id}^*)$

if $s_A + h_1^* \equiv 0 \bmod p$ **or** $s_B + h_2^* \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\mathsf{sk}_A^* \leftarrow [\frac{s_A}{s_A + h_1^*}]P_2,\ \mathsf{sk}_B^* \leftarrow [\frac{s_B}{s_B + h_2^*}]P_2,\ C_1^* \| C_2^* \| C_3^* \| C_4^* \leftarrow c^*$

if $C_1^* \notin \mathbb{G}_1^*$ **or** $C_2^* \notin \mathbb{G}_1^*$ **then return** $\perp$ **endif**

$u^* \leftarrow C_3^* / \hat{e}(C_1^*, \mathsf{sk}_A^*),\ t^* \leftarrow C_4^* / \hat{e}(C_2^*, \mathsf{sk}_B^*),\ s^* \leftarrow u^* / \mathsf{H}(t^*),\ r^* \leftarrow t^* / \mathsf{G}(s^*),\ m^* \leftarrow s^* / \mathsf{F}(r^*)$

if $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **or** $m^* = \perp$ **then return** $\perp$ **endif**

$r' \leftarrow\$ \mathbb{G}_T,\ s' \leftarrow \mathsf{F}(r') \cdot m^*,\ t' \leftarrow \mathsf{G}(s') \cdot r',\ u' \leftarrow \mathsf{H}(t') \cdot s'$

$Q_A^* \leftarrow [h_1^*]P_1 + P_A,\ Q_B^* \leftarrow [h_2^*]P_1 + P_B,\ x'_A, x'_B \leftarrow\$ [1, p-1], C_1' \leftarrow [x'_A]Q_A^*,$

$C_2' \leftarrow [x'_B]Q_B^*,\ C_3' \leftarrow g_A^{x'_A} \cdot u',\ C_4' \leftarrow g_B^{x'_B} \cdot t',\ c_0 \leftarrow C_1' \| C_2' \| C_3' \| C_4',\ x''_A, x''_B \leftarrow\$ [1, p-1]$

$C_1'' \leftarrow C_1^* + [x''_A]Q_A^*,\ C_2'' \leftarrow C_2^* + [x''_B]Q_B^*,\ C_3'' \leftarrow g_A^{x''_A} \cdot C_3^*,\ C_4'' \leftarrow g_B^{x''_B} \cdot C_4^*, c_1 \leftarrow C_1'' \| C_2'' \| C_3'' \| C_4''$

send the challenger ciphertext c_b to $\mathcal{A}$

Upon receiving an extraction query $\mathsf{id}_i \in \mathcal{ID}$, where $\mathsf{id}_i \neq \mathsf{id}^*$:

$\mathrm{List}^{\mathsf{id}}.\mathrm{append}(\mathsf{id}_i),\ h_{i,1} \leftarrow \mathsf{H}_1(\mathsf{id}_i), h_{i,2} \leftarrow \mathsf{H}_1'(\mathsf{id}_i)$

if $s_A + h_{i,1} \equiv 0 \bmod p$ **or** $s_B + h_{i,2} \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\mathsf{sk}_{i,A} \leftarrow [\frac{s_A}{s_A + h_{i,1}}]P_2,\ \mathsf{sk}_{i,B} \leftarrow [\frac{s_B}{s_B + h_{i,2}}]P_2,\ \mathsf{sk}_{\mathsf{id}_i} \leftarrow (\mathsf{sk}_{i,A}, \mathsf{sk}_{i,B})$

send the secret key $\mathsf{sk}_{\mathsf{id}_i}$ to $\mathcal{A}$

Upon receiving a decryption query $(\mathsf{id}_i, c_i) \in \mathcal{ID} \times \mathcal{C}$, where $\mathsf{id}_i \neq \mathsf{id}^*$:

$\mathsf{sk}_{\mathsf{id}_i} \leftarrow\$ \mathsf{Ext}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}_i)$

return $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}_i}, c_i)$

Upon receiving a H_1 random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

if $\mathsf{id}_i \notin \mathrm{Domain}(\mathrm{Map})$ **then** $\mathrm{Map}[\mathsf{id}_i] \leftarrow\$ \mathbb{Z}_p$ **endif**

send $\mathrm{Map}[\mathsf{id}_i]$ to $\mathcal{A}$

Upon receiving a H_1' random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

if $\mathsf{id}_i \notin \mathrm{Domain}(\mathrm{Map}')$ **then** $\mathrm{Map}'[\mathsf{id}_i] \leftarrow\$ \mathbb{Z}_p$ **endif**

send $\mathrm{Map}'[\mathsf{id}_i]$ to $\mathcal{A}$

Figure 9 Game 0 challenger in the proof of Theorem 3.

