Foundations of Single-Decryptor Encryption

Fuyuki Kitagawa[1,2] and Takashi Yamakawa[1,2]

[1]NTT Social Informatics Laboratories, Tokyo, Japan

{fuyuki.kitagawa,takashi.yamakawa}@ntt.com

[2]NTT Research Center for Theoretical Quantum Information, Atsugi, Japan

April 17, 2026

Abstract

Single decryptor encryption (SDE) is public key encryption (PKE) where the decryption key is an unclonable quantum state. Coladangelo, Liu, Liu, and Zhandry (CRYPTO 2021) realized the first SDE assuming subexponentially secure indistinguishability obfuscation (iO) and one-way functions (OWFs), along with the polynomial hardness of the learning with errors (LWE) assumption. Since then, SDE has played a pivotal role in recent advances in quantum cryptography. However, despite its central importance in unclonable cryptography, many fundamental questions about SDE remain unanswered. For example, a line of works has proposed various security notions for SDE, but their relationships have hardly been discussed. Moreover, while many subsequent works have adopted the construction methodology of Coladangelo et al., none have explored its improvement, leaving the possibility of a more efficient approach to SDE.

In this work, we address these fundamental questions concerning SDE. Our contributions are threefold.

New security notion: We introduce a strengthened indistinguishability-based security notion for SDE, which we call CPA$^+$anti-piracy security. We show that CPA$^+$security unifies the existing security notions for SDE, as detailed in the third item.

New construction: We present an SDE scheme that satisfies CPA$^+$anti-piracy security, based solely on polynomially secure iO and OWFs. In addition to relying on weaker and more general assumptions, our SDE scheme offers a significant advantage over the scheme of Coladangelo et al., as both the construction and its security proof are much simpler.

Relationships among security notions: We demonstrate that CPA$^+$anti-piracy security implies all existing security notions for SDE, with the sole exception of identical challenge ciphertext security proposed by Georgiou and Zhandry (EPRINT 2020). Although we do not establish a direct implication from CPA$^+$anti-piracy security to identical challenge ciphertext security, we provide a generic transformation from an SDE scheme satisfying the former to one achieving the latter in the quantum random oracle model. Additionally, we establish various relationships among different security notions for SDE. By combining these results with our SDE construction, we derive several new feasibility results.

We further show that our CPA$^+$anti-piracy security enjoys additional robustness properties. In particular, it is preserved under parallel composition, yielding a way to expand the message space of SDE while maintaining security. We also show that it is robust to arbitrary correlations between the challenge bits for the second-stage adversaries. To capture this setting, we introduce correlated-challenge-bits CPA anti-piracy security, parameterized by an arbitrary joint distribution on the challenge bits, and show that CPA$^+$anti-piracy security implies this notion.

Contents

1 Introduction **3**
- 1.1 Backgrounds . . . 3
- 1.2 Our Results . . . 4
- 1.3 Subsequent Work . . . 7
- 1.4 Related Works . . . 7

2 Technical Overview **7**
- 2.1 SDE based on iO and OWFs . . . 8
- 2.2 Implications from CPA$^+$ to Other Security Notions . . . 10

3 Preliminaries **11**
- 3.1 Classical Cryptographic Primitives . . . 12
- 3.2 Gentle Measurement Lemma . . . 12
- 3.3 Useful Lemmata . . . 12
- 3.4 Projective and Threshold Implementations . . . 13

4 New Security Definition of Single-Decryptor Encryption **15**
- 4.1 Syntax . . . 15
- 4.2 New Security Definition: CPA$^+$ Anti-Piracy Security . . . 15

5 Construction of SDE with CPA$^+$ Anti-Piracy **16**
- 5.1 Strong Monogamy Property of Coset States . . . 16
- 5.2 Construction . . . 17
- 5.3 Proof of Security . . . 19

6 Relationship among Security Definitions **21**
- 6.1 Existing Security Definitions and Their Generalizations . . . 21
- 6.2 CPA$^+$ Anti-Piracy Implies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA Anti-Piracy . . . 24
- 6.3 $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA Anti-Piracy Implies $\mathcal{D}_{\mathsf{unp}}$-Search Anti-Piracy . . . 25
- 6.4 Equivalence between CPA$^+$ and Strong Anti-Piracy . . . 26

7 Simultaneous Double-Sided One-Way to Hiding Lemma **30**

8 Achieving $\mathcal{D}_{\mathsf{identical}}$-CPA Anti-Piracy Security in the QROM **35**
- 8.1 Augmented $\mathsf{Id}_{\mathcal{U}}$-Search Anti-Piracy Security . . . 36
- 8.2 Augmented Identical-Challenge Search Anti-Piracy Security . . . 37
- 8.3 $\mathcal{D}_{\mathsf{identical}}$-CPA Anti-Piracy Security in the QROM . . . 39

9 From Search to CPA$^+$ Anti-Piracy **41**

10 Parallel Composition Theorem **42**

11 CPA Anti-Piracy under Arbitrarily Correlated Challenge Bits **45**

1 Introduction

1.1 Backgrounds

Unclonable cryptography. Quantum information introduces novel cryptographic primitives that go beyond the scope of classical cryptography. A cornerstone of these advancements is the non-cloning principle of quantum states, which has enabled remarkable unclonable cryptographic primitives. Notable examples include quantum money [Wie83], quantum copy-protection [Aar09], unclonable encryption [BL20], one-shot signatures [AGKZ20], and single-decryptor encryption [GZ20, CLLZ21].

Single-decryptor encryption (SDE). In this work, we address fundamental unanswered questions about SDE, the notion first introduced by Georgiou and Zhandry [GZ20]. SDE is public key encryption (PKE) where the decryption key is an unclonable quantum state. Specifically, it guarantees that any adversary who is given a single quantum decryption key cannot generate two (possibly entangled) quantum states both of which can be used to decrypt freshly generated ciphertexts.

Coladangelo, Liu, Liu, and Zhandry [CLLZ21] realized the first SDE assuming subexponentially secure indistinguishability obfuscation (iO) and one-way functions (OWFs), and the polynomial hardness of the learning with errors (LWE) assumption. Since then, SDE has played a pivotal role in recent exciting results in quantum cryptography. For example, the SDE construction by [CLLZ21] has served as the foundation for constructions of copy protection for pseudorandom functions and signatures [CLLZ21, LLQZ22], unclonable puncturable obfuscation [AB24], and unbounded leakage resilient encryption [ÇGLZR24], and so on.

Despite its central role in unclonable cryptography, many fundamental questions about SDE remain unanswered. These questions span security notions and construction methods, as elaborated below.

Security notions for SDE. Similar to classical PKE, we can define indistinguishability and search (i.e., one-wayness) security for SDE. Coladangelo et al. [CLLZ21] introduced an indistinguishability-based security notion called chosen plaintext attack (CPA)-style anti-piracy security, as well as a search anti-piracy security notion called random-challenge anti-piracy security. While one might expect the former to imply the latter as in the case of classical PKE, Coladangelo et al. left this implication as an open question. In fact, they argued that this implication is unlikely to hold under their definitions.[1]

Beyond these two basic security notions, additional security notions for SDE have been considered in prior works. These include identical challenge ciphertext security [GZ20], strong anti-piracy security [CLLZ21], and same challenge-bit security [AB24]. However, the relationships among these notions have remained largely unexplored.

This naturally raises the following question:

Can we define a single security notion for SDE that unifies the existing notions?

Establishing such a unified notion is not only theoretically appealing, but also useful as a foundation for future constructions and security analyses.

Moreover, a satisfactory unified notion should ideally enjoy additional robustness properties. For example, none of the existing notions are known to be preserved under parallel composition, leaving open whether one can expand the message space of SDE while maintaining security. Likewise, existing indistinguishability-based notions typically fix a particular joint distribution on the challenge bits for the second stage adversaries, whereas it is natural to ask for security guarantees that remain meaningful even when those bits are correlated arbitrarily. In this work, we address these issues as well.

Construction method for SDE. State-of-the-art SDE construction by Coladangelo et al. [CLLZ21] relies on subexponentially secure iO and OWFs and polynomial hardness of the LWE assumption, as stated above. Currently, iO appears unavoidable for realizing SDE due to its implication to public key quantum money whose realization without

[1] See Appendix D.4 of [CLLZ21].

using iO is one of the biggest open questions in quantum cryptography.[2] Nevertheless, given that public key quantum money is realized based only on polynomially secure iO and OWFs [Zha19], we have the following natural question.

Can we construct SDE based only on polynomially secure iO and OWFs?

This work aims to address this question with a *simpler* construction and security proof than those of [CLLZ21]. As stated above, the SDE construction by [CLLZ21] has been used in many subsequent works, and the usage is non-black-box in almost all of them. Establishing a cleaner approach for SDE would greatly benefit subsequent studies in quantum cryptography.

1.2 Our Results

Our contributions are threefold.

New security notion: We introduce a strengthened version of CPA-style anti-piracy security, which we call CPA$^+$ anti-piracy security. We show that CPA$^+$ security unifies the existing security notions for SDE as detailed in the third item.

New construction: We present an SDE scheme that satisfies CPA$^+$ anti-piracy security, based solely on polynomially secure iO and OWFs. In addition to relying on weaker and more general assumptions, our SDE scheme offers a significant advantage over the scheme of [CLLZ21], as both the construction and its security proof are much simpler.

Relationships among security notions: We demonstrate that CPA$^+$ anti-piracy security implies all existing security notions for SDE, with the sole exception of identical challenge ciphertext security. Although we do not establish a direct implication from CPA$^+$ anti-piracy security to identical challenge ciphertext security, we provide a generic transformation from an SDE scheme satisfying the former to one achieving the latter in the quantum random oracle model. Additionally, we explore various relationships among different security notions for SDE. By combining these results with our SDE construction, we derive several new feasibility insights.

In addition to these main contributions, we establish two further robustness properties of CPA$^+$ anti-piracy security. First, we prove that CPA$^+$ anti-piracy security is preserved under parallel composition, yielding a way to expand the message space of SDE while maintaining security. Second, we introduce correlated-challenge-bits CPA anti-piracy security, which allows the challenge bits for the second stage adversaries to follow an arbitrary joint distribution, and show that CPA$^+$ anti-piracy security also guarantees security in this generalized setting.

We discuss these contributions and robustness properties in detail below.

New security notion: CPA$^+$ anti-piracy security. We first quickly review CPA-style anti-piracy security introduced in [CLLZ21]. It is defined by using the following security game played between the challenger and a tuple of three adversaries $(\mathcal{A}, \mathcal{B}, \mathcal{C})$.

1. $\mathcal{A}$ is given the public key pk and a quantum decryption key $s\mathsf{k}$ and outputs the challenge message tuple $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and a bipartite state q over the registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$.
2. $\mathcal{B}$ (resp. $\mathcal{C}$) is given the register $\mathsf{R}_{\mathcal{B}}$ (resp, $\mathsf{R}_{\mathcal{C}}$) and its challenge ciphertext $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$ for $\mathsf{coin}_{\mathcal{B}} \leftarrow \{0,1\}$ (resp. $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}})$ for $\mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}$), and outputs $\mathsf{coin}'_{\mathcal{B}}$ (resp. $\mathsf{coin}'_{\mathcal{C}}$).

CPA-style anti-piracy security guarantees that the probability that $\mathcal{B}$ and $\mathcal{C}$ simultaneously guess the challenge bits, that is, $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$ holds, is at most negligibly greater than $1/2$.

CPA$^+$ anti-piracy security is defined using exactly the same security game as CPA-style anti-piracy security. The difference is that CPA$^+$ anti-piracy security guarantees that the probability that $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ holds

[2] There exist some constructions of public-key quantum money based on assumptions other than iO [FGH+12, KSS21, LMZ23, Zha23, BNZ25]. However, these assumptions are considered non-standard, as they have not yet been extensively studied.

is at most negligibly greater than $1/2$. Namely, it considers the adversary wins the game if $\mathcal{B}$ and $\mathcal{C}$ simultaneously succeed or simultaneously fail in guessing the challenge bits.

CPA$^+$anti-piracy security is stronger than CPA-style anti-piracy security, since the former employs a more relaxed winning condition for adversaries. At first glance, this change might seem unusual, but we argue below why it is a meaningful improvement. To illustrate the difference between CPA$^+$anti-piracy security and CPA-style anti-piracy security, consider the following scenario:

- The first-stage adversary $\mathcal{A}$ aborts with probability $3/4$, in which case $\mathcal{B}$ and $\mathcal{C}$ output independent and uniform bits.
- Whenever $\mathcal{A}$ does not abort, $\mathcal{B}$ and $\mathcal{C}$ can correctly guess the coins, i.e., $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$.

We believe that such an adversary should be considered successful and prevented by the security. However, under CPA-style anti-piracy security, it is not prevented, as seen below: When $\mathcal{A}$ aborts (probability $3/4$), $\mathcal{B}$ and $\mathcal{C}$ output random bits, in which case the probability that $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$ is $1/4$. Then, the overall probability of both guesses being correct is $3/4 \cdot 1/4 + 1/4 \cdot 1 = 7/16 < 1/2$. Hence, this does not violate CPA-style anti-piracy security.

On the other hand, when $\mathcal{A}$ aborts and $\mathcal{B}$ and $\mathcal{C}$ output random bits, we have $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ with probability $1/2$. Thus the overall probability of satisfying $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ is $3/4 \cdot 1/2 + 1/4 \cdot 1 = 5/8 > 1/2$. This violates CPA$^+$anti-piracy security, indicating that the adversary is successful.

This example demonstrates that CPA$^+$anti-piracy security captures certain realistic threats that CPA-style anti-piracy security overlooks. Consequently, we argue that CPA$^+$anti-piracy security is a more appropriate security notion.

We remark that the above attack is also prevented by strong anti-piracy security in [CLLZ21]. In fact, we prove that CPA$^+$anti-piracy security is *equivalent* to strong anti-piracy security. Despite their equivalence, CPA$^+$anti-piracy security has a significantly simpler formulation, making it easier to work with compared to strong anti-piracy security. This simplicity enables us to establish its implications for existing security notions more easily.

New construction. We propose an SDE scheme based solely on polynomially secure iO and OWFs. Our construction is significantly simpler than the one presented by [CLLZ21]. The quantum decryption key consists of just a single coset state, while the public key comprises two obfuscated membership-checking programs, one for the primary space and the other for the dual space.

We prove the CPA$^+$anti-piracy security of our construction. Not only is the construction itself simpler than that of [CLLZ21], but the security proof is also more direct. In particular, we avoid the use of compute-and-compare obfuscation [GKW17, WZ17] and the accompanying extraction paradigm, which relies on projective/threshold implementations [Zha20, ALL$^+$21].

Relationship among security notions. As discussed above, CPA$^+$anti-piracy security is stronger than CPA-style anti-piracy security and, in fact, equivalent to strong anti-piracy security defined by [CLLZ21]. Moreover, we examine its relationship with the following three existing security notions:

Identical challenge-bit security [AB24]: This security notion is defined similarly to CPA-style anti-piracy security from [CLLZ21], except that the challenge bit for $\mathcal{C}$ is always set as $\mathsf{coin}_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}}$ instead of being sampled uniformly at random. Following [AB24], we denote this notion as $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security. We show that CPA$^+$anti-piracy security implies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security.

Search anti-piracy security [CLLZ21]: This is a natural search variant of anti-piracy security, where the second-stage adversaries $\mathcal{B}$ and $\mathcal{C}$ receive ciphertexts of random challenge messages, and security ensures that the probability of both adversaries simultaneously outputting the correct challenge messages is negligible. We show that CPA$^+$anti-piracy security implies search anti-piracy security when the challenge messages $m_{\mathcal{B}}$ and $m_{\mathcal{C}}$ for $\mathcal{B}$ and $\mathcal{C}$ are sampled from any unpredictable distribution. Specifically, the challenge message tuple $(m_{\mathcal{B}}, m_{\mathcal{C}}, \mathsf{aux})$ can be sampled from any distribution, as long as no quantum polynomial-time (QPT) algorithm can recover $m_{\mathcal{B}}$ or $m_{\mathcal{C}}$ given only aux. We denote this security notion as $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security.

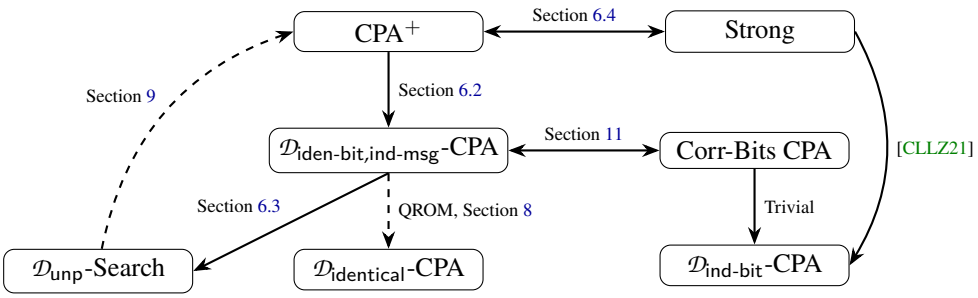

Figure 1: Relationships among security notions of SDE, where a non-dotted arrow "X$\to$Y" means that any SDE scheme that satisfies X anti-piracy security satisfies Y anti-piracy security, and a dotted arrow "X$\dashrightarrow$Y" means that if there is an SDE scheme that satisfies X anti-piracy security, there exists an SDE scheme that satisfies Y anti-piracy security. We denote CPA-style anti-piracy security by [CLLZ21] as "$\mathcal{D}_{\mathsf{ind\text{-}bit}}$-CPA" following [AB24]. We denote correlated-challenge-bits CPA anti-piracy security as "Corr-Bits CPA".

Conversely, we also show that any SDE scheme satisfying $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security can be transformed into one satisfying CPA$^+$anti-piracy security, using the quantum Goldreich-Levin technique.

Identical challenge ciphertext security [GZ20]: This security notion is defined similarly to CPA-style anti-piracy security from [CLLZ21], except that the challenge ciphertext for $\mathcal{C}$ is set as $\mathsf{ct}_{\mathcal{C}} = \mathsf{ct}_{\mathcal{B}}$ after generating $\mathsf{ct}_{\mathcal{B}}$. Following [AB24], we denote this as $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security.

Unfortunately, we have not established a direct relationship between this security notion and CPA$^+$anti-piracy security. Nevertheless, we show that any CPA$^+$-secure SDE scheme can be transformed into one satisfying $\mathcal{D}_{\mathsf{identical}}$-CPA security in the quantum random oracle model (QROM). As part of this transformation, we introduce a new technical tool, which we call the *simultaneous double-sided one-way to hiding (O2H) lemma*.

We note that establishing a direct implication or transformation from CPA$^+$anti-piracy security to $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the plain model remains highly challenging. SDE schemes satisfying the latter security notion imply the existence of unclonable encryption [BL20], whose realization in the plain model is a major open problem in quantum cryptography. If a direct transformation from CPA$^+$anti-piracy security to $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security could be achieved without relying on QROM, it immediately yields unclonable encryption in the plain model.

In fact, we prove more hierarchical relationships among security notions summarized in Figure 1.

Further robustness properties of CPA$^+$. We prove that strong anti-piracy security and consequently CPA$^+$anti-piracy security are preserved under parallel composition. In particular, this implies that the message space of SDE schemes satisfying these security notions can be freely expanded with simple parallel repetition.

We also introduce a generalized variant of CPA-style anti-piracy security, called correlated-challenge-bits CPA anti-piracy security, which allows the two challenge bits $\mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}}$ to be sampled from an arbitrary joint distribution $\mathcal{D}_{\mathsf{challbits}}$. The security requirement is that the adversary's success probability is bounded by the trivial success probability determined by $\mathcal{D}_{\mathsf{challbits}}$, namely

$$\max\{\Pr[\mathsf{coin}_{\mathcal{B}} = 0], \Pr[\mathsf{coin}_{\mathcal{B}} = 1], \Pr[\mathsf{coin}_{\mathcal{C}} = 0], \Pr[\mathsf{coin}_{\mathcal{C}} = 1]\}.$$

We show that $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security, and consequently CPA$^+$anti-piracy security, imply correlated-challenge-bits CPA anti-piracy security. Since $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security corresponds to a particular choice of the joint distribution in correlated-challenge-bits CPA anti-piracy security, the above implication also shows that the two notions are equivalent.

New feasibility results. We finally list new feasibility results obtained by combining our new construction and the relationships for security notions.

1. We achieve the first SDE scheme satisfying $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security assuming polynomially secure iO and OWFs. SDE with this security notion has not been achieved before from any assumption.

2. We achieve a $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy secure SDE scheme assuming polynomially secure iO and OWFs. The only existing construction by [AB24] relies on a conjecture called simultaneous inner product conjecture in addition to subexponentially secure iO and OWFs and the polynomial hardness of the LWE assumption.

3. We achieve a $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy secure SDE scheme assuming polynomially secure iO and OWFs in the QROM. The only existing construction by [AB24] relies on a conjecture called simultaneous inner product conjecture in addition to subexponentially secure iO and OWFs and the polynomial hardness of the LWE assumption.

1.3 Subsequent Work

Subsequent to the conference version of this work, Ananth, Behera, Huang, Kitagawa, and Yamakawa [ABH+25] showed that the perspective developed here is also useful beyond SDE, in the setting of quantum copy-protection. On the definitional side, they introduced a "+"-style strengthening of security for unclonable puncturable obfuscation (UPO) [AB24], explicitly inspired by the "+" notion introduced here for SDE. On the construction side, they developed a new construction of UPO by leveraging techniques from this work, in particular the reduction strategy to indistinguishability monogamy property of coset states underlying our SDE construction. Combining these ingredients with the UPO-to-copy-protection blueprint, they obtained new copy-protection results for several functionality classes under well-studied assumptions and with stronger security guarantees than in prior works.

1.4 Related Works

Secret-key SDE. There is a line of study exploring secret-key variants of SDE. Ananth, Kaleoglu, and Liu [AKL23] achieved information-theoretic one-time secret-key SDE for single-bit messages, defining a security notion as the secret-key one-time variant of CPA-style anti-piracy security. Concurrently, Kitagawa and Nishimaki [KN23] constructed one-time secret-key SDE for multi-bit messages based on the LWE assumption, adopting the secret-key one-time variant of strong anti-piracy security. More recently, Ananth, Kaleoglu, and Yuen [AKY25] achieved information-theoretic one-time secret-key SDE for single-bit messages with quantum ciphertexts, considering the secret-key one-time variant of identical challenge ciphertext security.

Collusion-resistant SDE. Collusion resistance in SDE provides an unclonable security guarantee ensuring that an adversary with access to t copies of the quantum decryption key cannot generate $t+1$ copies capable of decrypting freshly generated ciphertexts. Liu, Liu, Qian, and Zhandry [LLQZ22] constructed bounded collusion-resistant SDE, where the collusion bound t is fixed at setup. Their scheme relies on subexponentially secure iO and OWFs, along with the polynomial hardness of the LWE assumption. More recently, Çakan and Goyal [ÇG24] achieved unbounded collusion-resistant SDE. Their construction is based on subexponentially secure iO and OWFs, as well as the subexponential hardness of the LWE assumption. Both of these works employed a collusion-resistant variant of strong anti-piracy security.

2 Technical Overview

We provide the technical overview of our work.

2.1 SDE based on iO and OWFs

Coset states and new monogamy property. For a subspace $A \subseteq \mathbb{F}_2^n$, we use the following notions introduced by [CLLZ21, AKL+22].

- $A^\perp$ is the dual space of A.
- Can_A is a function such that for any $s \in \mathbb{F}_2^n$, $\mathsf{Can}_A(s)$ is the lexicographically smallest vector contained in the coset $A+s$, which we call the canonical representative of $A+s$. For any $s' \in A+s$, we have $\mathsf{Can}_A(s') = \mathsf{Can}_A(s)$. Can_A is polynonial-time computable given the description of A.
- $\mathsf{CS}(A)$ is the set of canonical representatives with respect to A, that is, $\mathsf{CS}(A) = \{\mathsf{Can}_A(s) : s \in \mathbb{F}_2^n\}$.

For a subspace $A \subseteq \mathbb{F}_2^n$ and two canonical representatives $(s,t) \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$, we define the coset state $|A_{s,t}\rangle$ as

$$|A_{s,t}\rangle := \sum_{a\in A} (-1)^{\langle a,t\rangle} |a+s\rangle .$$

By applying $H^{\otimes n}$ to $|A_{s,t}\rangle$, we obtain $\left|A^\perp_{t,s}\right\rangle$, where H is the Hadamard gate (thus $H^{\otimes n}$ is the Quantum Fourier Transformation over $\mathbb{F}_2^n$.)

When the context is clear, we below use $A+s$ and $A^\perp+t$ to refer to the program that verifies membership in $A+s$ and $A^\perp+t$, respectively. In particular, we will often write $i\mathcal{O}(A+s)$ and $i\mathcal{O}(A^\perp+t)$ to denote an obfuscation by $i\mathcal{O}$ of the program that verifies membership in $A+s$ and $A^\perp+t$, respectively.

In this work, we use the following variant of monogamy property of coset states that we call *computational strong indistinguishability monogamy property*, which immediately follows from the computational strong monogamy property shown by [CLLZ21, CV22] and the simultaneous quantum Goldreich-Levin lemma shown by [AKY25]. Consider the following experiment played by a tuple of adversaries $(\mathcal{A},\mathcal{B},\mathcal{C})$.

1. $\mathcal{A}$ is given a randomly generated coset state $|A_{s,t}\rangle$ and two obfuscated membership checking programs $i\mathcal{O}(A+s)$ and $i\mathcal{O}(A^\perp+t)$. $\mathcal{A}$ outputs a bipartite state q over the registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$.
2. $\mathcal{B}$ (resp. $\mathcal{C}$) is given the register $\mathsf{R}_\mathcal{B}$ (resp, $\mathsf{R}_\mathcal{C}$), the description of A, and a random string $r_\mathcal{B}$ (resp. $r_\mathcal{C}$), and outputs $b_\mathcal{B}$ (resp. $b_\mathcal{C}$).

The property guarantees that assuming that $i\mathcal{O}$ is secure iO and there exist OWFs, for any tuple of QPT adversaries, the probability that $b_\mathcal{B} \oplus b_\mathcal{C} = \langle r_\mathcal{B}, s\rangle \oplus \langle r_\mathcal{C}, t\rangle$ holds is at most negligibly greater than $1/2$.

Our SDE Construction. We now sketch our construction.

Key generation: It generates a random coset state $|A_{s,t}\rangle$ for $(s,t) \leftarrow \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$ together with the two obfuscated membership checking programs $\mathsf{C}_{\mathsf{mc}} = i\mathcal{O}(A+s)$ and $\mathsf{C}^\perp_{\mathsf{mc}} = i\mathcal{O}(A^\perp+t)$, and set the public key as $\mathsf{pk} = (\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^\perp_{\mathsf{mc}})$ and the quantum decryption key as $s\mathsf{k} = |A_{s,t}\rangle$.[3]

Encryption: On input the public key $\mathsf{pk} = (\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^\perp_{\mathsf{mc}})$ and a message $m \in \{0,1\}^{\ell_{\mathsf{msg}}}$, it first generates random ℓ_{msg}-bit string k. It then obfuscates the two circuits $P[\mathsf{C}_{\mathsf{mc}}, k\oplus m]$ and $P[\mathsf{C}^\perp_{\mathsf{mc}}, k]$, and obtains the obfuscated circuits $\widetilde{P}$ and $\widetilde{P}^\perp$, where the circuit P is described in Figure 2. In short, $P[\mathsf{C},\mathsf{str}]$ is a circuit that outputs str only when the input x is accepted by the hardwired circuit C that is supposed to be a (obfuscated) membership checking program. It finally outputs $\mathsf{ct} = (\widetilde{P}, \widetilde{P}^\perp)$.

Decryption The above ciphertext can be decrypted to m correctly by using the fact that we can compute $k\oplus m$ with probability 1 from $s\mathsf{k} = |A_{s,t}\rangle$ and $\widetilde{P}$, and k with probability 1 from $H^{\otimes n} s\mathsf{k} = \left|A^\perp_{t,s}\right\rangle$ and $\widetilde{P}^\perp$.

[3] In the actual syntax, the key generation algorithm is separated into classical one and quantum one, where the former outputs the classical public key and secret key given the security parameter, and the latter outputs the quantum decryption key given the classical secret key.

$P[C, \mathsf{str}](x)$

Hardwired constant: A description of a circuit C with 1-bit output and a ℓ_{msg}-bit string str.

Input: $x \in \{0,1\}^n$.

1. If $C(x) = 1$, output str. Otherwise, output $0^{\ell_{\mathsf{msg}}}$.

Figure 2: The description of the circuit P.

$Q[C, A, f, k](x)$

Hardwired constant: A description of a circuit C with 1-bit output, a description of a $n/2$-dimensional subspace A of $\mathbb{F}_2^n$, a function f, and a string k.

Input: $x \in \{0,1\}^n$.

1. If $C(x) = 1$, compute $s = \mathsf{Can}_A(x)$ and output $k \oplus f(s)$. Otherwise, output $0^{\ell_{\mathsf{msg}}}$.

Figure 3: The description of the circuit Q.

Proof sketch for CPA$^+$Security. We next talk about the CPA$^+$security of our construction. In the proof, we leverage the fact that an encryption of a message $f(s)$ and $f(t)$ for any efficiently computable function f, can be simulated only from pk, A, and f, against the adversary holding the quantum secret key $s\mathsf{k} = |A_{s,t}\rangle$. Concretely, consider the following simulated encryption process.

Simulated encryption for $f(s)$: On input the public key $\mathsf{pk} = (\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^{\perp}_{\mathsf{mc}})$, the description of A, and a function f, it first generates random ℓ_{msg}-bit string k. It then obfuscates the two circuits $Q[\mathsf{C}_{\mathsf{mc}}, A, f, k]$ and $P[\mathsf{C}^{\perp}_{\mathsf{mc}}, k]$, and obtain the obfuscated circuits $\widetilde{\mathsf{Q}}$ and $\widetilde{P}^{\perp}$, where the circuit Q is described in Figure 3. It finally outputs $\mathsf{ct} = (\widetilde{\mathsf{Q}}, \widetilde{P}^{\perp})$.

We can confirm that $Q[\mathsf{C}_{\mathsf{mc}}, A, f, k]$ is functionally equivalent to $P[\mathsf{C}_{\mathsf{mc}}, k \oplus f(s)]$, since on input x, both of them outputs $k \oplus f(s)$ if $x \in A + s$ and otherwise outputs $0^{\ell_{\mathsf{msg}}}$. Therefore, from the security of $i\mathcal{O}$, their obfuscations are computationally indistinguishable. As a result, the simulated ciphertext $\mathsf{ct} = (\widetilde{\mathsf{Q}}, \widetilde{P}^{\perp})$ is computationally indistinguishable from the real encryption of the message $f(s)$. Similarly, we can generate a simulated ciphertext for the message $f(t)$ that is computationally indistinguishable from the real one, using $\mathsf{C}^{\perp}_{\mathsf{mc}}$, A, and f, but not t. We emphasize that the computational indistinguishability holds even against a distinguisher holding the quantum secret key $s\mathsf{k} = |A_{s,t}\rangle$.

Given the above ciphertext simulatability, the security proof is done with the following two steps. Let $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ be a tuple of QPT adversaries, and we assume its advantage defined as $\Pr[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}]$ is $1/2 + \epsilon$, where $\mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}}$ are the challenge bits for $\mathcal{B}$ and $\mathcal{C}$, respectively, and $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$ are the outputs of $\mathcal{B}$ and $\mathcal{C}$, respectively.

In the first step, we replace the challenge bit $\mathsf{coin}_{\mathcal{B}}$ for $\mathcal{B}$ with $\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle$, and the challenge bit $\mathsf{coin}_{\mathcal{C}}$ for $\mathcal{C}$ with $\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle$, where $r_{\mathcal{B}}$ and $r_{\mathcal{C}}$ are uniform random n-bit strings. This does not change the distribution of the challenge bits, thus it also does not change $\mathcal{A}_{\mathsf{sde}}$'s advantage. More specifically, the following three changes are applied in this step.

- $\mathcal{B}$ is given an encryption of $m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle}$ as the challenge ciphertext, where $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$ are the challenge messages for $\mathcal{B}$.
- $\mathcal{C}$ is given an encryption of $m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle}$ as the challenge ciphertext, where $(m_{\mathcal{C},0}, m_{\mathcal{C},1})$ are the challenge messages for $\mathcal{C}$.
- $\mathcal{A}_{\mathsf{sde}}$'s advantage is defined as $\Pr[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle]$. Letting $b_{\mathcal{B}} = \mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}}$ and $b_{\mathcal{C}} = \mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}}$, we can rewrite it as $\Pr[b_{\mathcal{B}} \oplus b_{\mathcal{C}} = \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle]$.

We note that, letting $f[\mathsf{coin}, r, m_0, m_1]$ be a function that outputs $m_{\mathsf{coin} \oplus \langle r, x\rangle}$ for the input x, $\mathcal{B}$ is given an encryption of $f[\mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}](s)$ and $\mathcal{C}$ is given an encryption of $f[\mathsf{coin}_{\mathcal{C}}, r_{\mathcal{C}}, m_{\mathcal{C},0}, m_{\mathcal{C},1}](t)$, as the challenge ciphertexts.

As the second step, we construct the reduction algorithm $\mathcal{A}_{\mathsf{moe}} = (\widehat{\mathcal{A}}, \widehat{\mathcal{B}}, \widehat{\mathcal{C}})$ attacking the computational strong indistinguishability monogamy property using $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ as follows.

1. Given a coset state $|A_{s,t}\rangle$ and two obfuscated membership checking programs $C_{\mathsf{mc}} = i\mathcal{O}(A + s)$ and $C^{\perp}_{\mathsf{mc}} = i\mathcal{O}(A^{\perp} + t)$, $\widehat{\mathcal{A}}$ invokes $\mathcal{A}$ with $\mathsf{pk} = (C_{\mathsf{mc}}, C^{\perp}_{\mathsf{mc}})$ and $\mathsf{sk} = |A_{s,t}\rangle$, and obtains the challenge message tuple $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. $\widehat{\mathcal{A}}$ sends the registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$ to $\widehat{\mathcal{B}}$ and $\widehat{\mathcal{C}}$, respectively, together with pk and the challenge messages.
2. Given $\mathsf{R}_{\mathcal{B}}$, pk, the challenge messages, and $(A, r_{\mathcal{B}})$, $\widehat{\mathcal{B}}$ generates random bit $\mathsf{coin}_{\mathcal{B}}$, and generates simulated encryption $\mathsf{ct}_{\mathcal{B}}$ of the message $m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle}$, using pk, A, and the function $f[\mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}]$. $\widehat{\mathcal{B}}$ then runs $\mathcal{B}$ with $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{B}}$. When $\mathcal{B}$ outputs $\mathsf{coin}'_{\mathcal{B}}$, $\widehat{\mathcal{B}}$ outputs $b_{\mathcal{B}} = \mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}}$. Similarly, $\widehat{\mathcal{C}}$ generates a random bit $\mathsf{coin}_{\mathcal{C}}$ and a simulated encryption $\mathsf{ct}_{\mathcal{C}}$ for the message $m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle}$, runs $\mathcal{C}$ with $\mathsf{R}_{\mathcal{C}}$ and $\mathsf{ct}_{\mathcal{C}}$, and outputs $b_{\mathcal{C}} = \mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}}$ for the output $\mathsf{coin}'_{\mathcal{C}}$ of $\mathcal{C}$.

From the computational indistinguishability of the simulated ciphertexts, $\mathcal{A}_{\mathsf{moe}}$ simulates the CPA^{+}anti-piracy security experiments for $\mathcal{A}_{\mathsf{sde}}$ with the modifications applied in the first step, in a computationally indistinguishable way. It is crucial that the ciphertext simulatability holds against the adversary with the quantum decryption key $\mathsf{sk} = |A_{s,t}\rangle$, since it is required to simulate the view of $\mathcal{A}_{\mathsf{sde}}$. In the simulated experiment, $b_{\mathcal{B}} \oplus b_{\mathcal{C}} = \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle$ holds with probability negligibly close to $1/2 + \epsilon$. From the computational strong indistinguishability monogamy property of the coset states, we can conclude that ϵ is negligible thus SDE satisfies CPA^{+}anti-piracy security.

2.2 Implications from CPA^{+}to Other Security Notions

$\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security (Identical challenge-bit security). Somewhat surprisingly, this implication can be established through simple probability calculations, inspired by [AKY25], without requiring any reductions. Specifically, we prove the following: Let $\mathcal{A}_{\mathsf{sde}}$ be any adversary that achieves the winning probability $1/2 + \epsilon$ in the CPA^{+}anti-piracy security experiment. Then, when $\mathcal{A}_{\mathsf{sde}}$ is executed in the $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security experiment, its winning probability is at most $1/2 + \epsilon$. This demonstrates that CPA^{+}anti-piracy security implies identical challenge-bit security.

$\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security. Recall the implication from IND-CPA security to one-wayness for classical PKE. The reduction $\mathcal{A}$ attacking IND-CPA, is given the challenge ciphertext ct that is an encryption of either a random message m picked by itself or 0, feeds it to the one-way attacker $\mathcal{A}'$, and if the result is m, outputs 1; otherwise, it outputs 0. Suppose $\mathcal{A}'$ has inverse polynomial success probability ϵ. Conditioned on the challenge bit for $\mathcal{A}$ being 1 (thus ct is an encryption of m), $\mathcal{A}$ simulates the one-way security experiment for $\mathcal{A}'$ perfectly and outputs 1 with probability ϵ. On the other hand, conditioned on the challenge bit being 0 (thus ct is an encryption of 0), $\mathcal{A}'$ cannot output m except with negligible probability, so $\mathcal{A}$ outputs 0 with probability almost 1. Therefore, $\mathcal{A}$ can guess the challenge bit with probability negligibly close to $1/2 + \epsilon/2$, proving that the reduction works. The argument goes through as long as the challenge message in the one-way security experiment is sampled from computationally unpredictable distribution.

It is rather clear that the same strategy works to show that $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security implies $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security. Combining this with the first implication, we can conclude that CPA^{+}security implies $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security.

$\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security considers the setting where the two second-stage adversaries receive challenge ciphertexts generated using independent encryption randomness. However, leveraging the result of [AKL23], we can show that search anti-piracy security in this setting also implies security in a setting where the challenge ciphertexts are generated with correlated encryption randomness. In particular, $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security implies a variant in which both second-stage adversaries receive the exact same challenge ciphertext of a message m, where m is sampled from an unpredictable distribution. We use this extension below.

$\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security (Identical ciphertext security). SDE with this security notion is closely related to unclonable encryption with indistinguishability security. In particular, they are equivalent in the secret-key setting [GZ20]. Ananth et al. [AKL23] generalized the techniques from [AKL^{+}22] and showed that unclonable encryption

with indistinguishability security can be constructed in the QROM from one with augmented search security where the adversaries have access to the point function oracle $\mathcal{O}_m$ for the challenge message m. Building on their approach, we transform a CPA$^+$anti-piracy secure SDE scheme into one with $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security as follows:

1. By extending the implication to $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security, we establish that CPA$^+$(and $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA) anti-piracy security implies what we call augmented identical-challenge search anti-piracy security. This variant of search anti-piracy security ensures search security guarantee in the setting where the adversaries are given access to the point function oracle $\mathcal{O}_m$, and the second-stage adversaries receive the exact same challenge ciphertext of m, where m is a uniformly random message.

2. We then show how to transform any SDE scheme satisfying augmented identical-challenge search anti-piracy security into one satisfying $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the QROM. In this step, we generalize previous techniques [AKL$^+$22, AKL23] and introduce a new technical tool, which we call the *simultaneous double-sided one-way-to-hiding lemma*. We believe this lemma is of independent interest.

Strong anti-piracy security. This security notion can be informally defined as follows. Consider an experiment parameterized by γ where the adversary $\mathcal{A}$ is given the public key pk and the quantum decryption key $s\mathcal{K}$. The adversary outputs a challenge message tuple $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and possibly entangled quantum decryption programs $\mathcal{D}_{\mathcal{B}}$ and $\mathcal{D}_{\mathcal{C}}$. $\mathcal{A}$ wins this experiment if both $\mathcal{D}_{\mathcal{B}}$ and $\mathcal{D}_{\mathcal{C}}$ have a success probability greater than $1/2+\gamma$ in distinguishing the encryptions of $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$ and $(m_{\mathcal{C},0}, m_{\mathcal{C},1})$, respectively. Strong anti-piracy security guarantees that for any inverse polynomial γ and any QPT adversary $\mathcal{A}$, the probability of $\mathcal{A}$ winning in this experiment is negligible. Defining this concept rigorously involves subtle challenges because quantum programs are entangled and inherently stateful, making it nontrivial to define their success probabilities in a cryptographically meaningful way. Here, we focus on the intuition and proceed with an informal definition.

Reducing strong anti-piracy security to CPA$^+$anti-piracy security is relatively simple and can be outlined as follows. Assuming the former does not hold, the first-stage adversary $\mathcal{A}$ for CPA$^+$anti-piracy security can generate two quantum programs, each with success probability $1/2+\gamma$, with probability ϵ, for some inverse polynomials γ and ϵ. If $\mathcal{A}$ succeeds in generating quantum decryption programs, it provides them to the second-stage adversaries $\mathcal{B}$ and $\mathcal{C}$, who then apply them to the challenge ciphertexts and output the results. Conversely, if $\mathcal{A}$ fails, it instructs $\mathcal{B}$ and $\mathcal{C}$ to output 0. The winning probability (i.e., the probability that $\mathcal{B}$ and $\mathcal{C}$ either both succeed or both fail) can be estimated as

$$\epsilon\cdot\left((\frac{1}{2}+\gamma)(\frac{1}{2}+\gamma)+(\frac{1}{2}-\gamma)(\frac{1}{2}-\gamma)\right)+(1-\epsilon)\cdot\frac{1}{2}=\frac{1}{2}+\epsilon\cdot\gamma^2.$$

This breaks CPA$^+$anti-piracy and the reduction is done.

The above proof establishes that CPA$^+$anti-piracy security is at least as strong as strong anti-piracy security. In this paper, we further demonstrate that they are, in fact, equivalent. The proof for the reverse direction reveals that the ability to " simultaneously succeed or simultaneously fail " can be exploited to construct two quantum decryption programs with a high success probability.

3 Preliminaries

Notations and conventions. In this paper, standard math or sans serif font stands for classical algorithms (e.g., C or Gen) and classical variables (e.g., x or pk). Calligraphic font stands for quantum algorithms (e.g., $\mathcal{G}en$) and calligraphic font and/or the bracket notation for (mixed) quantum states (e.g., q or $|\psi\rangle$).

Let $[\ell]$ denote the set of integers $\{1,\cdots,\ell\}$, λ denote a security parameter, and $y:=z$ denote that y is set, defined, or substituted by z. For a finite set X and a distribution D, $x\leftarrow X$ denotes selecting an element from X uniformly at random, $x\leftarrow D$ denotes sampling an element x according to D. Let $y\leftarrow\mathsf{A}(x)$ and $y\leftarrow\mathcal{A}(\chi)$ denote assigning to y the output of a probabilistic or deterministic algorithm A and a quantum algorithm $\mathcal{A}$ on an input x and χ, respectively. When we explicitly show that A uses randomness r, we write $y\leftarrow\mathsf{A}(x;r)$. PPT and QPT algorithms stand for probabilistic polynomial-time algorithms and polynomial-time quantum algorithms, respectively. Let negl denote a negligible function, $\mathsf{non\text{-}negl}$ denote a non-negligible function, and poly denote a positive polynomial. For

a string $x \in \{0,1\}^n$, $x[i]$ is its i-th bit. For strings $x, y \in \{0,1\}^n$, $\langle x, y\rangle$ denotes $\bigoplus_{i\in[n]} x[i]\cdot y[i]$. We often use the similar notation for vectors $x, y \in \mathbb{F}_2^n$ by identifying elements of $\mathbb{F}_2$ and $\{0,1\}$ in the natural manner.

We use gray sans serif font (e.g., X) to stand for a quantum register. For a quantum state q over registers R_1 and R_2, we write $q[\mathsf{R}_1]$ to denote the portion of the state on register R_1. Similarly, for a pure quantum state $|\psi\rangle$ over registers R_1 and R_2, we write $|\psi\rangle_{\mathsf{R}_1}$ to denote the portion of the state on register R_1. For quantum states q and q', $\|q - q'\|_{tr}$ denotes their trace distance.

3.1 Classical Cryptographic Primitives

Definition 3.1 (Indistinguishability Obfuscator [BGI+12]). *A PPT algorithm $i\mathcal{O}$ is a secure IO for a classical circuit class $\{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$ if it satisfies the following two conditions.*

Functionality: *For any security parameter $\lambda \in \mathbb{N}$, circuit $C \in \mathcal{C}_\lambda$, and input x, we have that*

$$\Pr\left[C'(x) = C(x) \mid C' \leftarrow i\mathcal{O}(C)\right] = 1 \ .$$

Indistinguishability: *For any PPT* $\mathsf{Sampler}$ *and QPT distinguisher $\mathcal{D}$, the following holds:*

If $\Pr\left[\forall x\ C_0(x) = C_1(x) \wedge |C_0| = |C_1| \mid (C_0, C_1, \mathsf{aux}) \leftarrow \mathsf{Sampler}(1^\lambda)\right] > 1 - \mathsf{negl}(\lambda)$, *then we have*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{io}}_{i\mathcal{O},\mathcal{D}}(\lambda) := \Big|&\Pr\left[\mathcal{D}(i\mathcal{O}(C_0), \mathsf{aux}) = 1 \mid (C_0, C_1, \mathsf{aux}) \leftarrow \mathsf{Sampler}(1^\lambda)\right]\\ &- \Pr\left[\mathcal{D}(i\mathcal{O}(C_1), \mathsf{aux}) = 1 \mid (C_0, C_1, \mathsf{aux}) \leftarrow \mathsf{Sampler}(1^\lambda)\right]\Big| \leq \mathsf{negl}(\lambda).\end{aligned}$$

There are a few candidates of secure IO for polynomial-size classical circuits against quantum adversaries [BGMZ18, CHVW19, AP20, DQV+21].

3.2 Gentle Measurement Lemma

Lemma 3.2 (Gentle Measurement Lemma [Win99]). *Let q be any quantum state and $\mathcal{E} = (\boldsymbol{P}, \boldsymbol{I} - \boldsymbol{P})$ be a projective measurement on its register such that*

$$\|\operatorname{Tr}(\Pi q)\| \geq 1 - \epsilon$$

for $0 \leq \epsilon \leq 1$. Let q' be the state obtained by applying $\mathcal{E}$ to q and post-selecting to the first outcome, i.e.,

$$q' := \frac{\Pi q \Pi}{\|\operatorname{Tr}(\Pi q)\|}.$$

Then we have

$$\|q - q'\|_{tr} \leq 2\epsilon^{1/2}.$$

3.3 Useful Lemmata

Ananth et al. [AKY25] extended the quantum Goldreich-Levin lemma [AC02, CLLZ21] to the non-local setting, where two non-communicating algorithms with potentially entangled quantum inputs are involved.[4].

Lemma 3.3 (Simultaneous Quantum Goldreich-Levin [AKY25]). *There exists a QPT oracle algorithm $\mathcal{E}xt$ that satisfies the following. Let $n \in \mathbb{N}$, $x_{\mathcal{B}}, x_{\mathcal{C}} \in \{0,1\}^n$, $\epsilon \in [0, 1/2]$, and q be a quantum state over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Let $\mathcal{B}$ (resp. $\mathcal{C}$) be a quantum algorithm that takes $\mathsf{R}_{\mathcal{B}}$ (resp. $\mathsf{R}_{\mathcal{C}}$) and an n-bit string $r_{\mathcal{B}}$ (resp. $r_{\mathcal{C}}$) as input, and outputs a bit. If we have*

$$\Pr\left[b_{\mathcal{B}} \oplus b_{\mathcal{C}} = \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle : \begin{array}{l} r_{\mathcal{B}}, r_{\mathcal{C}} \leftarrow \{0,1\}^n \\ b_{\mathcal{B}} \leftarrow \mathcal{B}(q[\mathsf{R}_{\mathcal{B}}], r_{\mathcal{B}}) \\ b_{\mathcal{C}} \leftarrow \mathcal{C}(q[\mathsf{R}_{\mathcal{C}}], r_{\mathcal{C}}) \end{array}\right] \geq \frac{1}{2} + \epsilon,$$

[4] A slightly weaker version is also proven in [AKL23]

then, we have

$$\Pr\left[\mathcal{E}\mathit{xt}(\mathcal{B}, q[\mathsf{R}_{\mathcal{B}}]) \to x_{\mathcal{B}} \wedge \mathcal{E}\mathit{xt}(\mathcal{C}, q[\mathsf{R}_{\mathcal{C}}]) \to x_{\mathcal{C}}\right] \geq 4\epsilon^2.$$

where $\mathcal{B}$ and $\mathcal{C}$ in the input of $\mathcal{E}\mathit{xt}$ mean their descriptions.

Lemma 3.3 was originally proven in [AKY25, Lemma 5] for the special case of $x_{\mathcal{B}} = x_{\mathcal{C}}$. However, we observe that their proof does not rely on this assumption, and the same argument holds for the more general case where $x_{\mathcal{B}} \neq x_{\mathcal{C}}$.

The following technical lemma was shown in [AKL+22]. We rely on it in Section 7.

Lemma 3.4 ([AKL+22, Corollary 2.4]). *Let $\boldsymbol{P}_0$ and $\boldsymbol{P}_1$ be projections and $|\psi_0\rangle$ and $|\psi_1\rangle$ be eigenvectors of $(\boldsymbol{P}_0 + \boldsymbol{P}_1)/2$ with eigenvalues λ_0, λ_1, respectively. If $\lambda_0 \neq \lambda_1$ and $\lambda_0 + \lambda_1 \neq 1$, then*

$$\langle\psi_0|\,\boldsymbol{P}_0\,|\psi_1\rangle = \langle\psi_0|\,\boldsymbol{P}_1\,|\psi_1\rangle = 0.$$

3.4 Projective and Threshold Implementations

We review the notions of projective and threshold implementations and related notions introduced in [Zha20, ALL+21]. They are only used from Section 6 onwards, so readers interested in the direct construction of an SDE scheme in Section 5 may feel free to skip this subsection.