The purpose of such change is similar to $\mathsf{Game}_1(\lambda)$ in the proof of the Theorem 1. For consistency, line (8) is added in the rerandomization/re-encryption query step as shown in Figure 11.

Therefore,

$$|\Pr[W_1] - \Pr[W_0]| \leqslant \frac{1}{q_{\mathsf{H}_1} \cdot q_{\mathsf{H}_1'}}. \tag{4}$$

$\mathsf{Game}_2(\lambda)$. This game is same as Game 1, except that in the rerandomization/re-encryption query step $m^* \leftarrow s^*/\mathsf{F}(r^*)$ is replaced with $m^* \leftarrow\$ \mathcal{M}$. One could see that

$$|\Pr[W_2] - \Pr[W_1]| \leqslant \mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{B}, \Pi_{\text{RCCA-SM9}}}(\lambda) \tag{5}$$

for an efficient IND-ID-RCCA adversary $\mathcal{B}$ which works as follows. Upon receiving the rerandomization query (c^*, id^*), $\mathcal{B}$ forward the query to its IND-ID-RCCA challenger for decryption and gets the respond m^*. Then $\mathcal{B}$ sets $m_0 \leftarrow m^*, m_1 \leftarrow\$ \mathcal{M}$ and sends them to its IND-ID-RCCA challenger. The challenger chooses a random bit $b \leftarrow\$ \{0,1\}$, encrypts m_b and sends the corresponding ciphertext c to $\mathcal{B}$. Then $\mathcal{B}$ sends c to $\mathcal{A}$. For any other decryption oracle query from $\mathcal{A}$, $\mathcal{B}$ can ask its challenger's decryption oracle for help. Therefore, the combination of the IND-ID-RCCA challenger and $\mathcal{B}$ is equivalent to the role of the challenger to $\mathcal{A}$ in Game 1 when $b = 0$, or in Game 2 when $b = 1$. Therefore, when $\mathcal{A}$ outputs $\hat{b}$ at the end of the game, $\mathcal{B}$ outputs $\hat{b}$ as well.

Initialization:

$s_A \leftarrow\$ [1, p-1],\ s_B \leftarrow\$ [1, p-1],\ P_A \leftarrow [s_A]P_1,\ P_B \leftarrow [s_B]P_1$

$g_A \leftarrow \hat{e}(P_A, P_2),\ g_B \leftarrow \hat{e}(P_B, P_2),\ \mathsf{mpk} \leftarrow (P_A, P_B, g_A, g_B),\ \mathsf{msk} \leftarrow (s_A, s_B)$

(1) $i_1^* \leftarrow\$ [1, q_{\mathsf{H}_1}], h_1^*, h_{1,1}, \cdots, h_{q_{\mathsf{H}_1},1} \leftarrow\$ \mathbb{Z}_p$

(2) $i_2^* \leftarrow\$ [1, q_{\mathsf{H}_1'}], h_2^*, h_{1,2}, \cdots, h_{q_{\mathsf{H}_1'},2} \leftarrow\$ \mathbb{Z}_p$

(3) $x'_A, x'_B, x''_A, x''_B \leftarrow\$ [1, p-1]$

$\mathsf{id}^* \leftarrow \perp,\ \mathrm{List}^{\mathsf{id}} \leftarrow \emptyset,\ b \leftarrow\$ \{0,1\},$ initialize two empty associative arrays: $\mathsf{Map}, \mathsf{Map}' : \mathcal{ID} \to \mathbb{Z}_p$

send the master public key mpk to $\mathcal{A}$

Upon receiving a H_1 random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

(4) **if** $\mathsf{id}_i \notin$ Domain(Map) **then** $\mathsf{Map}[\mathsf{id}_i] \leftarrow h_{i,1}$ **endif**

(5) **if** $i = i_1^*$ **then** $\mathsf{Map}[\mathsf{id}_i] \leftarrow h_1^*$ **endif**

send $\mathsf{Map}[\mathsf{id}_i]$ to $\mathcal{A}$

Upon receiving a H_1' random oracle query $\mathsf{id}_i \in \mathcal{ID}$:

(6) **if** $\mathsf{id}_i \notin$ Domain(Map') **then** $\mathsf{Map}'[\mathsf{id}_i] \leftarrow h_{i,2}$ **endif**

(7) **if** $i = i_2^*$ **then** $\mathsf{Map}'[\mathsf{id}_i] \leftarrow h_2^*$ **endif**

send $\mathsf{Map}'[\mathsf{id}_i]$ to $\mathcal{A}$

Figure 10 Initialization and random oracle query steps of Game 1 challenger in the proof of Theorem 3.