Definition 3.5 (Projective Implementation [Zha20]). *Let $\mathcal{P}$ be a binary-outcome POVM and $\mathcal{E}$ be a projective measurement indexed by a finite set consisting of elements of $[0,1]$. We consider the following measurement procedure.*

1. *Apply $\mathcal{E}$ to obtain an outcome $p \in [0,1]$*
2. *Output 1 with probability p and 0 otherwise.*

We say $\mathcal{E}$ is the projective implementation of $\mathcal{P}$, denoted by $\mathsf{ProjImp}(\mathcal{P})$, if the measurement process above is equivalent to $\mathcal{P}$.

Remark 3.6. [Zha20] defines projective implementations for general POVMs, but we focus on *binary-outcome* POVMs for simplicity.

Theorem 3.7 ([Zha20, Lemma 1]). *Any binary outcome POVM $\mathcal{P}$ has a unique projective implementation $\mathsf{ProjImp}(\mathcal{P})$.*

Definition 3.8 (Threshold Implementation [Zha20, ALL+21]). *Let $\mathcal{P}$ be a binary-outcome POVM, $\mathcal{E}$ be a projective implementation $\mathsf{ProjImp}(\mathcal{P})$ of $\mathcal{P}$, and $\gamma > 0$. A threshold implementation of $\mathcal{P}$, denoted by $\mathcal{TI}_\gamma(\mathcal{P})$, is the following measurement procedure.*

- *Apply $\mathcal{E}$ to a quantum state and obtain p as an outcome.*
- *Output 1 if $p \geq \gamma$, and 0 otherwise.*

Following [CLLZ21], for a quantum state q, we abuse notation to denote by $\mathrm{Tr}[\mathcal{TI}_\gamma(\mathcal{P})q]$ to mean the probability that the threshold implementation applied to q outputs 1. This means that whenever $\mathcal{TI}_\gamma(\mathcal{P})$ appears inside a trace Tr, we treat $\mathcal{TI}_\gamma(\mathcal{P})$ as a projection onto the 1 outcome.

As a special case of binary-outcome POVMs, we introduce the notion of mixture of projective measurements following [Zha20].

Definition 3.9 (Mixture of Projetive Measurement [Zha20]). *Let $\mathcal{R}$ and $\mathcal{I}$ be finite sets and $D : \mathcal{R} \to \mathcal{I}$ be a function. Let $\{(\boldsymbol{P}_i, \boldsymbol{Q}_i)\}_{\in\mathcal{I}}$ be a collection of binary projective measurement. The mixture of projective measurements associated to D and $\{(\boldsymbol{P}_i, \boldsymbol{Q}_i)\}_{\in\mathcal{I}}$ is the binary POVM $\mathcal{P}_D = (\boldsymbol{P}_D, \boldsymbol{Q}_D)$ defined as follows*

$$\boldsymbol{P}_D = \sum_{i\in\mathcal{I}} \Pr[i \leftarrow D(R)]\boldsymbol{P}_i \qquad\qquad \boldsymbol{Q}_D = \sum_{i\in\mathcal{I}} \Pr[i \leftarrow D(R)]\boldsymbol{Q}_i,$$

where R is uniformly distributed in $\mathcal{R}$.

While projective and threshold implementations are not known to be efficiently doable, they are known to be efficiently approximated.

Definition 3.10 (Shift Distance [Zha20]). *For two distributions D_0, D_1, with cumulative density functions f_0, f_1, respectively, the shift distance with parameter ϵ is defined as*

$$\Delta^{\epsilon}_{\mathsf{Shift}}(D_0, D_1) := \sup_{x\in\mathbb{R}} \min_{y\in[f_1(x-\epsilon), f_1(x+\epsilon)]} |f_0(x) - y|.$$

For two real-valued measurements $\mathcal{M}$ and $\mathcal{N}$ over the same quantum system, the shift distance between $\mathcal{M}$ and $\mathcal{N}$ with parameter ϵ is

$$\Delta^{\epsilon}_{\mathsf{Shift}}(\mathcal{M}, \mathcal{N}) := \sup_{|\psi\rangle} \Delta^{\epsilon}_{\mathsf{Shift}}(\mathcal{M}(|\psi\rangle), \mathcal{N}(|\psi\rangle)).$$

Definition 3.11 (Almost Projective Measurements [Zha20]). *A real-valued measurement $\mathcal{M} = (M_i)_{i\in I}$ is (ϵ, η)-almost projective if the following is true: for any quantum state $|\psi\rangle$, apply $\mathcal{M}$ twice in a row to $|\psi\rangle$, obtaining outcomes x, y. Then $\Pr[|x - y| \le \epsilon] \ge 1 - \eta$.*

Lemma 3.12 (Approximate Projective Implementation [Zha20]). *For any $\epsilon, \delta \in (0,1)$, any finite sets $\mathcal{R}$ and $\mathcal{I}$, any collection of projective measurements $\mathcal{P} = \{(\boldsymbol{P}_i, \boldsymbol{I} - \boldsymbol{P}_i)\}_{i\in\mathcal{I}}$ and any function $D : \mathcal{R} \to \mathcal{I}$, there exists a measurement procedure $\mathcal{API}^{\epsilon,\delta}_{\mathcal{P},D}$ that satisfies the following.*

1. $\Delta^{\epsilon}_{\mathsf{Shift}}(\mathcal{API}^{\epsilon,\delta}_{\mathcal{P},D}, \mathsf{ProjImp}(\mathcal{P}_{\mathcal{D}})) \le \delta$.
2. *$\mathcal{API}^{\epsilon,\delta}_{\mathcal{P},D}$ is (ϵ, δ)-almost projective.*
3. *The running time of $\mathcal{API}^{\epsilon,\delta}_{\mathcal{P},D}$ is $T_{\mathcal{P},D} \cdot \mathrm{poly}(\epsilon^{-1}, \log(\delta^{-1}))$, where $T_{\mathcal{P},D}$ is the combined running time of computing D, of mapping i to $(\boldsymbol{P}_i, \boldsymbol{I} - \boldsymbol{P}_i)$, and of implementing the projective measurement $(\boldsymbol{P}_i, \boldsymbol{I} - \boldsymbol{P}_i)$.*

Remark 3.13. The original proof in [Zha20] only upper bounds the *expected* running time of $\mathcal{API}$. However, [Zha20, Remark 6.4] also sketches an idea to upper bound the *worst-case* running time by slightly modifying the algorithm, which is made formal in [CLPY25].

Definition 3.14 (Approximate Threshold Implementation [ALL+21]). *For any $\epsilon, \delta, \mathcal{R}, \mathcal{I}, \mathcal{P}, D$ as in Lemma 3.12 and any $\gamma \in (0,1)$, $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ is the measurement procedure that works similarly to $\mathcal{TI}_{\gamma}(\mathcal{P}_D)$ except that it uses $\mathcal{API}^{\epsilon,\delta}_{\mathcal{P},D}$ instead of $\mathsf{ProjImp}(\mathcal{P}_D)$. For simplicity, we denote the probability of the measurement outputting 1 on q by $\mathrm{Tr}\left[\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma} q\right]$.*

Lemma 3.15 ([ALL+21]). *For any $\epsilon, \delta, \gamma, \mathcal{R}, \mathcal{I}, \mathcal{P}, D$ be as in Definition 3.14, $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ satisfies the following.*

- *For all quantum state q,*
  - $\mathrm{Tr}\left[\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma-\epsilon} q\right] \ge \mathrm{Tr}[\mathcal{TI}_{\gamma}(\mathcal{P}_D) q] - \delta$ *and*
  - $\mathrm{Tr}[\mathcal{TI}_{\gamma-\epsilon}(\mathcal{P}_D) q] \ge \mathrm{Tr}\left[\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma} q\right] - \delta$.
- *For all quantum state q, let q' be the post-measurement state after applying $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P},D,\gamma}$ on q, and obtaining outcome 1. Then, it holds $\mathrm{Tr}\left[\mathcal{TI}_{\gamma-2\epsilon}(\mathcal{P}_D) q'\right] \ge 1 - 2\delta$.*

Lemma 3.16 ([ALL+21]). *Let $\mathcal{R}$ and $\mathcal{I}$ be finite sets. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two collections of projective measurements, indexed by elements of $\mathcal{I}$. Let $D_1 : \mathcal{R} \to \mathcal{I}$ and $D_2 : \mathcal{R} \to \mathcal{I}$ be functions. For any $\epsilon, \delta, \gamma \in (0,1)$, $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_j,D_j,\gamma}$ for $j \in \{1,2\}$ satisfy the following.*

- *For any bipartite (possibly entangled, mixed) quantum state* $q \in \mathcal{H}_1 \otimes \mathcal{H}_2$*,*

$$\mathrm{Tr}\left[(\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_1,D_1,\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_2,D_2,\gamma-\epsilon})q\right] \geq \mathrm{Tr}\left[(\mathcal{TI}_\gamma(\mathcal{P}_{1,D_1}) \otimes \mathcal{TI}_\gamma(\mathcal{P}_{2,D_2}))q\right] - 2\delta,$$

where $\mathcal{P}_{j,D_j}$ *is the mixture of projective measurement corresponding to* $\mathcal{P}_j$*,* D_j *for* $j \in \{1,2\}$*.*

- *For any (possibly entangled, mixed) quantum state* $q \in \mathcal{H}_1 \otimes \mathcal{H}_2$*, let* q' *be the (normalized) post-measurement state after applying the measurement* $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_1,D_1,\gamma}$ *and* $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_2,D_2,\gamma}$ *to* q *and obtaining outcome* 1 *for both. Then, it holds that*

$$\mathrm{Tr}\left[(\mathcal{TI}_{\gamma-2\epsilon}(\mathcal{P}_{1,D_1}) \otimes \mathcal{TI}_{\gamma-2\epsilon}(\mathcal{P}_{2,D_2}))q'\right] \geq 1 - 4\delta.$$

4 New Security Definition of Single-Decryptor Encryption

We review the notion of single-decryptor encryption (SDE) [GZ20, CLLZ21] and introduce a novel security definition for SDE, which we term *CPA$^+$anti-piracy security*. As we show in Section 6, this new definition subsumes most existing security notions.

4.1 Syntax

We review the syntax of SDE.

Definition 4.1 (Single-Decryptor Encryption [CLLZ21]). *A single-decryptor encryption scheme* SDE *is a tuple of four algorithms* $(\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{Dec})$*. Below, let* $\mathcal{M}$ *be the message space of* SDE*.*

$\mathsf{Setup}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$**:** *The setup algorithm takes a security parameter* 1^λ*, and outputs a public key* pk *and a secret key* sk*.*

$\mathcal{KG}(\mathsf{sk}) \to \mathit{sk}$**:** *The key generation algorithm* $\mathcal{KG}$ *takes a secret key* sk*, and outputs a quantum secret key* sk*.*

$\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$**:** *The encryption algorithm takes a public key* pk *and a message* $m \in \mathcal{M}$*, and outputs a ciphertext* ct*.*

$\mathcal{Dec}(\mathit{sk}, \mathsf{ct}) \to \tilde{m}$**:** *The decryption algorithm takes a quantum secret key* sk *and a ciphertext* ct*, and outputs a message* $\tilde{m} \in \{\bot\} \cup \mathcal{M}$*.*

Correctness: *For every* $m \in \mathcal{M}$*, we require*

$$\Pr\left[\mathcal{Dec}(\mathit{sk}, \mathsf{ct}) = m \;\middle|\; \begin{array}{l}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathit{sk} \leftarrow \mathcal{KG}(\mathsf{sk}) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)\end{array}\right] = 1 - \mathsf{negl}(\lambda).$$

4.2 New Security Definition: CPA$^+$Anti-Piracy Security

We introduce a new security notion for SDE, which we call CPA$^+$anti-piracy security. Syntactically, it is very similar to CPA-style anti-piracy introduced in [CLLZ21], with the only difference being a modification to the winning condition.

Definition 4.2 (CPA$^+$Anti-Piracy Security). *Let* $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{Dec})$ *be an SDE scheme. We consider the* $\mathcal{D}$*-CPA$^+$anti-piracy game* $\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ *between the challenger and an adversary* $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ *below.*

1. *The challenger generates* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$*.*
2. *The challenger generates* $\mathit{sk} \leftarrow \mathcal{KG}(\mathsf{sk})$ *and sends* $(1^\lambda, \mathsf{pk}, \mathit{sk})$ *to* $\mathcal{A}$*.*

3. *$\mathcal{A}$ chooses two pairs of messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) \in \mathcal{M}^2$ and $(m_{\mathcal{C},0}, m_{\mathcal{C},1}) \in \mathcal{M}^2$ such that $|m_{\mathcal{B},0}| = |m_{\mathcal{B},1}|$ and $|m_{\mathcal{C},0}| = |m_{\mathcal{C},1}|$, and creates a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then, $\mathcal{A}$ sends $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ to the challenger, register $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}$, and register $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{C}$.*

4. *The challenger chooses $\mathsf{coin}_{\mathcal{B}} \leftarrow \{0,1\}$ and $\mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}$, generates $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$ and $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}})$, and sends $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.*

5. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$. The challenger outputs 1 if $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ otherwise outputs 0.*

We say that SDE *is $\mathcal{D}$-CPA$^+$ anti-piracy secure if for any QPT adversary $\mathcal{A}_{\mathsf{sde}}$, it holds that*

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Remark 4.3. The definition is equivalent even if we replace the required inequality with

$$\left|\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda).$$

Note that a similar equivalence does not hold for CPA-style anti-piracy introduced in [CLLZ21], highlighting a crucial difference between them.

5 Construction of SDE with CPA$^+$ Anti-Piracy

In this section, we prove the following theorem.

Theorem 5.1. *If there exist a secure IO for polynomial size classical circuits and OWFs, then there exists a SDE scheme that satisfies CPA$^+$ anti-piracy security with message space $\{0,1\}^{\ell_{\mathsf{msg}}(\lambda)}$ for any polynomial ℓ_{msg}.*

5.1 Strong Monogamy Property of Coset States

We recall the coset state and its strong monogamy properties [CLLZ21].

Notations. For a subspace $A \subseteq \mathbb{F}_2^n$, we use the following notations introduced by [CLLZ21, AKL$^+$22].

- $A^\perp := \{b \in \mathbb{F}_2^n : \forall a \in A\ \langle a, b\rangle = 0\}$.
- Can_A is a function such that for any $s \in \mathbb{F}_2^n$, $\mathsf{Can}_A(s)$ is the lexicographically smallest vector contained in $A + s$, which we call the canonical representative of coset $A + s$. For any $s' \in A + s$, we have $\mathsf{Can}_A(s') = \mathsf{Can}_A(s)$. Can_A is polynonial-time computable given the description of A.
- $\mathsf{CS}(A) = \{\mathsf{Can}_A(s) : s \in \mathbb{F}_2^n\}$.

For a subspace $A \subseteq \mathbb{F}_2^n$ and two canonical representatives $(s,t) \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$, we define the *coset state* $|A_{s,t}\rangle$ as

$$|A_{s,t}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{\langle a,t\rangle} |a + s\rangle .$$

By applying $H^{\otimes n}$ to $|A_{s,t}\rangle$, we obtain $\left|A^\perp_{t,s}\right\rangle$, where H is the Hadamard gate (thus $H^{\otimes n}$ is the Quantum Fourier Transformation over $\mathbb{F}_2^n$.)

When the context is clear, we below use $A + s$ to refer to the program that verifies membership in $A + s$. In particular, we will often write $i\mathcal{O}(A + s)$ to denote an obfuscation by $i\mathcal{O}$ of the the program that verifies membership in $A + s$.

Strong monogamy property. The computational strong monogamy property of coset states, stated below, was proven by Coladangelo et al. [CLLZ21] based on a conjecture, which was subsequently proven by Culf and Vidick [CV22].

Theorem 5.2 (Computational Strong Monogamy Property of Coset States [CLLZ21, CV22]). *Let $i\mathcal{O}$ be IO. Consider the following experiment $\mathsf{Exp}^{\mathsf{comp\text{-}strong\text{-}moe}}_{i\mathcal{O},\mathcal{A}_{\mathsf{moe}}}(\lambda)$ between a challenger and an adversary $\mathcal{A}_{\mathsf{moe}} = (\mathcal{A},\mathcal{B},\mathcal{C})$.*

1. *The challenger picks a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$, and two uniformly random canonical representatives $(s,t) \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. It sends $|A_{s,t}\rangle$, $i\mathcal{O}(A+s)$, and $i\mathcal{O}(A^\perp+t)$ to $\mathcal{A}$.*
2. *$\mathcal{A}$ creates a bipartite state q over registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$. Then, $\mathcal{A}$ sends register $\mathsf{R}_\mathcal{B}$ to $\mathcal{B}$ and register $\mathsf{R}_\mathcal{C}$ to $\mathcal{C}$.*
3. *The description of A is then sent to both $\mathcal{B}$ and $\mathcal{C}$.*
4. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $s_\mathcal{B}$ and $t_\mathcal{C}$. The challenger outputs 1 if $s_\mathcal{B} \in (A+s)$ and $t_\mathcal{C} \in (A^\perp+t)$, and outputs 0 otherwise*

Assuming $i\mathcal{O}$ is a secure IO and there exist OWFs, for any QPT adversary $\mathcal{A}_{\mathsf{moe}} = (\mathcal{A},\mathcal{B},\mathcal{C})$ and polynomial n of λ, it holds that

$$\Pr\left[\mathsf{Exp}^{\mathsf{comp\text{-}strong\text{-}moe}}_{i\mathcal{O},\mathcal{A}_{\mathsf{moe}}}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda).$$

Remark 5.3. The original proof in [CLLZ21] assumes the existence of IO and *injective* OWFs. However, it is known that injective OWFs exist if IO and OWFs exist [BPW16].[5]

In Theorem 5.2, note that the statement remains equivalent even if the goals of $\mathcal{B}$ and $\mathcal{C}$ are modified to output s and t, respectively. With this observation, the following corollary follows immediately from Theorem 5.2 and Lemma 3.3.

Theorem 5.4 (Computational Strong Indistinguishability Monogamy Property of Coset States). *Let $i\mathcal{O}$ be IO. Consider the following experiment $\mathsf{Exp}^{\mathsf{comp\text{-}strong\text{-}ind\text{-}moe}}_{i\mathcal{O},\mathcal{A}_{\mathsf{moe}}}(\lambda)$ between a challenger and an adversary $\mathcal{A}_{\mathsf{moe}} = (\mathcal{A},\mathcal{B},\mathcal{C})$.*

1. *The challenger picks a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$, and two uniformly random canonical representatives $(s,t) \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. It sends $|A_{s,t}\rangle$, $i\mathcal{O}(A+s)$, and $i\mathcal{O}(A^\perp+t)$ to $\mathcal{A}$.*
2. *$\mathcal{A}$ creates a bipartite state q over registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$. Then, $\mathcal{A}$ sends register $\mathsf{R}_\mathcal{B}$ to $\mathcal{B}$ and register $\mathsf{R}_\mathcal{C}$ to $\mathcal{C}$.*
3. *The challenger chooses $r_\mathcal{B}, r_\mathcal{C} \leftarrow \{0,1\}^n$. The challenger sends $(A, r_\mathcal{B})$ to $\mathcal{B}$ and $(A, r_\mathcal{C})$ to $\mathcal{C}$.*
4. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $b_\mathcal{B}$ and $b_\mathcal{C}$. The challenger outputs 1 if $b_\mathcal{B} \oplus b_\mathcal{C} = \langle r_\mathcal{B}, s\rangle \oplus \langle r_\mathcal{C}, t\rangle$ and outputs 0 otherwise.*[6]

Assuming $i\mathcal{O}$ is a secure IO and there exist OWFs, for any QPT adversary $\mathcal{A}_{\mathsf{moe}} = (\mathcal{A},\mathcal{B},\mathcal{C})$ and polynomial n of λ, it holds that

$$\Pr\left[\mathsf{Exp}^{\mathsf{comp\text{-}strong\text{-}ind\text{-}moe}}_{i\mathcal{O},\mathcal{A}_{\mathsf{moe}}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

5.2 Construction

Let $i\mathcal{O}$ be IO for polynomial size classical circuits. We below construct a SDE scheme $\mathsf{SDE} = \mathsf{SDE}.(\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ for ℓ_{msg}-bit messages where $\ell_{\mathsf{msg}} = \ell_{\mathsf{msg}}(\lambda)$ is a polynomial.

$\mathsf{SDE.Setup}(1^\lambda)$**:**

- Generate a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$, and two uniformly random elements $s,t \in \mathbb{F}_2^n$, where $n = 2\lambda$.

[5] The proof in [BPW16] is in the classical setting, but the same proof works in the post-quantum setting as well.

[6] Recall that $r_\mathcal{B}$ is an n-bit string and $\mathsf{Can}_A(s)$ is an element of $\mathbb{F}_2^n$. However, $\langle r_\mathcal{B}, \mathsf{Can}_A(s)\rangle$ can be defined naturally by identifying elements of $\{0,1\}$ and $\mathbb{F}_2$.

$P[C, \mathsf{str}](x)$

Hardwired constant: A description of a circuit C with 1-bit output and a ℓ_{msg}-bit string str.

Input: $x \in \{0,1\}^n$.

1. If $C(x) = 1$, output str. Otherwise, output $0^{\ell_{\mathsf{msg}}}$.

Figure 4: The description of the circuit P.

- Outputs $\mathsf{sk} = (A, s, t)$ nad $\mathsf{pk} = (i\mathcal{O}(A+s), i\mathcal{O}(A^\perp + t))$.

$\mathsf{SDE}.\mathcal{KG}(\mathsf{sk})$**:**

- Parse $\mathsf{sk} = (A, s, t)$ and output $s\mathcal{k} := |A_{s,t}\rangle$.

$\mathsf{SDE}.\mathsf{Enc}(\mathsf{ek}, m)$**:**

- Parse $\mathsf{pk} = (C_{\mathsf{mc}}, C^\perp_{\mathsf{mc}})$, where C_{mc} and $C^\perp_{\mathsf{mc}}$ are interpreted as circuit descriptions that are respectively supposed to be $i\mathcal{O}(A+s)$ and $i\mathcal{O}(A^\perp + t)$.
- Generate $k \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}$.
- Generate two obfuscated circuits $\widetilde{P} \leftarrow i\mathcal{O}(P[C_{\mathsf{mc}}, k \oplus m])$ and $\widetilde{P}^\perp \leftarrow i\mathcal{O}(P[C^\perp_{\mathsf{mc}}, k])$, where P is a circuit described in Figure 4.
- Output $\mathsf{ct} := (\widetilde{P}, \widetilde{P}^\perp)$.

$\mathsf{SDE}.\mathcal{D}ec(s\mathcal{k}, \mathsf{ct})$**:**

- Parse $\mathsf{ct} = (\widetilde{P}, \widetilde{P}^\perp)$, where $\widetilde{P}$ and $\widetilde{P}^\perp$ are interpreted as descriptions of circuits with n-bit input and ℓ_{msg}-bit output. Let $s\mathcal{k}$ be a n qubit state.
- Let D and $D^\perp$ be unitaries that respectively work as follows:

$$|u\rangle|v\rangle \mapsto |u\rangle\left|v \oplus \widetilde{P}(u)\right\rangle \quad \text{and} \quad |u\rangle|v\rangle \mapsto |u\rangle\left|v \oplus \widetilde{P}^\perp(u)\right\rangle$$

  for any $u \in \{0,1\}^n$ and $v \in \{0,1\}^{\ell_{\mathsf{msg}}}$.
- Apply D to $s\mathcal{k} \otimes \left|0^{\ell_{\mathsf{msg}}}\right\rangle$ and measure the second register to obtain an outcome m'_1. Then, trace out the second register and obtain the state $s\mathcal{k}'$.
- Apply $D^\perp$ to $H^{\otimes n} s\mathcal{k}' \otimes \left|0^{\ell_{\mathsf{msg}}}\right\rangle$ and measure the second register to obtain an outcome m'_2.
- Output $m' := m'_1 \oplus m'_2$.

Correctness. Fix $m \in \{0,1\}^{\ell_{\mathsf{msg}}}$. Suppose that $\mathsf{pk} = (C_{\mathsf{mc}} = i\mathcal{O}(A+s), C^\perp_{\mathsf{mc}} = i\mathcal{O}(A^\perp + t))$, $s\mathcal{k} = |A_{s,t}\rangle$, and $\mathsf{ct} = (\widetilde{P}, \widetilde{P}^\perp)$ where $\widetilde{P} = i\mathcal{O}(P[C_{\mathsf{mc}}, k \oplus m])$ and $\widetilde{P}^\perp = i\mathcal{O}(P[C^\perp_{\mathsf{mc}}, k])$, are generated as specified in the description of SDE. Let m'_1 and m'_2 be the values computed when executing $\mathsf{SDE}.\mathcal{D}ec(s\mathcal{k}, \mathsf{ct})$.

We first prove that $m'_1 = k \oplus m$ holds. For any $a \in A$, we have $\widetilde{P}_1(a+s) = k \oplus m$ from the functionality of $i\mathcal{O}$. Thus, given that $s\mathcal{k} = |A_{s,t}\rangle = |A_{s,t}\rangle = \frac{1}{\sqrt{|A|}}\sum_{a\in A}(-1)^{\langle a,t\rangle}|a+s\rangle$, if we apply the unitary D_1 to $s\mathcal{k} \otimes \left|0^{\ell_{\mathsf{msg}}}\right\rangle$, we obtain the state $s\mathcal{k} \otimes |k \oplus m\rangle$. This means $m'_1 = k \oplus m$ holds, and the state obtained by tracing out the second register after measuring m'_1 is $s\mathcal{k}$.

We then prove that $m'_2 = k$ holds. For any $a \in A^\perp$, we have $\widetilde{P}_2(a+t) = k$ from the functionality of $i\mathcal{O}$. Thus, given that $H^{\otimes n} s\mathcal{k} = H^{\otimes n}|A_{s,t}\rangle = \frac{1}{\sqrt{|A^\perp|}}\sum_{a\in A^\perp}(-1)^{\langle a,s\rangle}|a+t\rangle$, if we apply the unitary D_2 to $H^{\otimes n} s\mathcal{k} \otimes \left|0^{\ell_{\mathsf{msg}}}\right\rangle$, we obtain the state $H^{\otimes n} s\mathcal{k} \otimes |k\rangle$. This means $m'_2 = k$ holds.

The above shows the correctness of SDE.

5.3 Proof of Security

We prove the following theorem.

Theorem 5.5. *Assuming $i\mathcal{O}$ is a secure IO and there exist OWFs, then* SDE *satisfies CPA$^+$anti-piracy security.*

Proof. Let $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ be a QPT adversary against CPA$^+$anti-piracy security of SDE. We consider the following sequence of hybrids.

Hyb_0**:** This is the original security experiment $\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda)$. More specifically, it works as follows.

1. The challenger generates a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$, and two uniformly random elements $s, t \in \mathbb{F}_2^n$. The challenger then sends 1^λ, $\mathsf{pk} := (\mathsf{C}_{\mathsf{mc}} = i\mathcal{O}(A+s), \mathsf{C}^\perp_{\mathsf{mc}} = i\mathcal{O}(A^\perp + t))$, and $\mathsf{sk} := |A_{s,t}\rangle$ to $\mathcal{A}$.
2. $\mathcal{A}$ creates a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then, $\mathcal{A}$ sends $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ to the challenger, register $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}$, and register $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{C}$.
3. The challenger chooses $\mathsf{coin}_{\mathcal{B}} \leftarrow \{0,1\}$ and $\mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}$, and generates $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ as follows.
   - Generate $k_{\mathcal{B}} \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}$, $\widetilde{P}_{\mathcal{B}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}}])$, and $\widetilde{P}^\perp_{\mathcal{B}} \leftarrow i\mathcal{O}(P[\mathsf{C}^\perp_{\mathsf{mc}}, k_{\mathcal{B}}])$, and set $\mathsf{ct}_{\mathcal{B}} := (\widetilde{P}_{\mathcal{B}}, \widetilde{P}^\perp_{\mathcal{B}})$.
   - Generate $k_{\mathcal{C}} \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}$, $\widetilde{P}_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}}])$, and $\widetilde{P}^\perp_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}^\perp_{\mathsf{mc}}, k_{\mathcal{C}}])$, and set $\mathsf{ct}_{\mathcal{C}} := (\widetilde{P}_{\mathcal{C}}, \widetilde{P}^\perp_{\mathcal{C}})$.

   The challenger sends $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.
4. $\mathcal{B}$ and $\mathcal{C}$ respectively output $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$. The challenger outputs 1 if $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ otherwise outputs 0.

By the definition, we clearly have

$$\Pr[\mathsf{Hyb}_0 = 1] = \Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right].$$

Hyb_1**:** This is identical to Hyb_0 except that $\mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}}$ are replaced with $\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle$ and $\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle$, respectively, where $r_{\mathcal{B}}, r_{\mathcal{C}} \leftarrow \{0,1\}^n$. More specifically, the following three changes are applied.

- $\widetilde{P}_{\mathcal{B}}$ is generated as $\widetilde{P}_{\mathcal{B}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle}])$.
- $\widetilde{P}_{\mathcal{C}}$ is generated as $\widetilde{P}_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle}])$.
- The challenger outputs 1 if $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle$ and otherwise outputs 0.

Since $\mathsf{coin}_{\mathcal{B}}$ (resp. $\mathsf{coin}_{\mathcal{C}}$) is distributed uniformly at random, so is $\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s\rangle$ (resp. $\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle$). Thus, we have

$$\Pr[\mathsf{Hyb}_0 = 1] = \Pr[\mathsf{Hyb}_1 = 1].$$

Hyb_2**:** This is identical to Hyb_1 except that $\mathsf{ct}_{\mathcal{C}}$ is generated as follows.

- Generate $k_{\mathcal{C}} \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}$, $\widetilde{P}_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{C}}])$, and $\widetilde{P}^\perp_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}^\perp_{\mathsf{mc}}, k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle}])$, and set $\mathsf{ct}_{\mathcal{C}} := (\widetilde{P}_{\mathcal{C}}, \widetilde{P}^\perp_{\mathcal{C}})$.

The tuple $(k_{\mathcal{C}}, k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle})$ is distributed identically to $(k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t\rangle}, k_{\mathcal{C}})$. Thus, we have

$$\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1].$$

We below use the circuit Q described in Figure 5.

$Q[C, S, \mathsf{coin}, r, \mathsf{str}_0, \mathsf{str}_1, k](x)$

Hardwired constant: A description of a circuit C with 1-bit output, a description of a $n/2$-dimensional subspace S of $\mathbb{F}_2^n$, a single bit coin, n-bit string r, and ℓ_{msg}-bit strings $\mathsf{str}_0, \mathsf{str}_1, k$.

Input: $x \in \{0,1\}^n$.

1. If $C(x) = 1$, output $k \oplus \mathsf{str}_{\mathsf{coin} \oplus \langle r, \mathsf{Can}_S(x) \rangle}$. Otherwise, output $0^{\ell_{\mathsf{msg}}}$.

Figure 5: The description of the circuit Q.

Hyb_3**:** This is identical to Hyb_2 except that $\widetilde{P}_{\mathcal{B}}$ is generated as $\widetilde{P}_{\mathcal{B}} \leftarrow i\mathcal{O}(Q[\mathsf{C}_{\mathsf{mc}}, A, \mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, k_{\mathcal{B}}])$.

We prove that $P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s \rangle}]$ and $Q[\mathsf{C}_{\mathsf{mc}}, A, \mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, k_{\mathcal{B}}]$ are functionally equivalent. First, for x such that $\mathsf{C}_{\mathsf{mc}}(x) = 0$, that is, $x \notin A + s$, both circuits outputs $0^{\ell_{\mathsf{msg}}}$. Next, we consider x such that $\mathsf{C}_{\mathsf{mc}}(x) = 1$, that is, $x \in A + s$. For such x, $Q[\mathsf{C}_{\mathsf{mc}}, A, \mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, k_{\mathcal{B}}]$ outputs $k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, \mathsf{Can}_A(x) \rangle}$. For x such that $x \in A + s$, we have $\mathsf{Can}_A(x) = s$. Therefore, we have

$$\begin{aligned} Q[\mathsf{C}_{\mathsf{mc}}, A, \mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, k_{\mathcal{B}}](x) &= k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, \mathsf{Can}_A(x) \rangle} \\ &= k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s \rangle} \\ &= P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{B}} \oplus m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}} \oplus \langle r_{\mathcal{B}}, s \rangle}](x) \end{aligned}$$

for x such that $x \in A + s$. This shows that the two circuits are functionally equivalent.

From the above discussion and the security of $i\mathcal{O}$, we have

$$|\Pr[\mathsf{Hyb}_2 = 1] - \Pr[\mathsf{Hyb}_3 = 1]| = \mathsf{negl}(\lambda).$$

Hyb_4**:** This is identical to Hyb_3 except that $\widetilde{P}^{\perp}_{\mathcal{C}}$ is generated as $\widetilde{P}^{\perp}_{\mathcal{C}} \leftarrow i\mathcal{O}(Q[\mathsf{C}^{\perp}_{\mathsf{mc}}, A^{\perp}, \mathsf{coin}_{\mathcal{C}}, r_{\mathcal{C}}, m_{\mathcal{C},0}, m_{\mathcal{C},1}, k_{\mathcal{C}}])$.

Similarly to the previous step, we can show that $P[\mathsf{C}^{\perp}_{\mathsf{mc}}, k_{\mathcal{C}} \oplus m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{C}}, t \rangle}]$ and $Q[\mathsf{C}^{\perp}_{\mathsf{mc}}, A^{\perp}, \mathsf{coin}_{\mathcal{C}}, r_{\mathcal{C}}, m_{\mathcal{C},0}, m_{\mathcal{C},1}, k_{\mathcal{C}}]$ are functionally equivalent. Thus, from the security of $i\mathcal{O}$, we have

$$|\Pr[\mathsf{Hyb}_3 = 1] - \Pr[\mathsf{Hyb}_4 = 1]| = \mathsf{negl}(\lambda).$$

Below, by a reduction to the computational strong indistinguishability monogamy property of coset states (Theorem 5.4), we show

$$\Pr[\mathsf{Hyb}_4 = 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

To this end, we construct the following adversary $\mathcal{A}_{\mathsf{moe}} = (\widehat{\mathcal{A}}, \widehat{\mathcal{B}}, \widehat{\mathcal{C}})$ using $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$.

1. On input $|A_{s,t}\rangle$, $\mathsf{C}_{\mathsf{mc}} = i\mathcal{O}(A + s)$, and $\mathsf{C}^{\perp}_{\mathsf{mc}} = i\mathcal{O}(A^{\perp} + t)$, $\widehat{\mathcal{A}}$ invokes $\mathcal{A}$ with 1^{λ}, $\mathsf{pk} = (\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^{\perp}_{\mathsf{mc}})$, and $\mathsf{sk} = |A_{s,t}\rangle$.
2. When $\mathcal{A}$ outputs a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$, and the challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$, $\widehat{\mathcal{A}}$ sends $(\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^{\perp}_{\mathsf{mc}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, q[\mathsf{R}_{\mathcal{B}}])$ to $\mathcal{B}$ and $(\mathsf{C}_{\mathsf{mc}}, \mathsf{C}^{\perp}_{\mathsf{mc}}, m_{\mathcal{C},0}, m_{\mathcal{C},1}, q[\mathsf{R}_{\mathcal{C}}])$ to $\mathcal{C}$.
3. $\widehat{\mathcal{B}}$ and $\widehat{\mathcal{C}}$ are respectively given $(A, r_{\mathcal{B}})$ and $(A, r_{\mathcal{C}})$ and behave as follows.
   - $\widehat{\mathcal{B}}$ generates $\mathsf{coin}_{\mathcal{B}} \leftarrow \{0,1\}$, $k_{\mathcal{B}} \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}$, $\widetilde{P}_{\mathcal{B}} \leftarrow i\mathcal{O}(Q[\mathsf{C}_{\mathsf{mc}}, A, \mathsf{coin}_{\mathcal{B}}, r_{\mathcal{B}}, m_{\mathcal{B},0}, m_{\mathcal{B},1}, k_{\mathcal{B}}])$, and $\widetilde{P}^{\perp}_{\mathcal{B}} \leftarrow i\mathcal{O}(P[\mathsf{C}^{\perp}_{\mathsf{mc}}, k_{\mathcal{B}}])$. Then $\widehat{\mathcal{B}}$ invokes $\mathcal{B}$ with $q[\mathsf{R}_{\mathcal{B}}]$ and $\mathsf{ct}_{\mathcal{B}} = (\widetilde{P}_{\mathcal{B}}, \widetilde{P}^{\perp}_{\mathcal{B}})$, and obtains $\mathsf{coin}'_{\mathcal{B}}$. $\widehat{\mathcal{B}}$ outputs $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}}$.
   - $\widehat{\mathcal{C}}$ generates $\mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}, k_{\mathcal{C}} \leftarrow \{0,1\}^{\ell_{\mathsf{msg}}}, \widetilde{P}_{\mathcal{C}} \leftarrow i\mathcal{O}(P[\mathsf{C}_{\mathsf{mc}}, k_{\mathcal{C}}])$, and $\widetilde{P}^{\perp}_{\mathcal{C}} \leftarrow i\mathcal{O}(Q[\mathsf{C}^{\perp}_{\mathsf{mc}}, A^{\perp}, \mathsf{coin}_{\mathcal{C}}, r_{\mathcal{C}}, m_{\mathcal{C},0}, m_{\mathcal{C},1}, k_{\mathcal{C}}])$. Then $\widehat{\mathcal{C}}$ invokes $\mathcal{C}$ with $q[\mathsf{R}_{\mathcal{C}}]$ and $\mathsf{ct}_{\mathcal{C}} = (\widetilde{P}_{\mathcal{C}}, \widetilde{P}^{\perp}_{\mathcal{C}})$, and obtains $\mathsf{coin}'_{\mathcal{C}}$. $\widehat{\mathcal{C}}$ outputs $\mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}}$.

$\mathcal{A}_{\mathsf{moe}}$ perfectly simulates Hyb_4 for $\mathcal{A}_{\mathsf{sde}}$. If $\mathcal{A}_{\mathsf{sde}}$ wins the simulated experiment (i.e., Hyb_4 outputs 1), we have $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \oplus \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle$, that is, $(\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}}) \oplus (\mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}}) = \langle r_{\mathcal{B}}, s\rangle \oplus \langle r_{\mathcal{C}}, t\rangle$. Thus, by Theorem 5.4, we have

$$\Pr[\mathsf{Hyb}_4 = 1] = \Pr\left[\mathsf{Exp}^{\mathsf{comp\text{-}strong\text{-}ind\text{-}moe}}_{i\mathcal{O},\mathcal{A}_{\mathsf{moe}}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Combining the above, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

This completes the proof of Theorem 5.5. □

6 Relationship among Security Definitions

In this section, we review the existing security definitions of SDE and discuss their relationships with CPA$^+$anti-piracy security. In particular, we show that CPA$^+$anti-piracy security implies most of the existing security definitions.

6.1 Existing Security Definitions and Their Generalizations

The literature presents a variety of security notions for SDE. To provide a unified framework for their presentation, we adopt the approach of Ananth and Behera [AB24], defining $\mathcal{D}$-search anti-piracy security and $\mathcal{D}$-CPA anti-piracy security parameterized by a distribution $\mathcal{D}$.[7] We also review strong anti-piracy security introduced in [CLLZ21].

Search anti-piracy security. First, we define a search-type definition of security called search anti-piracy, which is a generalization of random-challenge anti-piracy security in [CLLZ21].

Definition 6.1 ($\mathcal{D}$-Search Anti-Piracy Security). *Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M}$. Let $\mathcal{D}$ be a QPT algorithm that takes the security parameter 1^λ as input and outputs two messages $m_{\mathcal{B}}, m_{\mathcal{C}}$ and a quantum state aux. We consider the $\mathcal{D}$-search anti-piracy game $\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ between the challenger and an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ below.*

1. *The challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and $sk \leftarrow \mathcal{KG}(\mathsf{sk})$.*
2. *The challenger generates $(m_{\mathcal{B}}, m_{\mathcal{C}}, aux) \leftarrow \mathcal{D}(1^\lambda, \mathsf{pk})$ and sends $(1^\lambda, \mathsf{pk}, sk, aux)$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ creates a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then, $\mathcal{A}$ sends register $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}$ and register $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{C}$.*
4. *The challenger generates $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{B}})$ and $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{C}})$, and sends $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.*
5. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $m'_{\mathcal{B}}$ and $m'_{\mathcal{C}}$. The challenger outputs 1 if $m'_{\mathcal{B}} = m_{\mathcal{B}}$ and $m'_{\mathcal{C}} = m_{\mathcal{C}}$ and otherwise outputs 0.*

We say that SDE is $\mathcal{D}$-search anti-piracy secure if for any QPT adversary $\mathcal{A}_{\mathsf{sde}}$, it holds that

$$\Pr\left[\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda).$$

Remark 6.2 (Comparison with the definition in [AB24]). The above definition is identical to the one in [AB24, Appendix A.2] except that we consider auxiliary input aux that may be correlated with the challenge messages $(m_{\mathcal{B}}, m_{\mathcal{C}})$ and allow the distribution to be dependent on pk.

[7] Strictly speaking, $\mathcal{D}$ stands for a QPT sampler for some distribution rather than the distribution itself.

Remark 6.3. The above definition allows $m_{\mathcal{B}}$ and $m_{\mathcal{C}}$ to be correlated, but assumes that $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ are generated under independent randomness. However, we can show that security under the correlated randomness follows from that under the independent randomness using the result of Ananth et al. [AKL23].

Example 6.4. We are aware of the following instantiations of $\mathcal{D}$ considered in the literature.

$\mathcal{U}(1^\lambda, \mathsf{pk})$: Choose $m_{\mathcal{B}} \leftarrow \mathcal{M}$ and $m_{\mathcal{C}} \leftarrow \mathcal{M}$ and output $(m_{\mathcal{B}}, m_{\mathcal{C}}, \mathsf{null})$ where null is a null string.

$\mathsf{Id}_{\mathcal{U}}(1^\lambda, \mathsf{pk})$: Choose $m_{\mathcal{B}} \leftarrow \mathcal{M}$, set $m_{\mathcal{C}} := m_{\mathcal{B}}$, and output $(m_{\mathcal{B}}, m_{\mathcal{C}}, \mathsf{null})$ where null is a null string.

Random-challenge anti-piracy security in [CLLZ21] is captured as $\mathcal{U}$-search anti-piracy security. They constructed a scheme that satisfies it assuming subexponentially secure iO and OWFs and the LWE assumption. Ananth and Behera [AB24] constructed a scheme that is $\mathcal{U}$- and $\mathsf{Id}_{\mathcal{U}}$- search anti-piracy secure, assuming subexponentially secure iO and OWFs, the LWE assumption, and conjectures called the simultaneous inner product conjectures.

In this paper, we consider $\mathcal{D}$-search anti-piracy for general $\mathcal{D}$ that satisfies unpredictability defined below:

Definition 6.5 (Unpredictable Sampler). *Let $\mathcal{D}$ be as in Definition 6.1. We say that $\mathcal{D}$ is an unpredictable sampler if for any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\mathcal{A}(aux) \in \{m_{\mathcal{B}}, m_{\mathcal{C}}\} : (m_{\mathcal{B}}, m_{\mathcal{C}}, aux) \leftarrow \mathcal{D}(1^\lambda)\right] \leq \mathsf{negl}(\lambda).$$

Example 6.6. Both $\mathcal{U}$ and $\mathsf{Id}_{\mathcal{U}}$ in Example 6.4 is an unpredictable sampler if $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$.

Remark 6.7. If $\mathcal{D}$ is not an unpredictable sampler, then $\mathcal{D}$-search anti-piracy security is trivially broken. Thus, unpredictability of $\mathcal{D}$ is the minimal assumption for the existence of an SDE scheme that satisfies $\mathcal{D}$-search anti-piracy security.

Definition 6.8 ($\mathcal{D}_{\mathsf{unp}}$-Search Anti-Piracy Security). *We say that an SDE scheme is $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy secure if it is $\mathcal{D}$-search anti-piracy secure for all unpredictable samplers $\mathcal{D}$ and the message space $\mathcal{M}$ satisfies $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$.*

Remark 6.9. When $|\mathcal{M}|^{-1}$ is non-negligible, there is no unpredictable sampler. To exclude such a meaningless case, we explicitly require $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$ in the above definition.

CPA anti-piracy security. Next, we define an indistinguishability-type definition of security called CPA anti-piracy security, which is a generalization of CPA-style anti-piracy security in [CLLZ21].

Definition 6.10 ($\mathcal{D}$-CPA Anti-Piracy Security). *Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme. Let $\mathcal{D}$ be a QPT algorithm that takes a public key pk and four messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ as input and outputs two bits $\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}}$ and two ciphertexts $\mathsf{ct}_{\mathcal{B}}, \mathsf{ct}_{\mathcal{C}}$. We consider the $\mathcal{D}$-CPA anti-piracy game $\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ between the challenger and an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ below.*

1. *The challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$.*
2. *The challenger generates $sk \leftarrow \mathcal{KG}(\mathsf{sk})$ and sends $(1^\lambda, \mathsf{pk}, sk)$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ chooses two pairs of messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) \in \mathcal{M}^2$ and $(m_{\mathcal{C},0}, m_{\mathcal{C},1}) \in \mathcal{M}^2$ such that $|m_{\mathcal{B},0}| = |m_{\mathcal{B},1}|$ and $|m_{\mathcal{C},0}| = |m_{\mathcal{C},1}|$, and creates a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then, $\mathcal{A}$ sends $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ to the challenger, register $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}$, and register $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{C}$.*
4. *The challenger generates $(\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}}, \mathsf{ct}_{\mathcal{B}}, \mathsf{ct}_{\mathcal{C}}) \leftarrow \mathcal{D}(1^\lambda, \mathsf{pk}, (m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1}))$, and sends $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.*
5. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$. The challenger outputs 1 if $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$ and otherwise outputs 0.*

We say that SDE *is* $\mathcal{D}$*-CPA anti-piracy secure if for any QPT adversary* $\mathcal{A}_{\mathsf{sde}}$*, it holds that*

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right]\leq\frac{1}{2}+\mathsf{negl}(\lambda).$$

Remark 6.11 (Comparison with the definition in [AB24]). The above definition is identical to the one in [AB24, Appendix A.2] except that we consider separate challenge bits $\mathsf{coin}_{\mathcal{B}},\mathsf{coin}_{\mathcal{C}}$ for each party and treat them as output of $\mathcal{D}$ rather than input. This modification is made to also capture the CPA-style anti-piracy of [CLLZ21] in a unified manner.

Example 6.12. We are aware of the following instantiations of $\mathcal{D}$ considered in the literature.

$\mathcal{D}_{\mathsf{ind\text{-}bit}}(1^\lambda,\mathsf{pk},(m_{\mathcal{B},0},m_{\mathcal{B},1},m_{\mathcal{C},0},m_{\mathcal{C},1}))$: Choose $\mathsf{coin}_{\mathcal{B}}\leftarrow\{0,1\}$ and $\mathsf{coin}_{\mathcal{C}}\leftarrow\{0,1\}$, generate $\mathsf{ct}_{\mathcal{B}}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$ and $\mathsf{ct}_{\mathcal{C}}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}})$, and output $(\mathsf{coin}_{\mathcal{B}},\mathsf{coin}_{\mathcal{C}},\mathsf{ct}_{\mathcal{B}},\mathsf{ct}_{\mathcal{C}})$.

$\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}(1^\lambda,\mathsf{pk},(m_{\mathcal{B},0},m_{\mathcal{B},1},m_{\mathcal{C},0},m_{\mathcal{C},1}))$: Choose $\mathsf{coin}_{\mathcal{B}}\leftarrow\{0,1\}$, set $\mathsf{coin}_{\mathcal{C}}:=\mathsf{coin}_{\mathcal{B}}$, generate $\mathsf{ct}_{\mathcal{B}}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$ and $\mathsf{ct}_{\mathcal{C}}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}})$, and output $(\mathsf{coin}_{\mathcal{B}},\mathsf{coin}_{\mathcal{C}},\mathsf{ct}_{\mathcal{B}},\mathsf{ct}_{\mathcal{C}})$.

$\mathcal{D}_{\mathsf{identical}}(1^\lambda,\mathsf{pk},(m_{\mathcal{B},0},m_{\mathcal{B},1},m_{\mathcal{C},0},m_{\mathcal{C},1}))$: Choose $\mathsf{coin}_{\mathcal{B}}\leftarrow\{0,1\}$, set $\mathsf{coin}_{\mathcal{C}}:=\mathsf{coin}_{\mathcal{B}}$, generate $\mathsf{ct}_{\mathcal{B}}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$, set $\mathsf{ct}_{\mathcal{C}}:=\mathsf{ct}_{\mathcal{B}}$, and output $(\mathsf{coin}_{\mathcal{B}},\mathsf{coin}_{\mathcal{C}},\mathsf{ct}_{\mathcal{B}},\mathsf{ct}_{\mathcal{C}})$.[8]

CPA-style anti-piracy security in [CLLZ21] is captured as $\mathcal{D}_{\mathsf{ind\text{-}bit}}$-CPA anti-piracy security.[9] They construct a scheme that satisfies it assuming subexponentially secure iO and OWFs and the LWE assumption. Public-key security in [GZ20] is captured as $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security. They claim to construct a scheme that satisfies it assuming iO, OWF, and extractable witness encryption. However, there appears to be a technical issue in their proof [Zha22]. Ananth and Behera [AB24] constructed a scheme that is $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$- and $\mathcal{D}_{\mathsf{identical}}$- search anti-piracy secure, assuming subexponentially secure iO and OWFs, the LWE assumption, and conjectures called the simultaneous inner product conjectures.

Georgiou and Zhandry [GZ20] demonstrated that an SDE scheme satisfying $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security implies the existence of an unclonable encryption scheme. Since constructing unclonable encryption in the plain model has been considered a major open problem in the field, constructing an SDE scheme that satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the plain model would be extremely challenging.

Strong anti-piracy security. Finally, we review strong anti-piracy security introduced in [CLLZ21]. To state its definition, we first review definitions of quantum decryptors and tests for good quantum decryptors following [CLLZ21].