Upon receiving a rerandomization/re-encryption query $(c^*, \mathsf{id}^*) \in \mathcal{C} \times \mathcal{ID}$:

$h_1^* \leftarrow \mathsf{H}_1(\mathsf{id}^*),\ h_2^* \leftarrow \mathsf{H}_1'(\mathsf{id}^*)$

(8) **if** $\mathsf{id}^* \neq \mathsf{id}_{i_1^*}$ **and** $\mathsf{id}^* \neq \mathsf{id}_{i_2^*}$ **then return** $\perp$ **endif**

if $s_A + h_1^* \equiv 0 \bmod p$ **or** $s_B + h_2^* \equiv 0 \bmod p$ **then return** $\perp$ **endif**

$\cdots$

send the challenger ciphertext c_b to $\mathcal{A}$

Figure 11 Rerandomization/re-encryption query step of Game 1 challenger in the proof of Theorem 3.

Upon receiving a rerandomization/re-encryption query $(c^*, \mathsf{id}^*) \in \mathcal{C} \times \mathcal{ID}$:

$h_1^* \leftarrow \mathsf{H}_1(\mathsf{id}^*),\ h_2^* \leftarrow \mathsf{H}_1'(\mathsf{id}^*),$ **if** $\mathsf{id}^* \neq \mathsf{id}_{i_1^*}$ **and** $\mathsf{id}^* \neq \mathsf{id}_{i_2^*}$ **then return** $\perp$ **endif**

$C_1^* \| C_2^* \| C_3^* \| C_4^* \leftarrow c^*,$ **if** $C_1^* \notin \mathbb{G}_1^*$ **or** $C_2^* \notin \mathbb{G}_1^*$ **then return** $\perp$ **endif**

$m^* \leftarrow\$ \mathcal{M},$ **if** $\mathsf{id}^* \in \mathrm{List}^{\mathsf{id}}$ **then return** $\perp$ **endif**

$r' \leftarrow\$ \mathbb{G}_T,\ s' \leftarrow \mathsf{F}(r') \cdot m^*,\ t' \leftarrow \mathsf{G}(s') \cdot r',\ u' \leftarrow \mathsf{H}(t') \cdot s',\ Q_A^* \leftarrow [h_1^*]P_1 + P_A,\ Q_B^* \leftarrow [h_2^*]P_1 + P_B$

(9) $C_1' \leftarrow [x'_A]Q_A^*,\ C_2' \leftarrow [x'_B]Q_B^*,\ C_3' \leftarrow g_A^{x'_A} \cdot u',\ C_4' \leftarrow g_B^{x'_B} \cdot t',\ c_0 \leftarrow C_1' \| C_2' \| C_3' \| C_4'$

(10) $C_1'' \leftarrow C_1^* + [x''_A]Q_A^*,\ C_2'' \leftarrow C_2^* + [x''_B]Q_B^*,\ C_3'' \leftarrow g_A^{x''_A} \cdot C_3^*,\ C_4'' \leftarrow g_B^{x''_B} \cdot C_4^*, c_1 \leftarrow C_1'' \| C_2'' \| C_3'' \| C_4''$

send the challenger ciphertext c_b to $\mathcal{A}$

Figure 12 Rerandomization/re-encryption query step of Game 3 challenger in the proof of Theorem 3.

$\mathsf{Game}_3(\lambda)$. This game changes the rerandomization/re-encryption query step as shown in Figure 12.

The idea behind this setting is that since m^* is randomly chosen, the challenger does not need to encrypt c^* in the re-encryption process and does not need to extract the secret key for id^* neither. Thus, we have

$$\Pr[W_3] = \Pr[W_2]. \tag{6}$$

$\mathsf{Game}_4(\lambda)$. In Game 4, $C_3' \leftarrow g_A^{x'_A} \cdot u'$ (in Game 3) is replaced with $R_1 \leftarrow\$ \mathbb{G}_T,\ C_3' \leftarrow R_1 \cdot u'$. We show that

$$|\Pr[W_4] - \Pr[W_3]| \leqslant \mathsf{Adv}^{q_{\mathsf{H}_1}\text{-DBDHI*}}_{\mathcal{B}_1', \hat{e}}(\lambda) \tag{7}$$