Definition 6.13 (Quantum Decryptor [CLLZ21]). *Let* q *and* $\boldsymbol{U}$ *be a quantum state and a unitary quantum circuit acting on* $n+m$ *qubits, where* m *is the number of qubits of* q *and* n *is the length of ciphertexts. A quantum decryptor for ciphertexts is a pair* $(q,\boldsymbol{U})$.

When we say that we run the quantum decryptor $(q,\boldsymbol{U})$ *on ciphertext* ct*, we execute the circuit* $\boldsymbol{U}$ *on input* $\mathsf{ct}\otimes q$.

Definition 6.14 (Testing a Quantum Decryptor [CLLZ21]). *Let* $\gamma\in[0,1]$. *Let* pk *and* (m_0,m_1) *be a public key and a pair of messages, respectively. A test for a* γ*-good quantum decryptor with respect to* pk *and* (m_0,m_1) *is the following procedure.*

- *The procedure takes as input a quantum decryptor* $\mathcal{D}=(q,\boldsymbol{U})$.
- *Let* $\mathcal{P}=(\boldsymbol{P},\boldsymbol{I}-\boldsymbol{P})$ *be the following mixture of projective measurements acting on a quantum state* $\widetilde{q}$*:*
  - *Sample a uniformly random* $\mathsf{coin}\leftarrow\{0,1\}$ *and compute* $\mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{pk},m_{\mathsf{coin}})$.
  - *Run* $\mathsf{coin}'\leftarrow\widetilde{\mathcal{D}}(\mathsf{ct})$*, where* $\widetilde{\mathcal{D}}=(\widetilde{q},\boldsymbol{U})$*. If* $\mathsf{coin}'=\mathsf{coin}$*, output* 1*, otherwise output* 0.

[8] $\mathcal{D}_{\mathsf{identical}}$ simply ignores $m_{\mathcal{C},0},m_{\mathcal{C},1}$. However, we include them as inputs for the sake of notational consistency.

[9] Strictly speaking, CPA-style anti-piracy security in [CLLZ21] is slightly weaker than $\mathcal{D}_{\mathsf{ind\text{-}bit}}$-CPA anti-piracy security since it imposes an additional constraint that $(m_{\mathcal{B},0},m_{\mathcal{B},1})=(m_{\mathcal{C},0},m_{\mathcal{C},1})$. See also Remark 6.18.

Let $\mathcal{TI}_{1/2+\gamma}(\mathcal{P})$ be the threshold implementation of $\mathcal{P}$ with threshold $\frac{1}{2}+\gamma$. Apply $\mathcal{TI}_{1/2+\gamma}(\mathcal{P})$ to q. If the outcome is 1, we say that the test passed, otherwise the test failed.

We say that a quantum decryptor $\mathcal{D} = (q, \boldsymbol{U})$ is a γ-good quantum decryptor with respect to pk and (m_0, m_1) if it passes the above test with probability 1.

The following lemmas are immediate consequences of the fact that a threshold implementation is a projective measurement.

Lemma 6.15 ([CLLZ21, Corollary 6.9]). *Suppose that a quantum decryptor $\mathcal{D} = (q, \boldsymbol{U})$ passes the test for a γ-good quantum decryptor with respect to pk and (m_0, m_1). Let q' be the post-measurement state of the quantum part of the decryptor. Then the quantum decryptor $\mathcal{D} = (q', \boldsymbol{U})$ is a γ-good quantum decryptor with respect to pk and (m_0, m_1).*

Lemma 6.16 ([CLLZ21, Claim 6.18]). *Suppose that $(q[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}})$ is a γ-good quantum decryptor with respect to pk and $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$ and $(q[\mathsf{R}_C], \boldsymbol{U}_C)$ is a γ-good quantum decryptor with respect to pk and $(m_{C,0}, m_{C,1})$, where ρ is a bipartite state on registers $\mathsf{R}_{\mathcal{B}}$ and R_C. Let M be any POVM on $\mathsf{R}_{\mathcal{B}}$. Then, the post-measurement state on R_C together with $\boldsymbol{U}_C$ conditioned on any outcome is still a γ-good decryptor with respect to pk and $(m_{C,0}, m_{C,1})$.*

We are now ready to present the definition of strong anti-piracy security.

Definition 6.17 (Strong Anti-Piracy Security [CLLZ21]). *Let $\gamma : \mathbb{N} \to [0,1]$. We consider the strong γ-anti-piracy game $\mathsf{Exp}^{\mathsf{strong\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}}(\lambda, \gamma(\lambda))$ between the challenger and an adversary $\mathcal{A}$ below.*

1. *The challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$.*
2. *The challenger generates $sk \leftarrow \mathcal{KG}(\mathsf{sk})$ and sends $(1^\lambda, \mathsf{pk}, sk)$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ outputs $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{C,0}, m_{C,1}) \in \mathcal{M}^4$ and two (possibly entangled) quantum decryptors $\mathcal{D}_{\mathcal{B}} = (q[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}})$ and $\mathcal{D}_C = (q[\mathsf{R}_C], \boldsymbol{U}_C)$, where $|m_{\mathcal{B},0}| = |m_{\mathcal{B},1}|$ and $|m_{C,0}| = |m_{C,1}|$, q is a quantum state over registers $\mathsf{R}_{\mathcal{B}}$ and R_C, and $\boldsymbol{U}_{\mathcal{B}}$ and $\boldsymbol{U}_C$ are unitary quantum circuits.*
4. *The challenger runs the tests for a γ-good quantum decryptor (Definition 6.14) with respect to pk and $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$ on $\mathcal{D}_{\mathcal{B}}$, and with respect to pk and $(m_{C,0}, m_{C,1})$ on $\mathcal{D}_C$. The challenger outputs 1 if both tests pass; otherwise outputs 0.*

We say that SDE is strong γ-anti-piracy secure if for any QPT adversary $\mathcal{A}$, it satisfies that

$$\Pr\left[\mathsf{Exp}^{\mathsf{strong\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}}(\lambda, \gamma(\lambda)) = 1\right] \leq \mathsf{negl}(\lambda).$$

We say that SDE is strong anti-piracy secure if it is strong γ-anti-piracy secure for any inverse polynomial γ.

Remark 6.18. The original definition of strong anti-piracy security in [CLLZ21] is slightly weaker than the above since it imposes an additional constraint that $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) = (m_{C,0}, m_{C,1})$. However, we do not believe this constraint is essential. In fact, their security proof appears to remain valid even when $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) \neq (m_{C,0}, m_{C,1})$. Thus, we define it in a more general form that allows for $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) \neq (m_{C,0}, m_{C,1})$ as above.

Remark 6.19. [CLLZ21] also introduced a "strong" variant of random-challenge anti-piracy security in a similar manner. However, we observe that it is actually *equivalent* to the regular random challenge anti-piracy security.

6.2 CPA$^+$Anti-Piracy Implies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA Anti-Piracy

Theorem 6.20. *If an SDE scheme satisfies CPA$^+$anti-piracy security, then it also satisfies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security.*

Proof. Let $\mathcal{A}_{\mathsf{sde}}$ be any adversary against $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security of an SDE scheme SDE. We show that the same adversary $\mathcal{A}_{\mathsf{sde}}$ also breaks CPA$^+$anti-piracy security of SDE. In an execution of $\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda)$, let $\mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}}$ be the challenge bits chosen by the challenger for $\mathcal{B}$ and $\mathcal{C}$ and $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$ be the outputs of $\mathcal{B}$ and $\mathcal{C}$, respectively. Let $E_{\mathcal{B}}$ be the event that $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$, $E_{\mathcal{C}}$ be the event that $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$, and $E_{\mathsf{iden\text{-}bit}}$ be the event that $\mathsf{coin}_{\mathcal{B}} = \mathsf{coin}_{\mathcal{C}}$. Clearly, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}}] + \Pr[\neg E_{\mathcal{B}} \wedge \neg E_{\mathcal{C}}]$$

and

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}} \mid E_{\mathsf{iden\text{-}bit}}].$$

Our goal is to demonstrate that the former is greater than the latter. To prove this, we borrow the following claim that is implicitly shown in [AKY25].

Claim 6.21. Let E_0, E_1, E_2 be events. If $\Pr[E_0] = 1/2$, $\Pr[E_1 \mid E_0] = \Pr[E_1 \mid \neg E_0]$, and $\Pr[E_2 \mid E_0] = \Pr[E_2 \mid \neg E_0]$, then it holds that

$$\Pr[E_1 \wedge E_2] + \Pr[\neg E_1 \wedge \neg E_2] = \Pr[E_1 \wedge E_2 \mid E_0] + \Pr[\neg E_1 \wedge \neg E_2 \mid \neg E_0].$$

Claim 6.21 can be proven through straightforward probability calculations as in the proof of [AKY25, Lemma 18].

Clearly, we have $\Pr[E_{\mathsf{iden\text{-}bit}}] = 1/2$. Note that the view of $\mathcal{B}$ is independent of $E_{\mathsf{iden\text{-}bit}}$. Thus, by the no-signalling principle, we have

$$\Pr[E_{\mathcal{B}} \mid E_{\mathsf{iden\text{-}bit}}] = \Pr[E_{\mathcal{B}} \mid \neg E_{\mathsf{iden\text{-}bit}}].$$

Similarly, we have

$$\Pr[E_{\mathcal{C}} \mid E_{\mathsf{iden\text{-}bit}}] = \Pr[E_{\mathcal{C}} \mid \neg E_{\mathsf{iden\text{-}bit}}].$$

Thus, we can apply Claim 6.21 with $E_0 = E_{\mathsf{iden\text{-}bit}}$, $E_1 = E_{\mathcal{B}}$, and $E_2 = E_{\mathcal{C}}$ to obtain

$$\Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}}] + \Pr[\neg E_{\mathcal{B}} \wedge \neg E_{\mathcal{C}}] = \Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}} \mid E_{\mathsf{iden\text{-}bit}}] + \Pr[\neg E_{\mathcal{B}} \wedge \neg E_{\mathcal{C}} \mid \neg E_{\mathsf{iden\text{-}bit}}].$$

Since $\Pr[\neg E_{\mathcal{B}} \wedge \neg E_{\mathcal{C}} \mid \neg E_{\mathsf{iden\text{-}bit}}] \geq 0$, we have

$$\Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}}] + \Pr[\neg E_{\mathcal{B}} \wedge \neg E_{\mathcal{C}}] \geq \Pr[E_{\mathcal{B}} \wedge E_{\mathcal{C}} \mid E_{\mathsf{iden\text{-}bit}}].$$

This completes the proof of Theorem 6.20. □

6.3 $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA Anti-Piracy Implies $\mathcal{D}_{\mathsf{unp}}$-Search Anti-Piracy

Theorem 6.22. *If an SDE scheme satisfies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security and its message space $\mathcal{M}$ satisfies $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$, then it also satisfies $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security.*

Proof. Let SDE be a $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy secure SDE scheme. Assume toward contradiction that there is an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ that breaks $\mathcal{D}$-search anti-piracy security of SDE for some unpredictable sampler $\mathcal{D}$. Then we construct a QPT adversary $\tilde{\mathcal{A}}_{\mathsf{sde}} = (\tilde{\mathcal{A}}, \tilde{\mathcal{B}}, \tilde{\mathcal{C}})$ that breaks $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security of SDE as follows.

$\tilde{\mathcal{A}}$: Given the security parameter 1^λ, public key pk, and quantum secret key sk, $\tilde{\mathcal{A}}$ generates $(m_{\mathcal{B}}, m_{\mathcal{C}}, aux) \leftarrow \mathcal{D}(1^\lambda)$ and runs $\mathcal{A}$ on input $(1^\lambda, \mathsf{pk}, sk, aux)$ to obtain a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. $\tilde{\mathcal{A}}$ sends $(0^{|m_{\mathcal{B}}|}, m_{\mathcal{B}}, 0^{|m_{\mathcal{C}}|}, m_{\mathcal{C}})$ to the challenger, register $\mathsf{R}_{\mathcal{B}}$ and $m_{\mathcal{B}}$ to $\tilde{\mathcal{B}}$, and register $\mathsf{R}_{\mathcal{C}}$ and $m_{\mathcal{C}}$ to $\tilde{\mathcal{C}}$.

$\tilde{\mathcal{B}}$: Given register $\mathsf{R}_{\mathcal{B}}$, $m_{\mathcal{B}}$, and a ciphertext $\mathsf{ct}_{\mathcal{B}}$, run $\mathcal{B}$ on input $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{B}}$ to obtain $m'_{\mathcal{B}}$. $\tilde{\mathcal{B}}$ outputs 1 if $m'_{\mathcal{B}} = m_{\mathcal{B}}$ and outputs 0 otherwise.

$\tilde{\mathcal{C}}$: Given register $\mathsf{R}_{\mathcal{C}}$, $m_{\mathcal{C}}$, and a ciphertext $\mathsf{ct}_{\mathcal{C}}$, run $\mathcal{C}$ on input $\mathsf{R}_{\mathcal{C}}$ and $\mathsf{ct}_{\mathcal{C}}$ to obtain $m'_{\mathcal{C}}$. $\tilde{\mathcal{C}}$ outputs 1 if $m'_{\mathcal{C}} = m_{\mathcal{C}}$ and outputs 0 otherwise.

In an execution of $\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda)$, let $\mathsf{coin}_{\tilde{\mathcal{B}}}$ and $\mathsf{coin}_{\tilde{\mathcal{C}}}$ be the challenge bits chosen by the challenger for $\tilde{\mathcal{B}}$ and $\tilde{\mathcal{C}}$, respectively. Note that they are uniformly chosen under the constraint that $\mathsf{coin}_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}$. Clearly, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}\right].$$

Let E_b be the event that $\mathsf{coin}_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} = b$ for $b \in \{0,1\}$. Note that $\Pr[E_0] = \Pr[E_1] = 1/2$. Conditioned on E_1, $\tilde{\mathcal{A}}_{\mathsf{sde}}$ perfectly simulates $\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ for $\mathcal{A}_{\mathsf{sde}}$. Thus, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} \mid E_1\right].$$

On the other hand, by the unpredictability of $\mathcal{D}$, when E_0 occurs, $\mathcal{B}$ (resp. $\mathcal{C}$) outputs $m_{\mathcal{B}}$ (resp. $m_{\mathcal{C}}$) with a negligible probability, which implies that $\tilde{\mathcal{B}}$ (resp. $\tilde{\mathcal{C}}$) outputs 0 except for a negligible probability. Thus, we have

$$\Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} \mid E_0\right] \geq 1 - \mathsf{negl}(\lambda).$$

Combining the above, we have

$$\begin{aligned}\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] &= \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}\right] \\ &= \frac{1}{2}\Pr\left[\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] + \frac{1}{2}(1 - \mathsf{negl}(\lambda)).\end{aligned}$$

By the assumption that $\mathcal{A}_{\mathsf{sde}}$ breaks $\mathcal{D}$-search anti-piracy security, $\Pr\left[\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right]$ is non-negligible. Thus, $\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] - 1/2$ is non-negligible, which contradicts the assumed $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security. This completes the proof of Theorem 6.22. □

6.4 Equivalence between CPA$^+$and Strong Anti-Piracy

Theorem 6.23. *An SDE scheme satisfies CPA$^+$anti-piracy security if and only if it satisfies strong anti-piracy security.*

Proof. We prove each direction as follows.

CPA$^+$anti-piracy → Strong anti-piracy. Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme that satisfies CPA$^+$anti-piracy. Assume toward contradiction that SDE does not satisfy strong anti-piracy security. That is, suppose that SDE does not satisfy strong γ-anti-piracy secure for some inverse polynomial γ. Then, there is a QPT adversary $\mathsf{Strong}.\mathcal{A}$ such that $\mathsf{Adv}^{\mathsf{strong\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Strong}.\mathcal{A}}(\lambda,\gamma(\lambda))$ is non-negligible. Then we construct a QPT adversary $\mathsf{CPA}^+.\mathcal{A}_{\mathsf{sde}} = (\mathsf{CPA}^+.\mathcal{A}, \mathsf{CPA}^+.\mathcal{B}, \mathsf{CPA}^+.\mathcal{C})$ that breaks CPA$^+$anti-piracy security of SDE. Let $\epsilon = \frac{\gamma}{6}$ and $\delta = 2^{-\lambda}$. The adversary $\mathsf{CPA}^+.\mathcal{A}_{\mathsf{sde}} = (\mathsf{CPA}^+.\mathcal{A}, \mathsf{CPA}^+.\mathcal{B}, \mathsf{CPA}^+.\mathcal{C})$ works as follows:

$\mathsf{CPA}^+.\mathcal{A}$**:** Given the security parameter 1^λ, public key pk, and quantum secret key $s\mathcal{K}$, $\mathsf{CPA}^+.\mathcal{A}$ runs $\mathsf{Strong}.\mathcal{A}(1^\lambda, \mathsf{pk}, s\mathcal{K})$ to obtain challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and two (possibly entangled) quantum decryptors $\mathcal{D}_{\mathcal{B}} = (q[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}})$ and $\mathcal{D}_{\mathcal{C}} = (q[\mathsf{R}_{\mathcal{C}}], \boldsymbol{U}_{\mathcal{C}})$, where q is a quantum state over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$, and $\boldsymbol{U}_{\mathcal{B}}$ and $\boldsymbol{U}_{\mathcal{C}}$ are unitary quantum circuits. For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$, let $\mathcal{P}_{\mathcal{X},D_{\mathcal{X}}}$ be a mixture of projective measurements associated to a function $D_{\mathcal{X}}$ and a family $\mathcal{P}_{\mathcal{X}} = \{\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{ct})}\}_{\mathsf{coin},\mathsf{ct}}$ of projective measurements defined as follows:

- $D_{\mathcal{X}}$ takes $\mathsf{coin} \in \{0,1\}$ and a randomness r_{Enc} for Enc as input and outputs coin and $\mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{X},\mathsf{coin}}; r_{\mathsf{Enc}})$.
- $\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{ct})}$ is a projective measurement corresponding to the following procedure: On a quantum state $\widetilde{q}$ on register $\mathsf{R}_{\mathcal{X}}$, run $\mathsf{coin}' \leftarrow \widetilde{\mathcal{D}}_{\mathcal{X}}(\mathsf{ct})$ where $\widetilde{\mathcal{D}}_{\mathcal{X}} = (\widetilde{q}, \boldsymbol{U}_{\mathcal{X}})$. If $\mathsf{coin}' = \mathsf{coin}$, output 1, otherwise output 0.

Apply $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{B}},D_{\mathcal{B}},1/2+\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{C}},D_{\mathcal{C}},1/2+\gamma-\epsilon}$ on q where the first and second $\mathcal{ATI}$ act on registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$, respectively.If the both measurements result in outcome 1, send $\mathcal{D}'_{\mathcal{B}} = (q'[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}})$ to $\mathcal{B}$ and $\mathcal{D}'_{\mathcal{C}} = (q'[\mathsf{R}_{\mathcal{C}}], \boldsymbol{U}_{\mathcal{C}})$ to $\mathcal{C}$. Otherwise, send $\bot$ to $\mathcal{B}$ and $\mathcal{C}$.

$\mathsf{CPA}^+.\mathcal{B}$**:** If $\mathsf{CPA}^+.\mathcal{B}$ receives $\bot$ from $\mathsf{CPA}^+.\mathcal{A}$, it chooses $\mathsf{coin}'_{\mathcal{B}} \leftarrow \{0,1\}$ and outputs $\mathsf{coin}'_{\mathcal{B}}$. Otherwise, let $\mathcal{D}'_{\mathcal{B}} = (q'[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}})$ be a quantum decryptor received from $\mathsf{CPA}^+.\mathcal{A}$ and $\mathsf{ct}_{\mathcal{B}}$ be a ciphertext received from the challenger. $\mathsf{CPA}^+.\mathcal{B}$ runs $\mathcal{D}'_{\mathcal{B}}(\mathsf{ct}_{\mathcal{B}})$ to obtain $\mathsf{coin}'_{\mathcal{B}}$ and outputs $\mathsf{coin}'_{\mathcal{B}}$.

$\mathsf{CPA}^+.\mathcal{C}$**:** If $\mathsf{CPA}^+.\mathcal{C}$ receives $\bot$ from $\mathsf{CPA}^+.\mathcal{A}$, it chooses $\mathsf{coin}'_{\mathcal{C}} \leftarrow \{0,1\}$ and outputs $\mathsf{coin}'_{\mathcal{C}}$. Otherwise, let $\mathcal{D}'_{\mathcal{C}} = (q'[\mathsf{R}_{\mathcal{C}}], \boldsymbol{U}_{\mathcal{C}})$ be a quantum decryptor received from $\mathsf{CPA}^+.\mathcal{A}$ and $\mathsf{ct}_{\mathcal{C}}$ be a ciphertext received from the challenger. $\mathsf{CPA}^+.\mathcal{C}$ runs $\mathcal{D}'_{\mathcal{C}}(\mathsf{ct}_{\mathcal{C}})$ to obtain $\mathsf{coin}'_{\mathcal{C}}$ and outputs $\mathsf{coin}'_{\mathcal{C}}$.

In an execution of $\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{CPA}^+.\mathcal{A}_{\mathsf{sde}}}(\lambda)$, let E be the event that $\mathsf{CPA}^+.\mathcal{A}$ does not send $\bot$ to $\mathcal{B}$ and $\mathcal{C}$. We show the following lemmas.

Lemma 6.24. $\Pr[E]$ *is non-negligible.*

Proof of Lemma 6.24. $\Pr[E]$ can be written as

$$\mathrm{Tr}\Big[(\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{B}},D_{\mathcal{B}},1/2+\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{C}},D_{\mathcal{C}},1/2+\gamma-\epsilon})q\Big].$$

By the first item of Lemma 3.16,

$$\mathrm{Tr}\Big[(\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{B}},D_{\mathcal{B}},1/2+\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{C}},D_{\mathcal{C}},1/2+\gamma-\epsilon})q\Big] \geq \mathrm{Tr}\big[(\mathcal{TI}_{1/2+\gamma}(\mathcal{P}_{\mathcal{B},D_{\mathcal{B}}}) \otimes \mathcal{TI}_{1/2+\gamma}(\mathcal{P}_{\mathcal{C},D_{\mathcal{C}}}))q\big] - 2\delta.$$

By the assumption that $\mathsf{Strong}.\mathcal{A}$ breaks strong γ-anti-piracy security of SDE, $\mathrm{Tr}\big[(\mathcal{TI}_{1/2+\gamma}(\mathcal{P}_{\mathcal{B},D_{\mathcal{B}}}) \otimes \mathcal{TI}_{1/2+\gamma}(\mathcal{P}_{\mathcal{C},D_{\mathcal{C}}}))q\big]$ is non-negligible. Since $\delta = \mathsf{negl}(\lambda)$, $\Pr[E]$ is non-negligible. □

Lemma 6.25. *It holds that*

$$\Pr\big[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \mid E\big] \geq \frac{1}{2} + \frac{\gamma^2}{2} - 4\delta$$

Proof of Lemma 6.25. Suppose that E occurs. Define single-bit random variables $d_{\mathcal{B}}$ and $d_{\mathcal{C}}$ that take 1 if and only if $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$, respectively. In other words, $d_{\mathcal{B}} := \mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}} \oplus 1$ and $d_{\mathcal{C}} := \mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}} \oplus 1$. Suppose that we apply $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{B},D_{\mathcal{B}}})$ and $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{C},D_{\mathcal{C}}})$ to $q'[\mathsf{R}_{\mathcal{B}}]$ and $q'[\mathsf{R}_{\mathcal{C}}]$, respectively, and let p_1 and p_2 be the outcomes. Let P_{p_1,p_2} be the probability that the outcomes are (p_1,p_2). By the definition of projective implementations (Definition 3.5), the distribution of $(d_{\mathcal{B}},d_{\mathcal{C}})$ is identical to that of the following procedure: take (p_1,p_2) with probability P_{p_1,p_2} and then setting $d_{\mathcal{B}} := 1$ with probability p_1 and $d_{\mathcal{C}} := 1$ with probability p_2. In the following, whenever we take a sum over (p_1,p_2), it should be understood as a sum over all (p_1,p_2) such that $P_{p_1,p_2} \neq 0$.

Since E occurs when $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{B}},D_{\mathcal{B}},\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_{\mathcal{C}},D_{\mathcal{C}},\gamma-\epsilon}$ results in outcome 1 for both registers, conditioned that E occurs, the second item of Lemma 3.16 implies

$$\mathrm{Tr}\big[(\mathcal{TI}_{1/2+\gamma-3\epsilon}(\mathcal{P}_{\mathcal{B},D_{\mathcal{B}}}) \otimes \mathcal{TI}_{1/2+\gamma-3\epsilon}(\mathcal{P}_{\mathcal{C},D_{\mathcal{C}}}))q'\big] \geq 1 - 4\delta.$$

The above inequality together with $\gamma - 3\epsilon = \gamma/2$ implies

$$\sum_{\substack{p_1 \geq 1/2+\gamma/2 \\ p_2 \geq 1/2+\gamma/2}} P_{p_1,p_2} \geq 1 - 4\delta.$$

Then, we have

$$\begin{aligned}
&\Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \mid E\right] \\
=&\Pr[(d_{\mathcal{B}}, d_{\mathcal{C}}) = (1,1) \mid E] + \Pr[(d_{\mathcal{B}}, d_{\mathcal{C}}) = (0,0) \mid E] \\
=&\sum_{p_1,p_2} P_{p_1,p_2}(p_1p_2 + (1-p_1)(1-p_2)) \\
\geq&\sum_{\substack{p_1,p_2:\\ p_1\geq 1/2+\gamma/2\\ p_2\geq 1/2+\gamma/2}} P_{p_1,p_2}(p_1p_2 + (1-p_1)(1-p_2)) \\
\geq&\sum_{\substack{p_1,p_2:\\ p_1\geq 1/2+\gamma/2\\ p_2\geq 1/2+\gamma/2}} P_{p_1,p_2}(1/2 + \gamma^2/2) \\
\geq&1/2 + \gamma^2/2 - 4\delta
\end{aligned}$$

where the second inequality follows from the following claim and the final inequality follows from the above inequality.

Claim 6.26. For $\gamma > 0$ and $1/2 + \gamma/2 \leq p_1, p_2 \leq 1$, it holds that $p_1p_2 + (1-p_1)(1-p_2) \geq 1/2 + \gamma^2/2$.

Proof of Claim 6.26. Let $p_1 = 1/2 + \gamma_1$ and $p_2 = 1/2 + \gamma_2$ where $\gamma_1, \gamma_2 \geq \gamma/2$. Then we have $p_1p_2 + (1-p_1)(1-p_2) = (1/2+\gamma_1)(1/2+\gamma_2) + (1/2-\gamma_1)(1/2-\gamma_2) = 1/2 + 2\gamma_1\gamma_2 \geq 1/2 + \gamma^2/2$. □

This completes the proof of Lemma 6.25. □

Lemma 6.27. $\Pr[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \mid \neg E] = \frac{1}{2}$.

Proof of Lemma 6.27. This is obvious since $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$ are uniformly random independently of $\mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}}$ when E does not occur. □

By Lemmata 6.25 and 6.27,

$$\begin{aligned}
&\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{CPA}^+.\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \\
=&\Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}\right] \\
=&\Pr[E] \cdot \Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \mid E\right] + (1 - \Pr[E]) \cdot \Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}} \mid \neg E\right] \\
\geq&\Pr[E] \cdot \left(\frac{1}{2} + \frac{\gamma^2}{2} - 4\delta\right) + (1 - \Pr[E]) \cdot \frac{1}{2} \\
=&\frac{1}{2} + \Pr[E] \cdot \left(\frac{\gamma^2}{2} - 4\delta\right).
\end{aligned}$$

Since $\Pr[E]$ is non-negligible by Lemma 6.24, γ is inverse-polynomial, and $\delta = 2^{-\lambda}$, the above means that $\mathsf{CPA}^+.\mathcal{A}_{\mathsf{sde}}$ breaks CPA^+anti-piracy security of SDE, leading to contradiction. This completes the proof that CPA^+anti-piracy security implies strong anti-piracy.

Strong anti-piracy $\to$ CPA^+anti-piracy. Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{Dec})$ be an SDE scheme that satisfies strong anti-piracy security. Assume toward contradiction that SDE does not satisfy CPA^+anti-piracy security. Then, there are a polynomial p and a QPT adversary $\mathsf{CPA}^+.\mathcal{A}$ such that $\mathsf{Adv}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{CPA}^+.\mathcal{A}}(\lambda) \geq 1/p(\lambda)$ for infinitely many λ. We construct an adversary $\mathsf{Strong}.\mathcal{A}$ that breaks strong anti-piracy security of SDE as follows.

$\mathsf{Strong}.\mathcal{A}$**:** Given the security parameter 1^λ, public key pk, and quantum secret key sk, $\mathsf{Strong}.\mathcal{A}$ runs $\mathsf{CPA}^+.\mathcal{A}(1^\lambda, \mathsf{pk}, sk)$ to obtain challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and two (possibly entangled) states q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then $\mathsf{Strong}.\mathcal{A}$ chooses $b_{\mathcal{B}}, b_{\mathcal{C}} \leftarrow \{0,1\}$ and defines a quantum decryptor $\mathcal{D}^{b_{\mathcal{X}}}_{\mathcal{X}} = (q[\mathsf{R}_{\mathcal{X}}], \boldsymbol{U}^{b_{\mathcal{X}}}_{\mathcal{X}})$ for $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$ that works as follows:

$\mathcal{D}_{\mathcal{X}}^{b_{\mathcal{X}}}$**:** Given ct as input, run $\mathcal{X}(q[\mathsf{R}_{\mathcal{X}}], \mathsf{ct})$ to obtain coin' and output $\mathsf{coin}' \oplus b_{\mathcal{X}}$.

$\mathsf{Strong}.\mathcal{A}$ outputs challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ and quantum decryptors $\mathcal{D}_{\mathcal{B}}^{b_{\mathcal{B}}} = (q[\mathsf{R}_{\mathcal{B}}], \boldsymbol{U}_{\mathcal{B}}^{b_{\mathcal{B}}})$ and $\mathcal{D}_{\mathcal{C}}^{b_{\mathcal{C}}} = (q[\mathsf{R}_{\mathcal{C}}], \boldsymbol{U}_{\mathcal{C}}^{b_{\mathcal{C}}})$.

For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$, let $\mathcal{P}_{\mathcal{X},D_{\mathcal{X}}}$ be a mixture of projective measurements associated to a function $D_{\mathcal{X}}$ and a family $\mathcal{P}_{\mathcal{X}}^{b_{\mathcal{X}}} = \{\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{ct})}^{b_{\mathcal{X}}}\}_{\mathsf{coin},\mathsf{ct}}$ of projective measurements defined as follows:

- $D_{\mathcal{X}}$ takes $\mathsf{coin} \in \{0,1\}$ and a randomness r_{Enc} for Enc as input and outputs coin and $\mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{X},\mathsf{coin}}; r_{\mathsf{Enc}})$.
- $\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{ct})}^{b_{\mathcal{X}}}$ is a projective measurement corresponding to the following procedure: On a quantum state $\widetilde{q}$ on register $\mathsf{R}_{\mathcal{X}}$, run $\mathsf{coin}' \leftarrow \widetilde{\mathcal{D}}_{\mathcal{X}}^{b_{\mathcal{X}}}(\mathsf{ct})$ where $\widetilde{\mathcal{D}}_{\mathcal{X}}^{b_{\mathcal{X}}} = (\widetilde{q}, \boldsymbol{U}_{\mathcal{X}}^{b_{\mathcal{X}}})$. If $\mathsf{coin}' = \mathsf{coin}$, output 1, otherwise output 0.

For $(b_{\mathcal{B}}, b_{\mathcal{C}}) \in \{0,1\}^2$, let $P_{p_1,p_2}^{b_{\mathcal{B}},b_{\mathcal{C}}}$ be the probability that $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{B},D_{\mathcal{B}}}^{b_{\mathcal{B}}}) \otimes \mathsf{ProjImp}(\mathcal{P}_{\mathcal{C},D_{\mathcal{C}}}^{b_{\mathcal{C}}})$ on q results in outcome (p_1, p_2). Then the following claim is obvious from the definition.

Claim 6.28. For each (p_1, p_2), we have $P_{p_1,p_2}^{0,1} = P_{p_1,1-p_2}^{0,0}$, $P_{p_1,p_2}^{1,0} = P_{1-p_1,p_2}^{0,0}$, and $P_{p_1,p_2}^{1,1} = P_{1-p_1,1-p_2}^{0,0}$.

In the following, whenever we take a sum over (p_1, p_2), it should be understood as a sum over all (p_1, p_2) such that $P_{p_1,p_2}^{b_{\mathcal{B}},b_{\mathcal{C}}} \neq 0$ for some $(b_{\mathcal{B}}, b_{\mathcal{C}})$. We prove the following lemma.

Lemma 6.29. *For* $\gamma := 1/(2p(\lambda))$,

$$P_{\mathsf{good}} := \sum_{\substack{p_1,p_2:\\ |p_1-1/2|\geq\gamma\\ |p_2-1/2|\geq\gamma}} P_{p_1,p_2}^{0,0}$$

is non-negligible.

Assuming that Lemma 6.29 is correct, Then it is easy to show that $\mathsf{Strong}.\mathcal{A}$ breaks strong γ-anti-piracy security. Indeed, we have

$$\begin{aligned}\Pr\left[\mathsf{Exp}_{\mathsf{SDE},\mathsf{Strong}.\mathcal{A}}^{\mathsf{strong\text{-}anti\text{-}piracy}}(\lambda,\gamma(\lambda)) = 1\right] &= \frac{1}{4}\sum_{\substack{p_1,p_2:\\ p_1\geq 1/2+\gamma\\ p_2\geq 1/2+\gamma}} (P_{p_1,p_2}^{0,0} + P_{p_1,p_2}^{0,1} + P_{p_1,p_2}^{1,0} + P_{p_1,p_2}^{1,1})\\ &= \frac{1}{4}\sum_{\substack{p_1,p_2:\\ |p_1-1/2|\geq\gamma\\ |p_2-1/2|\geq\gamma}} P_{p_1,p_2}^{0,0}\end{aligned}$$

where the second equality follows from Claim 6.28. By Lemma 6.29, this is non-negligible. Thus, $\mathsf{Strong}.\mathcal{A}$ breaks strong γ-anti-piracy security, leading to contradiction.

We are left to prove Lemma 6.29.

Proof of Lemma 6.29. In an execution of $\mathsf{Exp}_{\mathsf{SDE},\mathsf{CPA}^+.\mathcal{A}}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}(\lambda)$, define single-bit random variables $d_{\mathcal{B}}$ and $d_{\mathcal{C}}$ that take 1 if and only if $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$, respectively. In other words, $d_{\mathcal{B}} := \mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{B}} \oplus 1$ and $d_{\mathcal{C}} := \mathsf{coin}'_{\mathcal{C}} \oplus \mathsf{coin}_{\mathcal{C}} \oplus 1$. By the definition of projective implementations (Definition 3.5), the distribution of $(d_{\mathcal{B}}, d_{\mathcal{C}})$ is identical to that of the following procedure: take (p_1, p_2) with probability $P_{p_1,p_2}^{0,0}$ and then setting $d_{\mathcal{B}} := 1$ with

probability p_1 and $d_C := 1$ with probability p_2. We have

$$\begin{aligned}
&\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{CPA}^+,\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right]\\
&=\Pr\left[\mathsf{coin}'_{\mathcal{B}}\oplus\mathsf{coin}'_{C}=\mathsf{coin}_{\mathcal{B}}\oplus\mathsf{coin}_{C}\right]\\
&=\Pr[d_{\mathcal{B}}=d_C]\\
&=\sum_{p_1,p_2}P^{0,0}_{p_1,p_2}\left(p_1p_2+(1-p_1)(1-p_2)\right)\\
&=\sum_{\substack{p_1,p_2:\\ |p_1-1/2|\geq\gamma\\ |p_2-1/2|\geq\gamma}}P^{0,0}_{p_1,p_2}\left(p_1p_2+(1-p_1)(1-p_2)\right)\\
&\quad+\sum_{\substack{p_1,p_2:\\ |p_1-1/2|<\gamma}}P^{0,0}_{p_1,p_2}\left(p_1p_2+(1-p_1)(1-p_2)\right)\\
&\quad+\sum_{\substack{p_1,p_2:\\ |p_1-1/2|\geq\gamma\\ |p_2-1/2|<\gamma}}P^{0,0}_{p_1,p_2}\left(p_1p_2+(1-p_1)(1-p_2)\right)\\
&\leq P_{\mathsf{good}}+(1/2+\gamma)
\end{aligned}$$

where the final inequality follows from the following claim:

Claim 6.30. For $\gamma>0$ and $0\leq p_1,p_2\leq 1$ such that either $|p_1-1/2|\leq\gamma$ or $|p_2-1/2|\leq\gamma$ holds, it holds that $p_1p_2+(1-p_1)(1-p_2)\leq 1/2+\gamma$.

Proof of Claim 6.30. We show the claim in the case of $|p_1-1/2|\leq\gamma$ since the other case can be shown similarly. Note that $p_1p_2+(1-p_1)(1-p_2)=(2p_2-1)p_1+1-p_2$. For each fixed p_2, if $p_2\geq 1/2$ (resp. $p_2<1/2$), it takes the maximum value when $p_1=1/2+\gamma$ (resp. $p_1=1/2-\gamma$). For $p_1=1/2\pm\gamma$, we have $p_1p_2+(1-p_1)(1-p_2)=(1/2\pm\gamma)p_2+(1/2\mp\gamma)(1-p_2)=1/2\pm(2p_2-1)\gamma\leq 1/2+\gamma$. □

By our assumption, $\Pr\left[\mathsf{Exp}^{\mathsf{cpaplus\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{CPA}^+,\mathcal{A}}(\lambda)=1\right]\geq 1/2+1/p(\lambda)$ for infinitely many λ. Thus, we have $P_{\mathsf{good}}\geq 1/p(\lambda)-\gamma=1/(2p(\lambda))$ for infinitely many λ. This means that P_{good} is non-negligible. This completes the proof of Lemma 6.29. □

This concludes the proof that strong anti-piracy security implies CPA$^+$anti-piracy security, thereby completing the proof of Theorem 6.23. □

7 Simultaneous Double-Sided One-Way to Hiding Lemma

In this section, we prove a novel variant of the one-way to hiding lemma, which we call *simultaneous double-sided one-way to hiding* lemma. Looking ahead, this is used in the construction of a $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy secure SDE scheme in the QROM in Section 8.

First, we review the regular one-way to hiding lemma.

Lemma 7.1 (One-Way to Hiding Lemma [AHU19]). *Let $H_0,H_1:X\to Y$ be any functions and q be any quantum state, where (H_0,H_1,q) may have arbitrary joint distribution. Let $S\subseteq X$ be the subset consisting of all $x\in X$ such that $H_0(x)\neq H_1(x)$. Let $\mathcal{A}$ be a quantum oracle algorithm that makes at most Q quantum queries. Let $\mathcal{A}'^{H_0}$ be an algorithm that on input q, choose $i\leftarrow[Q]$, runs $\mathcal{A}^{H_0}(q)$, measures $\mathcal{A}$'s i-th query, and outputs the measurement outcome. Then, we have*

$$\left|\Pr\left[\mathcal{A}^{H_0}(q)=1\right]-\Pr\left[\mathcal{A}^{H_1}(q)=1\right]\right|\leq 2Q\cdot\sqrt{\Pr\left[\mathcal{A}'^{H_0}(q)\in S\right]}\ .$$

Then we introduce the following variant.

Lemma 7.2 (Simultaneous Double-Sided One-Way to Hiding Lemma). *There is a QPT oracle algorithm $\mathcal{Ext}$ that satisfies the following. Let $H_0, H_1 : X \to Y$ be any functions and q be any quantum state over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$, where (H_0, H_1, q) may have arbitrary joint distribution. Let $S \subseteq X$ be the subset consisting of all $x \in X$ such that $H_0(x) \neq H_1(x)$. Let $\mathcal{B}$ and $\mathcal{C}$ be quantum oracle algorithms that take a state in $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$ as input, respectively, make at most Q quantum queries, and output a bit. Suppose that we have*

$$\Pr\left[\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin} : \begin{array}{l}\mathsf{coin} \leftarrow \{0,1\} \\ \mathsf{coin}'_{\mathcal{B}} \leftarrow \mathcal{B}^{H_{\mathsf{coin}}}(q[\mathsf{R}_{\mathcal{B}}]) \\ \mathsf{coin}'_{\mathcal{C}} \leftarrow \mathcal{C}^{H_{\mathsf{coin}}}(q[\mathsf{R}_{\mathcal{C}}])\end{array}\right] \geq \frac{1}{2} + \epsilon$$

for $\epsilon > 0$. Then it holds that

$$\Pr\left[x_{\mathcal{B}} \in S \wedge x_{\mathcal{C}} \in S : \begin{array}{l}x_{\mathcal{B}} \leftarrow \mathcal{Ext}^{H_0,H_1}(1^\lambda, \mathcal{B}, q[\mathsf{R}_{\mathcal{B}}]) \\ x_{\mathcal{C}} \leftarrow \mathcal{Ext}^{H_0,H_1}(1^\lambda, \mathcal{C}, q[\mathsf{R}_{\mathcal{C}}])\end{array}\right] \geq \frac{\epsilon^6}{2^{12}Q^4} - 2^{-\lambda}$$

where $\mathcal{B}$ and $\mathcal{C}$ in the input of $\mathcal{Ext}$ mean their descriptions.

Remark 7.3. Other forms of simultaneous one-way-to-hiding have been studied in the literature [BL20, CMP24]. These works, however, primarily focus on extractors that operate by running $\mathcal{B}$ or $\mathcal{C}$ using either oracle H_0 or H_1 and then measuring a randomly chosen query. Unfortunately, such approaches fail to achieve a desirable search-to-decision conversion. In fact, Majenz et al.[MST21] identify a limitation of simultaneous one-way-to-hiding with such simple extractors. We circumvent this limitation by designing an extractor that operates in a more general manner, utilizing both oracles H_0 and H_1. This approach is reminiscent of *double-sided* one-way-to-hiding [BHH+19], which inspired the naming of the above lemma.

The proof of Lemma 7.2 is partially very similar to the proof of [AKL23, Theorem 28], but we give a full proof for completeness.

Proof of Lemma 7.2. We can assume without loss of generality that H_0, H_1 are fixed functions and q is a fixed pure state rather than being randomly chosen from some distribution by convexity.[10] Moreover by the deffered measurement principle, we can assume without loss of generality that $\mathcal{B}$ and $\mathcal{C}$ do not perform any intermediate measurements and do not use ancilla qubits[11] by augmenting registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$ with a sufficient number of 0s.

For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$, let $\mathcal{P}_{\mathcal{X},D}$ be a mixture of projective measurements associated to a function D and a family $\mathcal{P}_{\mathcal{X}} = \{\mathcal{P}_{\mathcal{X},\mathsf{coin}}\}_{\mathsf{coin}\in\{0,1\}}$ of projective measurements defined as follows:

- D takes a bit $\mathsf{coin} \in \{0,1\}$ and outputs coin.
- $\mathcal{P}_{\mathcal{X},\mathsf{coin}}$ is a projective measurement corresponding to the following procedure: On a quantum state $q_{\mathcal{X}}$ on register $\mathsf{R}_{\mathcal{X}}$, run $\mathsf{coin}'_{\mathcal{X}} \leftarrow \mathcal{X}^{H_{\mathsf{coin}}}(q_{\mathcal{X}})$, and output 1 if $\mathsf{coin}'_{\mathcal{X}} = \mathsf{coin}$ and output 0 otherwise.

Then we construct $\mathcal{Ext}$ as follows.

$\mathcal{Ext}^{H_0,H_1}(1^\lambda, \mathcal{X}, q[\mathsf{R}_{\mathcal{X}}])$**:** Let $\delta := 2^{-(2\lambda+6)}$. $\mathcal{Ext}$ applies $\mathcal{API}^{\epsilon/12,\delta}_{\mathcal{P}_{\mathcal{X},D}}$ on $q[\mathsf{R}_{\mathcal{X}}]$. Let $\tilde{p}$ be the outcome. If $|\tilde{p} - 1/2| \leq 5\epsilon/12$, $\mathcal{Ext}$ aborts. Otherwise, $\mathcal{Ext}$ runs ${\mathcal{X}'}^{H_0}$ on the leftover state $q'_{\mathcal{X}}$ on $\mathsf{R}_{\mathcal{X}}$ where ${\mathcal{X}'}^{H_0}$ is defined below:

> ${\mathcal{X}'}^{H_0}$**:** Given a state $q'_{\mathcal{X}}$, choose $i \leftarrow [Q]$, run $\mathcal{X}^{H_0}$ on input $q'_{\mathcal{X}}$, measure i-th query of $\mathcal{X}$, and outputs a measurement outcome x.
>
> $\mathcal{Ext}$ outputs the output x of ${\mathcal{X}'}^{H_0}$.

Suppose that we apply $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{B},D})$ and $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{C},D})$ to $q[\mathsf{R}_{\mathcal{B}}]$ and $q[\mathsf{R}_{\mathcal{C}}]$, respectively, and let p_1 and p_2 be the outcomes. Let P_{p_1,p_2} be the probability that the outcomes are (p_1, p_2). In the following, whenever we take a sum over (p_1, p_2), it should be understood as a sum over all (p_1, p_2) such that $P_{p_1,p_2} \neq 0$. We prove the following lemma.

[10] This assumption is used in the proof of Lemma 7.4.

[11] This assumption is used to ensure that $\mathcal{P}_{\mathcal{X},\mathsf{coin}}$ defined below can be regarded as a projective measurement.

Lemma 7.4. *It holds that*

$$\sum_{\substack{p_1,p_2:\\ |p_1-1/2|>\epsilon/2,\\ |p_2-1/2|>\epsilon/2}} P_{p_1,p_2} \geq \frac{\epsilon^2}{16}.$$

Proof of Lemma 7.4. Recall that we assume that H_0, H_1 are fixed functions and q is a fixed pure state. Thus, we can write $q = |\psi\rangle\langle\psi|$ using a pure state $|\psi\rangle$.

For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$ and $\mathsf{coin} \in \{0,1\}$, let $\boldsymbol{P}_{\mathcal{X},\mathsf{coin}}$ be the projection corresponding to post-selecting the outcome 1 for $\mathcal{P}_{\mathcal{X},\mathsf{coin}}$, and let $\boldsymbol{P}_{\mathcal{X},D} := (\boldsymbol{P}_{\mathcal{X},0} + \boldsymbol{P}_{\mathcal{X},1})/2$. Let $\{|\beta_i\rangle\}_i$ and $\{|\gamma_j\rangle\}_j$ be the normalized eigenbases of $\boldsymbol{P}_{\mathcal{B},D}$ and $\boldsymbol{P}_{\mathcal{C},D}$, where $|\beta_i\rangle$ and $|\gamma_j\rangle$ have eigenvalues $p_{1,i}$ and $p_{2,j}$, respectively. Then we can express $|\psi\rangle$ as follows:

$$|\psi\rangle = \sum_{i,j} c_{i,j} |\beta_i\rangle \otimes |\gamma_j\rangle.$$

Define projective measurements $\mathcal{E}_{\mathcal{B}} = \{\Pi_{\mathcal{B},p_1}\}_{p_1}$ and $\mathcal{E}_{\mathcal{C}} = \{\Pi_{\mathcal{C},p_2}\}_{p_2}$ where $\Pi_{\mathcal{B},p_1} := \sum_{i:p_{1,i}=p_1} |\beta_i\rangle\langle\beta_i|$ and $\Pi_{\mathcal{C},p_2} := \sum_{j:p_{2,j}=p_2} |\gamma_j\rangle\langle\gamma_j|$ are labeled by p_1 and p_2, respectively. Then it is easy to see that $\mathcal{E}_{\mathcal{B}}$ and $\mathcal{E}_{\mathcal{C}}$ are projective implementations of $\mathcal{P}_{\mathcal{B},D}$ and $\mathcal{P}_{\mathcal{C},D}$, respectively. Thus, we have $\sum_{\substack{i:p_{1,i}=p_1\\ j:p_{2,j}=p_2}} |c_{i,j}|^2 = P_{p_1,p_2}$. Decompose $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle + |\psi_3\rangle$ where $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$ are defined as follows:

$$\begin{aligned}
|\psi_1\rangle &:= \sum_{\substack{i,j:\\ |p_{1,i}-1/2|\leq\epsilon/2}} c_{i,j} |\beta_i\rangle \otimes |\gamma_j\rangle, \\
|\psi_2\rangle &:= \sum_{\substack{i,j:\\ |p_{1,i}-1/2|>\epsilon/2\\ |p_{2,j}-1/2|\leq\epsilon/2}} c_{i,j} |\beta_i\rangle \otimes |\gamma_j\rangle, \\
|\psi_3\rangle &:= \sum_{\substack{i,j:\\ |p_{1,i}-1/2|>\epsilon/2\\ |p_{2,j}-1/2|>\epsilon/2}} c_{i,j} |\beta_i\rangle \otimes |\gamma_j\rangle.
\end{aligned}$$

By $\sum_{\substack{i:p_{1,i}=p_1\\ j:p_{2,j}=p_2}} |c_{i,j}|^2 = P_{p_1,p_2}$, we have

$$\sum_{\substack{p_1,p_2:\\ |p_1-1/2|>\epsilon/2,\\ |p_2-1/2|>\epsilon/2}} P_{p_1,p_2} = \| |\psi_3\rangle \|^2.$$

Let $\boldsymbol{P} := \frac{\boldsymbol{P}_{\mathcal{B},0}\otimes\boldsymbol{P}_{\mathcal{C},0} + \boldsymbol{P}_{\mathcal{B},1}\otimes\boldsymbol{P}_{\mathcal{C},1}}{2}$. We show the following claim:

Claim 7.5. It holds that

$$(\langle\psi_1| + \langle\psi_2|)\boldsymbol{P}(|\psi_1\rangle + |\psi_2\rangle) = \langle\psi_1|\boldsymbol{P}|\psi_1\rangle + \langle\psi_2|\boldsymbol{P}|\psi_2\rangle.$$

Proof of Claim 7.5. For any i, i' such that $|p_{1,i} - 1/2| \leq \epsilon/2$ and $|p_{1,i'} - 1/2| > \epsilon/2$, we have $p_{1,i} \neq p_{1,i'}$ and $p_{1,i} + p_{1,i'} \neq 1$. Thus, by Lemma 3.4, we have $\langle\beta_i|\boldsymbol{P}_{\mathcal{B},0}|\beta_{i'}\rangle = \langle\beta_i|\boldsymbol{P}_{\mathcal{B},1}|\beta_{i'}\rangle = 0$. Using this, we have

$$\langle\psi_1|(\boldsymbol{P}_{\mathcal{B},0}\otimes\boldsymbol{P}_{\mathcal{C},0})|\psi_2\rangle = \sum_{\substack{i,j:\\ |p_{1,i}-1/2|\leq\epsilon/2}} \sum_{\substack{i',j':\\ |p_{1,i'}-1/2|>\epsilon/2\\ |p_{2,j'}-1/2|\leq\epsilon/2}} c^*_{i,j}c_{i',j'} \langle\beta_i|\boldsymbol{P}_{\mathcal{B},0}|\beta_{i'}\rangle \langle\gamma_j|\boldsymbol{P}_{\mathcal{C},0}\left|\gamma_{j'}\right\rangle = 0.$$

Similarly, we have

$$\langle\psi_1|\left(\boldsymbol{P}_{\mathcal{B},1}\otimes\boldsymbol{P}_{C,1}\right)|\psi_2\rangle=0.$$

Combining the above, we have

$$\langle\psi_1|\,\boldsymbol{P}\,|\psi_2\rangle=0.$$

This immediately implies Claim 7.5. □

By the assumption of Lemma 7.2, we have

$$\begin{aligned}
\frac{1}{2}+\epsilon &\le \langle\psi|\,\boldsymbol{P}\,|\psi\rangle\\
&= (\langle\psi_1|+\langle\psi_2|)\boldsymbol{P}(|\psi_1\rangle+|\psi_2\rangle)+(\langle\psi_1|+\langle\psi_2|+\langle\psi_3|)\boldsymbol{P}\,|\psi_3\rangle+\langle\psi_3|\,\boldsymbol{P}(|\psi_1\rangle+|\psi_2\rangle)\\
&\le (\langle\psi_1|+\langle\psi_2|)\boldsymbol{P}(|\psi_1\rangle+|\psi_2\rangle)+2\|\,|\psi_3\rangle\,\|\\
&= \langle\psi_1|\,\boldsymbol{P}\,|\psi_1\rangle+\langle\psi_2|\,\boldsymbol{P}\,|\psi_2\rangle+2\|\,|\psi_3\rangle\,\|\\
&\le \langle\psi_1|\left(\frac{\boldsymbol{P}_{\mathcal{B},0}\otimes\boldsymbol{I}+\boldsymbol{P}_{\mathcal{B},1}\otimes\boldsymbol{I}}{2}\right)|\psi_1\rangle+\langle\psi_2|\left(\frac{\boldsymbol{I}\otimes\boldsymbol{P}_{C,0}+\boldsymbol{I}\otimes\boldsymbol{P}_{C,1}}{2}\right)|\psi_2\rangle+2\|\,|\psi_3\rangle\,\|\\
&\le \frac{1}{2}+\frac{\epsilon}{2}+2\|\,|\psi_3\rangle\,\|.
\end{aligned}$$

where we used Claim 7.5 in the fourth line. From this, we obtain $\|\,|\psi_3\rangle\,\|^2\ge\epsilon^2/16$. This completes the proof of Lemma 7.4.