for an efficient q_{H_1}-DBDHI* adversary $\mathcal{B}_1'$ which works as follows. After receiving the problem instance $(P_1,\ [\alpha]P_1,\ (h_0,\ [\beta(h_0+\alpha)]P_1),\ P_2,\ (h_1, [\frac{\alpha}{\alpha+h_1}]P_2), \ldots, (h_{q_{\mathsf{H}_1}}, [\frac{\alpha}{\alpha+h_{q_{\mathsf{H}_1}}}]P_2), R)$, $\mathcal{B}_1'$ plays the role

of the challenger role to $\mathcal{A}$ in Game 3 by using the given problem instance. Instead of sampling $h_1^*, h_{1,1}, \ldots, h_{q_{\mathsf{H}_1},1} \leftarrow\$\, \mathbb{Z}_p$ in line (1), $\mathcal{B}_1'$ sets $(h_1^*, h_{1,1}, \ldots, h_{q_{\mathsf{H}_1},1}) \leftarrow (h_0, h_1, \ldots, h_{q_{\mathsf{H}_1}})$. Let $s_A = \alpha$, then $P_A = [\alpha]P_1$, and the secret key $\mathsf{sk}_{i,A}$ for id_i is equal to $[\frac{\alpha}{\alpha+h_i}]P_2$. Although $\mathcal{B}_1'$ does not know the value of α which is a part of the master secret key msk, it can still simulate the extraction and decryption oracles using the problem instance well. Now $x_A' \leftarrow\$\, [1, p-1]$ in line (3) is replaced by $x_A' \leftarrow\$\, \beta$, then in the rerandomization/re-encryption query step, one have $C_1' = [\beta(h_0+\alpha)]P_1$. Furthermore, $C_3' \leftarrow g_A^{x_A'} \cdot u'$ is changed to $C_3' \leftarrow R \cdot u'$. Now, one can see that if $R = \hat{e}(P_1, P_2)^{\alpha\beta}$, then this is equivalent to Game 3; othereise, this is equivalent to Game 4. At the end of the game, $\mathcal{B}_1'$ outputs 1 if $\hat{b} = b$ and 0 otherwise.

$\mathsf{Game}_5(\lambda)$. In this game, Game 4 is modified by replacing $C_4' \leftarrow g_B^{x_B'} \cdot t'$ with $R_2 \leftarrow\$\, \mathbb{G}_T, C_4' \leftarrow R_2 \cdot t'$. With the similar analysis as done in Game 4, one has

$$|\Pr[W_5] - \Pr[W_4]| \leqslant \mathsf{Adv}^{q_{\mathsf{H}_1'}\text{-DBDHI}*}_{\mathcal{B}_2',\hat{e}}(\lambda). \tag{8}$$

$\mathsf{Game}_6(\lambda)$. Since C_1', C_2', C_3', C_4' are independent of each other, line (9) in Game 5 could be modified to $c_0 \leftarrow\$\, \mathbb{G}_1 \| \mathbb{G}_1 \| \mathbb{G}_T \| \mathbb{G}_T$. It is clear that

$$\Pr[W_6] = \Pr[W_5]. \tag{9}$$

$\mathsf{Game}_7(\lambda)$. This game is same as Game 6, except that line (10) is changed to $c_1 \leftarrow\$\, \mathbb{G}_1 \| \mathbb{G}_1 \| \mathbb{G}_T \| \mathbb{G}_T$. With the similar analysis as done from Game 4 to Game 6, one has

$$|\Pr[W_7] - \Pr[W_6]| \leqslant \mathsf{Adv}^{q_{\mathsf{H}_1}\text{-DBDHI}*}_{\mathcal{B}_1',\hat{e}}(\lambda) + \mathsf{Adv}^{q_{\mathsf{H}_1'}\text{-DBDHI}*}_{\mathcal{B}_2',\hat{e}}(\lambda). \tag{10}$$

Now, both c_0 and c_1 are randomly chosen from the ciphertext space $\mathcal{C} = \mathbb{G}_1 \| \mathbb{G}_1 \| \mathbb{G}_T \| \mathbb{G}_T$, so the adversary $\mathcal{A}$ can only distinguish them with probability 1/2. Therefore

$$\Pr[W_7] = 1/2. \tag{11}$$

Combining (3)–(11), we have

$$\mathsf{Adv}^{\text{IND-ID-RR}}_{\mathcal{A},\Pi_{\text{RCCA-SM9}}}(\lambda) \leqslant \frac{1}{q_{\mathsf{H}_1} \cdot q_{\mathsf{H}_1'}} + \mathsf{Adv}^{\text{IND-ID-RCCA}}_{\mathcal{B},\Pi_{\text{RCCA-SM9}}}(\lambda) + 2 \cdot \mathsf{Adv}^{q_{\mathsf{H}_1}\text{-DBDHI}*}_{\mathcal{B}_1',\hat{e}}(\lambda) + 2 \cdot \mathsf{Adv}^{q_{\mathsf{H}_1'}\text{-DBDHI}*}_{\mathcal{B}_2',\hat{e}}(\lambda).$$