□

Let E be the event that neither $\mathcal{E}\mathcal{X}\mathcal{t}^{H_0,H_1}(1^\lambda,\mathcal{B},q[\mathsf{R}_{\mathcal{B}}])$ nor $\mathcal{E}\mathcal{X}\mathcal{t}^{H_0,H_1}(1^\lambda,C,q[\mathsf{R}_C])$ aborts. The following lemma easily follows from Lemma 7.4.

Lemma 7.6. *It holds that*

$$\Pr[E]\ge\frac{\epsilon^2}{16}-2\delta.$$

Proof of Lemma 7.6. Suppose that we apply $\mathcal{APPI}^{\epsilon/12,\delta}_{\mathcal{P}_{\mathcal{B}},D}$ and $\mathcal{APPI}^{\epsilon/12,\delta}_{\mathcal{P}_C,D}$ to $q[\mathsf{R}_{\mathcal{B}}]$ and $q[\mathsf{R}_C]$, respectively, and let $\tilde{p}_1$ and $\tilde{p}_2$ be the outcomes. By Lemma 7.4 and the first item of Lemma 3.12, we have

$$\Pr\left[\left|\tilde{p}_1-\frac{1}{2}\right|>\frac{5\epsilon}{12}\wedge\left|\tilde{p}_2-\frac{1}{2}\right|>\frac{5\epsilon}{12}\right]\ge\frac{\epsilon^2}{16}-2\delta.$$

This immediately implies Lemma 7.6. □

Conditioned that E occurs, let q' be the leftover state on registers $\mathsf{R}_{\mathcal{B}}$ and R_C after applying the APIs on both registers. We prove the following lemma.

Lemma 7.7. *Conditioned that E occurs, we have*

$$\Pr\left[x_{\mathcal{B}}\in S\wedge x_C\in S:\ \begin{array}{l}x_{\mathcal{B}}\leftarrow\mathcal{E}\mathcal{X}\mathcal{t}^{H_0,H_1}(1^\lambda,\mathcal{B},q'[\mathsf{R}_{\mathcal{B}}])\\ x_C\leftarrow\mathcal{E}\mathcal{X}\mathcal{t}^{H_0,H_1}(1^\lambda,C,q'[\mathsf{R}_C])\end{array}\right]\ge\left(\frac{\epsilon}{4Q}\right)^4-4\delta^{1/2}$$

Proof of Lemma 7.7. When E occurs, we have $|\tilde{p}_1-1/2|>5\epsilon/12$ and $|\tilde{p}_2-1/2|>5\epsilon/12$. In particular, there are the following four possible cases:

1. $\tilde{p}_1>1/2+5\epsilon/12$ and $\tilde{p}_2>1/2+5\epsilon/12$,
2. $\tilde{p}_1>1/2+5\epsilon/12$ and $\tilde{p}_2<1/2-5\epsilon/12$,

3. $\tilde{p}_1 < 1/2 - 5\epsilon/12$ and $\tilde{p}_2 > 1/2 + 5\epsilon/12$,
4. $\tilde{p}_1 < 1/2 - 5\epsilon/12$ and $\tilde{p}_2 < 1/2 - 5\epsilon/12$.

Since the proofs for each case are similar, we focus on the first case.

Let p'_1 and p'_2 be random variables according to the distributions of the outcomes of $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{B},D})q'[\mathsf{R}_{\mathcal{B}}]$ and $\mathsf{ProjImp}(\mathcal{P}_{C,D})q'[\mathsf{R}_C]$, respectively. Similarly, $\tilde{p}'_1$ and $\tilde{p}'_2$ be random variables according to the distributions of the outcomes of $\mathcal{API}^{\epsilon/12,\delta}_{\mathcal{P}_{\mathcal{B}},D}(q'[\mathsf{R}_{\mathcal{B}}])$ and $\mathcal{API}^{\epsilon/12,\delta}_{\mathcal{P}_{C},D}(q'[\mathsf{R}_C])$, respectively.

By the first item of Lemma 3.12, we have

$$\Pr\left[\left|\tilde{p}'_1 - p'_1\right| \leq \frac{\epsilon}{12} \wedge \left|\tilde{p}'_2 - p'_2\right| \leq \frac{\epsilon}{12}\right] \geq 1 - 2\delta.$$

By the second item of Lemma 3.12, we have

$$\Pr\left[\left|\tilde{p}'_1 - \tilde{p}_1\right| \leq \frac{\epsilon}{12} \wedge \left|\tilde{p}'_2 - \tilde{p}_2\right| \leq \frac{\epsilon}{12}\right] \geq 1 - 2\delta.$$

Combining the above, we have

$$\Pr\left[\left|p'_1 - \tilde{p}_1\right| \leq \frac{\epsilon}{6} \wedge \left|p'_2 - \tilde{p}_2\right| \leq \frac{\epsilon}{6}\right] \geq 1 - 4\delta.$$

Since we assume $\tilde{p}_1 > 1/2 + 5\epsilon/12$ and $\tilde{p}_2 > 1/2 + 5\epsilon/12$, we have

$$\Pr\left[p'_1 > \frac{1}{2} + \frac{\epsilon}{4} \wedge p'_2 > \frac{1}{2} + \frac{\epsilon}{4}\right] \geq 1 - 4\delta.$$

By the gentle measurement lemma (Lemma 3.2), this implies that q' is within a trace distance of $4\delta^{1/2}$ from a state such that both $\mathsf{ProjImp}(\mathcal{P}_{\mathcal{B},D})$ and $\mathsf{ProjImp}(\mathcal{P}_{C,D})$ always result in values larger than $1/2 + \epsilon/4$. Therefore, it suffices to prove

$$\Pr\left[x_{\mathcal{B}} \in S \wedge x_C \in S : \begin{array}{l} x_{\mathcal{B}} \leftarrow \mathcal{B}'^{H_0}(q'[\mathsf{R}_{\mathcal{B}}]) \\ x_C \leftarrow C'^{H_0}(q'[\mathsf{R}_C]) \end{array}\right] \geq \left(\frac{\epsilon}{4Q}\right)^4$$

assuming that $\Pr\left[p'_1 > 1/2 + \epsilon/4 \wedge p'_2 > 1/2 + \epsilon/4\right] = 1$.

For a state q' such that $\Pr\left[p'_1 > 1/2 + \epsilon/4 \wedge p'_2 > 1/2 + \epsilon/4\right] = 1$, suppose that we apply an arbitrary measurement on $\mathsf{R}_{\mathcal{B}}$. Conditioned on any outcome of the measurement, $\mathsf{ProjImp}(\mathcal{P}_{C,D})$ on R_C still results in an outcome larger than $1/2 + \epsilon/4$ with probability 1. Based on this observation, it suffices to prove the following:

- If $\Pr\left[p'_1 > 1/2 + \epsilon/4\right] = 1$, we have

$$\Pr\left[\mathcal{B}'^{H_0}(q'[\mathsf{R}_{\mathcal{B}}]) \in S\right] \geq \left(\frac{\epsilon}{4Q}\right)^2.$$

- If $\Pr\left[p'_2 > 1/2 + \epsilon/4\right] = 1$, we have

$$\Pr\left[C'^{H_0}(q'[\mathsf{R}_C]) \in S\right] \geq \left(\frac{\epsilon}{4Q}\right)^2.$$

We only prove the former since the proof of the latter is similar. Since $\Pr\left[p'_1 > 1/2 + \epsilon/4\right] = 1$, we have

$$\Pr\left[\mathcal{B}^{H_{\mathsf{coin}}}(q'[\mathsf{R}_{\mathcal{B}}]) = \mathsf{coin} \mid \mathsf{coin} \leftarrow \{0,1\}\right] > \frac{1}{2} + \frac{\epsilon}{4}.$$

In particular, we have

$$\left|\Pr\left[\mathcal{B}^{H_0}(q'[\mathsf{R}_{\mathcal{B}}]) = 1\right] - \Pr\left[\mathcal{B}^{H_1}(q'[\mathsf{R}_{\mathcal{B}}]) = 1\right]\right| > \frac{\epsilon}{2}.$$

Thus, by Lemma 7.1, we have

$$\Pr\left[\mathcal{B}'^{H_0}(q'[\mathsf{R}_{\mathcal{B}}]) \in S\right] \geq \left(\frac{\epsilon}{4Q}\right)^2.$$

This completes the proof of Lemma 7.7. □

We are now ready to finish the proof of Lemma 7.2. We have

$$\begin{aligned}
&\Pr\left[x_{\mathcal{B}} \in S \wedge x_C \in S : \begin{array}{l} x_{\mathcal{B}} \leftarrow \mathcal{E}\mathcal{X}t^{H_0,H_1}(1^\lambda, \mathcal{B}, q[\mathsf{R}_{\mathcal{B}}]) \\ x_C \leftarrow \mathcal{E}\mathcal{X}t^{H_0,H_1}(1^\lambda, C, q[\mathsf{R}_C]) \end{array}\right] \\
=&\Pr[E] \cdot \Pr\left[x_{\mathcal{B}} \in S \wedge x_C \in S : \begin{array}{l} x_{\mathcal{B}} \leftarrow \mathcal{E}\mathcal{X}t^{H_0,H_1}(1^\lambda, \mathcal{B}, q'[\mathsf{R}_{\mathcal{B}}]) \\ x_C \leftarrow \mathcal{E}\mathcal{X}t^{H_0,H_1}(1^\lambda, C, q'[\mathsf{R}_C]) \end{array}\right] \\
\geq&\left(\frac{\epsilon^2}{16} - 2\delta\right) \cdot \left(\left(\frac{\epsilon}{4Q}\right)^4 - 4\delta^{1/2}\right) \\
\geq&\frac{\epsilon^6}{2^{12}Q^4} - (2\delta + 4\delta^{1/2})
\end{aligned}$$

where the first inequality follows from Lemmata 7.6 and 7.7. Since $2\delta + 4\delta^{1/2} \leq 8\delta^{1/2} = 2^{-\lambda}$, this completes the proof of Lemma 7.2. □

8 Achieving $\mathcal{D}_{\mathsf{identical}}$-CPA Anti-Piracy Security in the QROM

In Section 6, we demonstrate that CPA$^+$anti-piracy security implies most of the existing definitions, with the exception of $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security. To address this gap, we present a generic compiler that converts a $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy secure scheme into $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy secure scheme in the QROM. Notably CPA$^+$anti-piracy security implies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy (Theorem 6.20), which means that the conversion can also be applied starting from a CPA$^+$anti-piracy secure scheme constructed in Section 5.2.

We prove the following theorem:

Theorem 8.1. *If there exists an SDE scheme that satisfies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security and has message space $\mathcal{M}$ such that $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$, then there exists an SDE scheme that satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the QROM.*

Combining the above with Theorems 5.1 and 6.20 we obtain the following corollary.

Corollary 8.2. *If there exist a secure IO for polynomial size classical circuits and OWFs, then there exists a SDE scheme with $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the QROM.*

The proof of Theorem 8.1 is structured into the following three steps:

1. We introduce an *augmented* $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security notion, where the security requirement is extended to hold even when an equality-checking oracle for the challenge message is available. We demonstrate that $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security implies augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security.
2. Next, we define a variant of augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security, termed augmented *identical-challenge* search anti-piracy security, where the same challenge ciphertext is used for both parties. We prove that augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security implies augmented identical-challenge search anti-piracy security.
3. Finally, we construct a transformation that converts any SDE scheme satisfying augmented identical-challenge search anti-piracy security into an SDE scheme that satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the QROM. In this step, we rely on the simultaneous double-sided one-way to hiding lemma (Lemma 7.2).

The idea of going through *augmented* security notions is inspired by [AKL23].

8.1 Augmented $\mathsf{Id}_{\mathcal{U}}$-Search Anti-Piracy Security

We introduce augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security and construct a scheme that satisfies it based on a $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA secure scheme.

The definition of augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security is similar to that of $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security except that the adversary is given quantum oracle access to an equality-checking oracle for the challenge message. Formally, it is defined as follows where we highlight the difference from $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security in **red bold text.**

Definition 8.3 (Augmented $\mathsf{Id}_{\mathcal{U}}$-Search Anti-Piracy Security). *Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M}$. We consider the augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy game $\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ between the challenger and an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ below.*

1. *The challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and $sk \leftarrow \mathcal{KG}(\mathsf{sk})$ and chooses $m \leftarrow \mathcal{M}$.* **Throughout the experiment, the adversary is given quantum oracle access to an equality-checking oracle O_m for m, i.e., $O_m(m') = 1$ if $m' = m$ and $O_m(m') = 0$ otherwise.**
2. *The challenger sends $(1^\lambda, \mathsf{pk}, sk)$ to $\mathcal{A}$*
3. *$\mathcal{A}$ creates a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. Then, $\mathcal{A}$ sends register $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}$ and register $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{C}$.*
4. *The challenger generates $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$ and $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$, and sends $\mathsf{ct}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.*
5. *$\mathcal{B}$ and $\mathcal{C}$ respectively output $m'_{\mathcal{B}}$ and $m'_{\mathcal{C}}$. The challenger outputs 1 if $m'_{\mathcal{B}} = m'_{\mathcal{C}} = m$ and otherwise outputs 0.*

We say that SDE is augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy secure if for any QPT adversary $\mathcal{A}_{\mathsf{sde}}$, it holds that

$$\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda).$$

We show the following lemma.

Lemma 8.4. *If an SDE scheme with message space $\mathcal{M}$ satisfies $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security and $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$, then the scheme also satisfies augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security.*

Proof. The proof is very similar to that of Theorem 6.22.

Let SDE be a $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy secure SDE scheme with message space $\mathcal{M}$. Assume toward contradiction that there is an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ that breaks augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security of SDE. Let $Q = \mathrm{poly}(\lambda)$ be the number of queries to the equality-check oracle O_m by $\mathcal{A}_{\mathsf{sde}}$. Then we construct a QPT adversary $\tilde{\mathcal{A}}_{\mathsf{sde}} = (\tilde{\mathcal{A}}, \tilde{\mathcal{B}}, \tilde{\mathcal{C}})$ that breaks $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security of SDE as follows.

$\tilde{\mathcal{A}}$: Given the security parameter 1^λ, public key pk, and quantum secret key sk, $\tilde{\mathcal{A}}$ generates $m \leftarrow \mathcal{M}$ and runs $\mathcal{A}^{O_m}$ on input $(1^\lambda, \mathsf{pk}, sk)$ to obtain a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$. $\tilde{\mathcal{A}}$ sends $(0^{|m|}, m, 0^{|m|}, m)$ to the challenger, register $\mathsf{R}_{\mathcal{B}}$ and m to $\tilde{\mathcal{B}}$, and register $\mathsf{R}_{\mathcal{C}}$ and m to $\tilde{\mathcal{C}}$.

$\tilde{\mathcal{B}}$: Given register $\mathsf{R}_{\mathcal{B}}$, m, and a ciphertext $\mathsf{ct}_{\mathcal{B}}$, run $\mathcal{B}^{O_m}$ on input $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{ct}_{\mathcal{B}}$ to obtain $m'_{\mathcal{B}}$. $\tilde{\mathcal{B}}$ outputs 1 if $m'_{\mathcal{B}} = m$ and outputs 0 otherwise.

$\tilde{\mathcal{C}}$: Given register $\mathsf{R}_{\mathcal{C}}$, m, and a ciphertext $\mathsf{ct}_{\mathcal{C}}$, run $\mathcal{C}^{O_m}$ on input $\mathsf{R}_{\mathcal{C}}$ and $\mathsf{ct}_{\mathcal{C}}$ to obtain $m'_{\mathcal{C}}$. $\tilde{\mathcal{C}}$ outputs 1 if $m'_{\mathcal{C}} = m$ and outputs 0 otherwise.

In an execution of $\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda)$, let $\mathsf{coin}_{\tilde{\mathcal{B}}}$ and $\mathsf{coin}_{\tilde{\mathcal{C}}}$ be the challenge bits chosen by the challenger for $\tilde{\mathcal{B}}$ and $\tilde{\mathcal{C}}$, respectively. Note that they are uniformly chosen under the constraint that $\mathsf{coin}_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}$. Clearly, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}\right].$$

Let E_b be the event that $\mathsf{coin}_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} = b$ for $b \in \{0,1\}$. Note that $\Pr[E_0] = \Pr[E_1] = 1/2$. Conditioned on E_1, $\tilde{\mathcal{A}}_{\mathsf{sde}}$ perfectly simulates for $\mathcal{A}_{\mathsf{sde}}$. Thus, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] = \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} \mid E_1\right].$$

On the other hand, when E_0 occurs, no information of m is given to $\mathcal{B}$ and $\mathcal{C}$ except for those obtained through oracle access to O_m. Since m is uniformly random, by the well-known bound for unstructured search [BBBV97], when E_0 occurs, the probability that either $\mathcal{B}^{O(m)}$ or $\mathcal{C}^{O(m)}$ outputs m is $O(Q^2/|\mathcal{M}|) = \mathsf{negl}(\lambda)$.[12] This implies that $\tilde{\mathcal{B}}$ (resp. $\tilde{\mathcal{C}}$) outputs 0 except for a negligible probability. Thus, we have

$$\Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}} \mid E_0\right] \geq 1 - \mathsf{negl}(\lambda).$$

Combining the above, we have

$$\begin{aligned}\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] &= \Pr\left[\mathsf{coin}'_{\tilde{\mathcal{B}}} = \mathsf{coin}_{\tilde{\mathcal{B}}} \wedge \mathsf{coin}'_{\tilde{\mathcal{C}}} = \mathsf{coin}_{\tilde{\mathcal{C}}}\right] \\ &= \frac{1}{2}\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] + \frac{1}{2}(1 - \mathsf{negl}(\lambda)).\end{aligned}$$

By the assumption that $\mathcal{A}_{\mathsf{sde}}$ breaks augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security, $\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right]$ is non-negligible. Thus, $\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\tilde{\mathcal{A}}_{\mathsf{sde}}}(\lambda) = 1\right] - 1/2$ is non-negligible, which contradicts the assumed $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security. This completes the proof of Lemma 8.4. □

8.2 Augmented Identical-Challenge Search Anti-Piracy Security

We introduce augmented identical-challenge search anti-piracy security and show that it is implied by augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security.

The definition of augmented identical-challenge search anti-piracy security is similar to that of augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security except that the same challenge ciphertext is given to both parties $\mathcal{B}$ and $\mathcal{C}$. Formally, it is defined as follows where we highlight the difference from augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security in **red bold text**.

Definition 8.5 (Augmented Identical-Challenge Search Anti-Piracy Security). *Let* $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ *be an SDE scheme with message space* $\mathcal{M}$. *We consider the augmented identical-challenge search anti-piracy game* $\mathsf{Exp}^{\mathsf{augiden\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ *between the challenger and an adversary* $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ *below.*

1. *The challenger generates* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and* $sk \leftarrow \mathcal{KG}(\mathsf{sk})$ *and chooses* $m \leftarrow \mathcal{M}$. *Throughout the experiment, the adversary is given quantum oracle access to an equality-checking oracle* O_m *for* m, *i.e.,* $O(m') = 1$ *if* $m' = m$ *and* $O(m') = 0$ *otherwise.*
2. *The challenger sends* $(1^\lambda, \mathsf{pk}, sk)$ *to* $\mathcal{A}$
3. $\mathcal{A}$ *creates a bipartite state* q *over registers* $\mathsf{R}_{\mathcal{B}}$ *and* $\mathsf{R}_{\mathcal{C}}$. *Then,* $\mathcal{A}$ *sends register* $\mathsf{R}_{\mathcal{B}}$ *to* $\mathcal{B}$ *and register* $\mathsf{R}_{\mathcal{C}}$ *to* $\mathcal{C}$.
4. **The challenger generates** $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$ **and sends** ct **to both** $\mathcal{B}$ **and** $\mathcal{C}$**.**
5. $\mathcal{B}$ *and* $\mathcal{C}$ *respectively output* $m'_{\mathcal{B}}$ *and* $m'_{\mathcal{C}}$. *The challenger outputs* 1 *if* $m'_{\mathcal{B}} = m'_{\mathcal{C}} = m$ *and otherwise outputs* 0.

We say that SDE *is augmented identical-challenge search anti-piracy secure if for any QPT adversary* $\mathcal{A}_{\mathsf{sde}}$, *it holds that*

$$\Pr\left[\mathsf{Exp}^{\mathsf{augiden\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq \mathsf{negl}(\lambda).$$

We show the following lemma.

[12] One can also see this from the one-way to hiding lemma (Lemma 7.1).

Lemma 8.6. *If an SDE scheme satisfies augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security, then it also satisfies augmented identical-challenge search anti-piracy security*

To prove Lemma 8.6, we borrow the following lemma shown in [AKL23].

Lemma 8.7 ([AKL23, Lemma 18]). *Let q be a bipartite state over registers R_1 and R_2. Let $\boldsymbol{P}_1 = \{\boldsymbol{P}_{1,r}\}_{r\in\mathcal{R}}$ and $\boldsymbol{P}_2 = \{\boldsymbol{P}_{2,r}\}_{r\in\mathcal{R}}$ be families of projections indexed by an element r of a finite set $\mathcal{R}$ on registers R_1 and R_2, respectively. Let $\tilde{D}$ be a distribution over $\mathcal{R}\times\mathcal{R}$ such that the marginal distributions of the first and second components are an identical distribution D. Define*

$$P_{cor} := \mathop{\mathbb{E}}_{(r_1,r_2)\leftarrow\tilde{D}} \mathrm{Tr}\left[(\boldsymbol{P}_{1,r_1}\otimes\boldsymbol{P}_{2,r_2})q\right], \quad P_{ind} := \mathop{\mathbb{E}}_{r_1\leftarrow D, r_2\leftarrow D} \mathrm{Tr}\left[(\boldsymbol{P}_{1,r_1}\otimes\boldsymbol{P}_{2,r_2})q\right].$$

Then we have

$$P_{cor} \le 6P_{ind}^{1/3}.$$

Then we prove Lemma 8.6.