6 Conclusion

In this paper, we enhance the security of the SM9 IBE scheme against subversion attacks. We design a new variant of the SM9 IBE scheme that offers RCCA security while enjoys rerandomizability. This distinctive feature allows us to use the notion of CRF to efficiently rerandomize SM9 IBE ciphertexts, thereby enhancing their resistance to subversion. To prove the security of our proposed scheme, we introduce a new hardness assumption and conduct a comprehensive security analysis.

Looking ahead, there are several intriguing avenues for future research. One compelling direction is the design of an efficient RCCA-secure SM9 IBE scheme within the standard model, eliminating the reliance on random oracles. Additionally, it would be worthwhile to explore effective strategies to bolster subversion resilience for other cryptographic algorithms of SM9, such as the authenticated key exchange protocol and signature scheme.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62122092, 62032005).

References

1 Lu S Q, Zheng J H, Cao Z F, et al. A survey on cryptographic techniques for protecting big data security: present and forthcoming. Sci China Inf Sci, 2022, 65: 201301
2 Young A, Yung M. Kleptography: using cryptography against cryptography. In: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'97), 1997. 62–74
3 Young A, Yung M. The prevalence of kleptographic attacks on discrete-log based cryptosystems. In: Proceedings of the 17th Annual International Cryptology Conference (CRYPTO'97), 1997. 264–276
4 Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2015), 2015. 657–686
5 Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2002), 2002. 45–64

6 Hong H B, Shao J, Wang L C, et al. A CCA secure public key encryption scheme based on finite groups of Lie type. Sci China Inf Sci, 2022, 65: 119102
7 Pan J, Zhang J, Zhang F G, et al. Lattice-based group encryptions with only one trapdoor. Sci China Inf Sci, 2022, 65: 152304
8 Zhang J, Yu Y, Fan S Q, et al. Improved lattice-based CCA2-secure PKE in the standard model. Sci China Inf Sci, 2020, 63: 182101
9 Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines. In: Proceedings of the 36th Annual International Cryptology Conference (CRYPTO 2016), 2016. 341–372
10 Phan D H, Pointcheval D. OAEP 3-round: a generic and secure asymmetric encryption padding. In: Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2004), 2004. 63–77
11 Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004), 2004. 223–238
12 An J H, Dodis Y, Rabin T. On the security of joint signature and encryption. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam (EUROCRYPT 2002), 2002. 83–107
13 Chen R, Wang Y, Huang X Y. RCCA-secure public-key encryption based on SM2 (in Chinese). Sci Sin Inform, 2023, 53: 266–281
14 Canetti R, Krawczyk H, Nielsen J B. Relaxing chosen-ciphertext security. In: Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003), 2003. 565–582
15 Golle P, Jakobsson M, Juels A, et al. Universal re-encryption for mixnets. In: Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA 2004), 2004. 163–178
16 Groth J. Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In: Proceedings of the 1st Theory of Cryptography Conference (TCC 2004), 2004. 152–170
17 Prabhakaran M, Rosulek M. Rerandomizable RCCA encryption. In: Proceedings of the 27th Annual International Cryptology Conference (CRYPTO 2007), 2007. 517–534
18 Libert B, Peters T, Qian C. Structure-preserving chosen-ciphertext security with shorter verifiable ciphertexts. In: Proceedings of the 20th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC 2017), 2017. 247–276
19 Faonio A, Fiore D, Herranz J, et al. Structure-preserving and re-randomizable rcca-secure public key encryption and its applications. In: Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2019). 2019. 159–190
20 Faonio A, Fiore D. Improving the efficiency of re-randomizable and replayable CCA secure public key encryption. In: Proceedings of the 18th International Conference on Applied Cryptography and Network Security (ACNS 2020), 2020. 271–291
21 Wang Y, Chen R M, Yang G M, et al. Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved. In: Proceedings of the 41st Annual International Cryptology Conference (CRYPTO 2021), 2021. 270–300
22 Wang Y, Chen R M, Huang X Y, et al. Identity-based encryption for fair anonymity applications: defining, implementing, and applying rerandomizable RCCA-secure IBE. In: Proceedings of the 27th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2021), 2021. 427–455
23 Gentry C. Practical identity-based encryption without random oracles. In: Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2006), 2006. 445–464