Proof of Lemma 8.6. Let SDE be a $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy secure SDE scheme. Assume toward contradiction that there is an adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A},\mathcal{B},\mathcal{C})$ that breaks augmented identical-challenge search anti-piracy security of SDE. Then we show that the same adversary $\mathcal{A}_{\mathsf{sde}}$ breaks $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security of SDE.

For each public key pk, message m, and $\mathcal{X}\in\{\mathcal{B},\mathcal{C}\}$, let $\mathcal{P}_{\mathcal{X}}^{\mathsf{pk},m} = \{\mathcal{P}_{\mathcal{X},\mathsf{ct}}^{\mathsf{pk},m}\}_{\mathsf{ct}}$ be the following family of projective measurements indexed by a ciphertext ct of SDE:

$\mathcal{P}_{\mathcal{X},\mathsf{ct}}^{\mathsf{pk},m}$**:** This is a projection corresponding to the following procedure on a state on register $\mathsf{R}_{\mathcal{X}}$: Run $\mathcal{X}^{O(m)}$ on input $\mathsf{R}_{\mathcal{X}}$ and ct to obtain an outcome $m'_{\mathcal{X}}$. Output 1 if $m'_{\mathcal{X}} = m$ and output 0 otherwise.

Let $\boldsymbol{P}_{\mathcal{X},\mathsf{ct}}^{\mathsf{pk},m}$ be the projection corresponding to post-selecting the outcome to 1 for $\mathcal{P}_{\mathcal{X},\mathsf{ct}}^{\mathsf{pk},m}$. Then we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{augiden\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right] = \mathop{\mathbb{E}}_{\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q,\mathsf{ct}} \mathrm{Tr}\left[\left(\boldsymbol{P}_{\mathcal{B},\mathsf{ct}}^{\mathsf{pk},m}\otimes\boldsymbol{P}_{\mathcal{C},\mathsf{ct}}^{\mathsf{pk},m}\right)q\right]$$

where the expectation is taken over $(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{Setup}(1^\lambda)$, $s\mathcal{k}\leftarrow\mathcal{KG}(\mathsf{sk})$, $m\leftarrow\mathcal{M}$, $q\leftarrow\mathcal{A}^{O_m}(1^\lambda,\mathsf{pk},s\mathcal{k})$, and $\mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$. By our assumption that $\mathcal{A}_{\mathsf{sde}}$ breaks augmented identical-challenge search anti-piracy, there is a positive polynomial p such that

$$\mathop{\mathbb{E}}_{\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q,\mathsf{ct}} \mathrm{Tr}\left[\left(\boldsymbol{P}_{\mathcal{B},\mathsf{ct}}^{\mathsf{pk},m}\otimes\boldsymbol{P}_{\mathcal{C},\mathsf{ct}}^{\mathsf{pk},m}\right)q\right] \ge 1/p(\lambda)$$

for infinitely many λ.

By an averaging argument, with probability at least $1/(2p(\lambda))$ over the choice of $(\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q)$,

$$\mathop{\mathbb{E}}_{\mathsf{ct}} \mathrm{Tr}\left[\left(\boldsymbol{P}_{\mathcal{B},\mathsf{ct}}^{\mathsf{pk},m}\otimes\boldsymbol{P}_{\mathcal{C},\mathsf{ct}}^{\mathsf{pk},m}\right)q\right] \ge 1/(2p(\lambda))$$

for infinitely many λ where the expectation is taken over $\mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$.

By Lemma 8.7, for such $(\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q)$,

$$\mathop{\mathbb{E}}_{\mathsf{ct}_{\mathcal{B}},\mathsf{ct}_{\mathcal{C}}} \mathrm{Tr}\left[\left(\boldsymbol{P}_{\mathcal{B},\mathsf{ct}_{\mathcal{B}}}^{\mathsf{pk},m}\otimes\boldsymbol{P}_{\mathcal{C},\mathsf{ct}_{\mathcal{C}}}^{\mathsf{pk},m}\right)q\right] \ge 1/(1728p(\lambda)^3)$$

for infinitely many λ where the expectation is taken over $\mathsf{ct}_{\mathcal{B}}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$ and $\mathsf{ct}_{\mathcal{C}}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$.

Since this holds with probability at least $1/(2p(\lambda))$ over the choice of $(\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q)$, we have

$$\mathop{\mathbb{E}}_{\mathsf{pk},\mathsf{sk},s\mathcal{k},m,q,\mathsf{ct}_{\mathcal{B}},\mathsf{ct}_{\mathcal{C}}} \mathrm{Tr}\left[\left(\boldsymbol{P}_{\mathcal{B},\mathsf{ct}_{\mathcal{B}}}^{\mathsf{pk},m}\otimes\boldsymbol{P}_{\mathcal{C},\mathsf{ct}_{\mathcal{C}}}^{\mathsf{pk},m}\right)q\right] \ge 1/(3456p(\lambda)^4)$$

where the expectation is taken over $(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{Setup}(1^\lambda)$, $s\mathcal{k}\leftarrow\mathcal{KG}(\mathsf{sk})$, $m\leftarrow\mathcal{M}$, $q\leftarrow\mathcal{A}^{O_m}(1^\lambda,\mathsf{pk},s\mathcal{k})$, $\mathsf{ct}_{\mathcal{B}}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$ and $\mathsf{ct}_{\mathcal{C}}\leftarrow\mathsf{Enc}(\mathsf{pk},m)$.

One can see that the left hand side of the above inequality is equal to $\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right]$. Thus, the above means that $\mathcal{A}_{\mathsf{sde}}$ breaks augmented $\mathsf{Id}_{\mathcal{U}}$-search anti-piracy security of SDE, leading to contradiction. This completes the proof of Lemma 8.6. □

8.3 $\mathcal{D}_{\mathsf{identical}}$-CPA Anti-Piracy Security in the QROM

In this section, we present a conversion that transforms an augmented identical-challenge search anti-piracy secure scheme into a $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy secure scheme in the QROM.

Lemma 8.8. *If there exists an SDE scheme that satisfies augmented identical-challenge search anti-piracy security, then there exists an SDE scheme that satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security in the QROM.*

Proof. Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M}$ that satisfies augmented identical-challenge search anti-piracy security. Note that $|\mathcal{M}|^{-1}$ is negligible since otherwise identical-challenge search anti-piracy security can be trivially broken by a random guess. Let $H : \mathcal{M} \to \mathcal{M}'$ be a random oracle.

We construct an SDE scheme $\mathsf{SDE}' = (\mathsf{Setup}', \mathcal{KG}', \mathsf{Enc}', \mathcal{D}ec')$ with message space $\mathcal{M}'$ that satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security as follows.

$\mathsf{Setup}'(1^\lambda)$**:** On input the security parameter 1^λ, run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and output $(\mathsf{pk}, \mathsf{sk})$.

$\mathcal{KG}'(\mathsf{sk})$**:** On input a classical secret key sk, run $s\mathcal{k} \leftarrow \mathcal{KG}(\mathsf{sk})$ and output $s\mathcal{k}$.

$\mathsf{Enc}'(\mathsf{pk}, m)$**:** On input a public key pk and a message $m \in \mathcal{M}'$, choose $x \leftarrow \mathcal{M}$, generate $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, x)$, set $t := H(x) \oplus m$, and output a ciphertext $\mathsf{ct}' := (\mathsf{ct}, t)$.

$\mathcal{D}ec'(s\mathcal{k}, \mathsf{ct})$**:** On input a quantum secret key $s\mathcal{k}$ and a ciphertext $\mathsf{ct}' = (\mathsf{ct}, t)$, compute $\tilde{x} \leftarrow \mathcal{D}ec(s\mathcal{k}, \mathsf{ct})$ and output $\tilde{m} := H(\tilde{x}) \oplus t$.

We prove that the above scheme satisfies $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security. Assume toward contradiction that there is a QPT adversary $\mathcal{A}'_{\mathsf{sde}} = (\mathcal{A}', \mathcal{B}', \mathcal{C}')$ that breaks $\mathcal{D}_{\mathsf{identical}}$-CPA anti-piracy security of SDE'. Let $Q(\lambda) = \mathrm{poly}(\lambda)$ be the maximum number of total queries made by $\mathcal{A}'_{\mathsf{sde}}$. We consider the following sequence of hybrids.

Hyb_0**:** This is identical to $\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE}', \mathcal{D}_{\mathsf{identical}}, \mathcal{A}'_{\mathsf{sde}}}(\lambda)$. That is, it works as follows. A random function $H : \mathcal{M} \to \mathcal{M}'$ is uniformly chosen. Quantum access to H are given to all the parties throughut the hybrid. The challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and $s\mathcal{k} \leftarrow \mathcal{KG}(\mathsf{sk})$, and sends $(1^\lambda, \mathsf{pk}, s\mathcal{k})$ to $\mathcal{A}'$. $\mathcal{A}'$ generates (m_0, m_1) and a bipartite state q on registers R_B and R_C,[13] and sends (m_0, m_1) to the challenger, $\mathsf{R}_{\mathcal{B}}$ to $\mathcal{B}'$, and R_C to $\mathcal{C}'$. The challenger chooses $\mathsf{coin} \leftarrow \{0,1\}$ and $x \leftarrow \mathcal{M}$, generates $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, x)$, sets $t := H(x) \oplus m_{\mathsf{coin}}$ and $\mathsf{ct}' := (\mathsf{ct}, t)$, and sends ct' to $\mathcal{B}'$ and $\mathcal{C}'$. Then $\mathcal{B}'$ and $\mathcal{C}'$ output $\mathsf{coin}'_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}}$, respectively. The hybrid outputs 1 if and only of $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}$ and outputs 0 otherwise.

By our assumption, we have

$$\Pr[\mathsf{Hyb}_0 = 1] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(\lambda).$$

Hyb_1**:** This hybrid is identical to the previous one except that x is chosen at the beginning and the oracle of $\mathcal{A}'$ is replaced with $H_\perp$ defined below:

$$H_\perp(x') = \begin{cases} \perp & \text{if } x' = x \\ H(x') & \text{else} \end{cases}.$$

In Hyb_2, the only information about x given to $\mathcal{A}'$ is through the oracle $H_\perp$, which returns $\perp$ if and only if the query is x. Thus, by the well-known bound for unstructured search [BBBV97], the probability that measurement of its random query happens to be x is $O(Q^2 \cdot |\mathcal{M}|^{-1})$. Thus, Lemma 7.1 implies

$$|\Pr[\mathsf{Hyb}_0 = 1] - \Pr[\mathsf{Hyb}_1 = 1]| \leq 2Q(\lambda)O(Q \cdot |\mathcal{M}|^{-1/2}) = \mathsf{negl}(\lambda).$$

Therefore, we have

$$\Pr[\mathsf{Hyb}_1 = 1] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(\lambda).$$

[13] According to the syntax in Definition 6.10, $\mathcal{A}'$ should output four challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$. However, the latter two are ignored in the rest of the security game, and thus we omit them and simply write (m_0, m_1) to mean $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$.

Hyb_2: This hybrid is identical to the previous one except that we take uniformly random $t \leftarrow \mathcal{M}'$ and then replace the oracles for $\mathcal{B}'$ and $\mathcal{C}'$ with $H_{\mathsf{coin}}^{x,m_0,m_1,t}$ defined below:

$$H_{\mathsf{coin}}^{x,m_0,m_1,t}(x') = \begin{cases} m_{\mathsf{coin}} \oplus t & \text{if } x' = x \\ H(x') & \text{else} \end{cases}$$

It is easy to see that the joint distribution of t and the oracle does not change from the previous hybrid. Therefore, we have $\Pr[\mathsf{Hyb}_1 = 1] = \Pr[\mathsf{Hyb}_2 = 1]$ and thus

$$\Pr[\mathsf{Hyb}_2 = 1] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(\lambda).$$

Then we construct a QPT adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ that breaks augmented identical-challenge search anti-piracy security of SDE as follows.

$\mathcal{A}^{O_x}$: Given the security parameter 1^λ, public key pk and quantum secret key $s\mathcal{k}$ as input, and quantum oracle access to O_x, $\mathcal{A}$ chooses a function $H : \mathcal{M} \to \mathcal{M}'$ from a $2Q$-wise independent hash family. $\mathcal{A}$ runs $\mathcal{A}'^{H_\perp}$ on input $(1^\lambda, \mathsf{pk}, s\mathcal{k})$. Let (m_0, m_1) be the challenge messages and q be a state over registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$ output by $\mathcal{A}'$. $\mathcal{A}$ chooses $t \leftarrow \mathcal{M}'$. $\mathcal{A}$ sends $\mathsf{R}_\mathcal{B}$ and (H, m_0, m_1, t) to $\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$ and (H, m_0, m_1, t) to $\mathcal{C}$.

$\mathcal{B}^{O_x}$: Given register $\mathsf{R}_\mathcal{B}$, (H, m_0, m_1, t), and a ciphertext ct as input and quantum oracle access to O_x, $\mathcal{B}$ defines $\tilde{\mathcal{B}}$ as follows:

$\tilde{\mathcal{B}}^{H_{\mathsf{coin}}^{x,m_0,m_1,t}}(q[\mathsf{R}_\mathcal{B}])$: Given input $q[\mathsf{R}_\mathcal{B}]$ and quantum oracle access to $H_{\mathsf{coin}}^{x,m_0,m_1,t}$, set $\mathsf{ct}'_\mathcal{B} = (\mathsf{ct}_\mathcal{B}, t)$, run $\mathcal{B}'^{H_{\mathsf{coin}}^{x,m_0,m_1,t}}$ on input $q[\mathsf{R}_\mathcal{B}]$ to obtain an output $\mathsf{coin}'_\mathcal{B}$ and output $\mathsf{coin}'_\mathcal{B}$.

Run $\tilde{x}_\mathcal{B} \leftarrow \mathcal{E}\mathit{xt}^{H_0^{x,m_0,m_1,t}, H_1^{x,m_0,m_1,t}}(1^\lambda, \tilde{\mathcal{B}}, q[\mathsf{R}_\mathcal{B}])$, and output $\tilde{x}_\mathcal{B}$ where $\mathcal{E}\mathit{xt}$ is the algorithm as in Lemma 7.2. Note that $\mathcal{B}$ can perfectly simulate the oracles $H_0^{x,m_0,m_1,t}$ and $H_1^{x,m_0,m_1,t}$ for $\mathcal{E}\mathit{xt}$ by using its own oracle O_x without knowing x itself.

$\mathcal{C}^{O_x}$: Do the same as $\mathcal{B}$ except that $\mathsf{R}_\mathcal{B}$ is replaced with $\mathsf{R}_\mathcal{C}$. We write $\tilde{x}_\mathcal{C}$ to mean its output.

Since $2Q$-wise independent functions are indistinguishable from uniformly random functions for algorithms that make at most Q quantum queries to the function [Zha12], $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ perfectly simulates Hyb_2 for $\mathcal{A}'_{\mathsf{sde}} = (\mathcal{A}', \mathcal{B}', \mathcal{C}')$. Since $\Pr[\mathsf{Hyb}_2 = 1] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(\lambda)$, there is a positive polynomial $p(\lambda)$ such that we have

$$\Pr\left[\mathsf{coin}'_\mathcal{B} = \mathsf{coin}'_\mathcal{C} = \mathsf{coin}\right] \geq \frac{1}{2} + \frac{1}{p(\lambda)}$$

for infinitely many λ in Hyb_2.

By an averaging argument, with probability at least $1/(2p(\lambda))$ over the choice of $(x, H, \mathsf{pk}, \mathsf{sk}, m_0, m_1, s\mathcal{k}, q, \mathsf{ct}, t)$, we have

$$\Pr\left[\mathsf{coin}'_\mathcal{B} = \mathsf{coin}'_\mathcal{C} = \mathsf{coin} : \begin{array}{l} \mathsf{coin} \leftarrow \{0,1\} \\ \mathsf{coin}'_\mathcal{B} \leftarrow \tilde{\mathcal{B}}^{H_{\mathsf{coin}}^{x,m_0,m_1,t}}(q[\mathsf{R}_\mathcal{B}]) \\ \mathsf{coin}'_\mathcal{C} \leftarrow \tilde{\mathcal{C}}^{H_{\mathsf{coin}}^{x,m_0,m_1,t}}(q[\mathsf{R}_\mathcal{C}]) \end{array}\right] \geq \frac{1}{2} + \frac{1}{2p(\lambda)}$$

for infinitely many λ.

Since $H_0^{x,m_0,m_1,t}$ and $H_1^{x,m_0,m_1,t}$ differ only at x, by Lemma 7.2, for such $(x, H_\perp, \mathsf{pk}, \mathsf{sk}, m_0, m_1, s\mathcal{k}, q, \mathsf{ct}, t)$, we have

$$\Pr\left[x'_\mathcal{B} = x'_\mathcal{C} = x : \begin{array}{l} \tilde{x}_\mathcal{B} \leftarrow \mathcal{E}\mathit{xt}^{H_0^{x,m_0,m_1,t}, H_1^{x,m_0,m_1,t}, \tilde{\mathcal{B}}}(1^\lambda, q[\mathsf{R}_\mathcal{B}]) \\ \tilde{x}_\mathcal{C} \leftarrow \mathcal{E}\mathit{xt}^{H_0^{x,m_0,m_1,t}, H_1^{x,m_0,m_1,t}, \tilde{\mathcal{C}}}(1^\lambda, q[\mathsf{R}_\mathcal{C}]) \end{array}\right] \geq \frac{1}{2^{18} p(\lambda)^6 Q(\lambda)^4} - 2^{-\lambda}$$

for infinitely many λ. Since this holds with probability at least $1/(2p(\lambda))$ over the choice of $(x, H, \mathsf{pk}, \mathsf{sk}, m_0, m_1, s\mathcal{k}, q, \mathsf{ct}, t)$, we have

$$\Pr\left[\mathsf{Exp}^{\mathsf{aug\text{-}search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathsf{Id}_{\mathcal{U}},\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right] \geq \frac{1}{2^{19}p(\lambda)^7Q(\lambda)^4} - 2^{-\lambda}$$

for infinitely many λ, leading to contradiction. This completes the proof of Lemma 8.8. □

Theorem 8.1 is obtained by combining Lemmata 8.4, 8.6 and 8.8.

9 From Search to CPA$^+$Anti-Piracy

In this section, we present a conversion that upgrades $\mathcal{U}$-search anti-piracy security to CPA$^+$anti-piracy security.

Theorem 9.1. *If there exists an SDE scheme that satisfies $\mathcal{U}$-search anti-piracy security, where $\mathcal{U}$ is as in Example 6.4, then there exists an SDE scheme that satisfies CPA$^+$anti-piracy security.*

Note that $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security implies $\mathcal{U}$-search anti-piracy security since $\mathcal{U}$ is unpredictable when $|\mathcal{M}|^{-1} = \mathsf{negl}(\lambda)$. Thus, we obtain the following corollary.

Corollary 9.2. *If there exists an SDE scheme that satisfies $\mathcal{D}_{\mathsf{unp}}$-search anti-piracy security, then there exists an SDE scheme that satisfies CPA$^+$anti-piracy security.*

Proof of Theorem 9.1. Let $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M} \subseteq \{0,1\}^n$ that satisfies $\mathcal{U}$-search anti-piracy security.

We construct an SDE scheme $\mathsf{SDE}' = (\mathsf{Setup}', \mathcal{KG}', \mathsf{Enc}', \mathcal{D}ec')$ with message space $\{0,1\}$ that satisfies CPA$^+$security as follows.

$\mathsf{Setup}'(1^\lambda)$**:** On input the security parameter 1^λ, run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and output $(\mathsf{pk}, \mathsf{sk})$.

$\mathcal{KG}'(\mathsf{sk})$**:** On input a classical secret key sk, run $s\mathcal{k} \leftarrow \mathcal{KG}(\mathsf{sk})$ and output $s\mathcal{k}$.

$\mathsf{Enc}'(\mathsf{pk}, m)$**:** On input a public key pk and a message $m \in \{0,1\}$, choose $r \leftarrow \{0,1\}^n$ and $x \leftarrow \mathcal{M}$ generate $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, x)$, set $b := (x \cdot r) \oplus m$, and output a ciphertext $\mathsf{ct}' := (\mathsf{ct}, r, b)$.

$\mathcal{D}ec'(s\mathcal{k}, \mathsf{ct})$**:** On input a quantum secret key $s\mathcal{k}$ and a ciphertext $\mathsf{ct}' = (\mathsf{ct}, r, b)$, compute $\tilde{x} \leftarrow \mathcal{D}ec(s\mathcal{k}, \mathsf{ct})$ and output $\tilde{m} := (\tilde{x} \cdot r) \oplus b$.

We prove that the above scheme satisfies CPA$^+$anti-piracy security. Assume toward contradiction that there is a QPT adversary $\mathcal{A}'_{\mathsf{sde}} = (\mathcal{A}', \mathcal{B}', \mathcal{C}')$ that breaks CPA$^+$anti-piracy security of SDE'. Since the message space of SDE' is single-bits, we can assume that the challenge messages $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ chosen by $\mathcal{A}'$ is $(0,1,0,1)$ without loss of generality. Then we construct a QPT adversary $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ that breaks $\mathcal{M}$-search anti-piracy security of SDE as follows.

$\mathcal{A}$**:** Given the security parameter 1^λ, public key pk and quantum secret key $s\mathcal{k}$, $\mathcal{A}$ runs $\mathcal{A}'$ on input $(1^\lambda, \mathsf{pk}, s\mathcal{k}, aux)$ to obtain a bipartite state q over registers $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$.[14] $\mathcal{A}$ sends $\mathsf{R}_{\mathcal{B}}$ and $\mathsf{R}_{\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$, respectively.

$\mathcal{B}$**:** Given register $\mathsf{R}_{\mathcal{B}}$ and a ciphertext $\mathsf{ct}_{\mathcal{B}}$, $\mathcal{B}$ defines an algorithm $\tilde{\mathcal{B}}$ as follows.

$\tilde{\mathcal{B}}(q[\mathsf{R}_{\mathcal{B}}], r_{\mathcal{B}})$**:** On input $q[\mathsf{R}_{\mathcal{B}}]$ and $r_{\mathcal{B}} \in \{0,1\}^n$, choose $b_{\mathcal{B}} \leftarrow \{0,1\}$, set $\mathsf{ct}'_{\mathcal{B}} = (\mathsf{ct}_{\mathcal{B}}, r_{\mathcal{B}}, b_{\mathcal{B}})$, run $\mathcal{B}'$ on input $q[\mathsf{R}_{\mathcal{B}}]$ and $\mathsf{ct}'_{\mathcal{B}}$ to obtain an output $\mathsf{coin}'_{\mathcal{B}}$, and output $\widetilde{\mathsf{coin}}_{\mathcal{B}} := \mathsf{coin}'_{\mathcal{B}} \oplus b_{\mathcal{B}}$.

Run $\tilde{x}_{\mathcal{B}} \leftarrow \mathcal{E}xt(\tilde{\mathcal{B}}, q[\mathsf{R}_{\mathcal{B}}])$, and output $\tilde{x}_{\mathcal{B}}$ where $\mathcal{E}xt$ is the algorithm as in Lemma 3.3.

$\mathcal{C}$**:** Do the same as $\mathcal{B}$ except for the input being replaced with $\mathsf{R}_{\mathcal{C}}$ and $\mathsf{ct}_{\mathcal{C}}$. We write $\tilde{x}_{\mathcal{C}}$ to mean its output.

[14] Since we assume that the challenge messages are $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1}) = (0,1,0,1)$, we omit it.

Since $\mathcal{A}'_{\mathsf{sde}} = (\mathcal{A}', \mathcal{B}', \mathcal{C}')$ breaks CPA$^+$anti-piracy security, there is a positive polynomial $p(\lambda)$ such that we have

$$\Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}\right] \geq \frac{1}{2} + \frac{1}{p(\lambda)}$$

for infinitely many λ where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $s\mathcal{k} \leftarrow \mathcal{KG}(\mathsf{sk})$, $q \leftarrow \mathcal{A}(1^\lambda, \mathsf{pk}, s\mathcal{k})$ $x_{\mathcal{B}}, x_{\mathcal{C}} \leftarrow \mathcal{M}$, $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, x_{\mathcal{B}})$, $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, x_{\mathcal{C}})$, $r_{\mathcal{B}}, r_{\mathcal{C}} \leftarrow \{0,1\}^n$, $\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}$, $b_{\mathcal{B}} := \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \mathsf{coin}_{\mathcal{B}}$, $b_{\mathcal{C}} := \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle \oplus \mathsf{coin}_{\mathcal{C}}$, $\mathsf{ct}'_{\mathcal{B}} = (\mathsf{ct}_{\mathcal{B}}, r_{\mathcal{B}}, b_{\mathcal{B}})$, $\mathsf{ct}'_{\mathcal{C}} = (\mathsf{ct}_{\mathcal{C}}, r_{\mathcal{C}}, b_{\mathcal{C}})$, $\mathsf{coin}'_{\mathcal{B}} \leftarrow \mathcal{B}(\mathsf{R}_{\mathcal{B}}, \mathsf{ct}'_{\mathcal{B}})$, and $\mathsf{coin}'_{\mathcal{C}} \leftarrow \mathcal{C}(\mathsf{R}_{\mathcal{C}}, \mathsf{ct}'_{\mathcal{C}})$.

By an averaging argument, with probability at least $1/(2p(\lambda))$ over the choice of $(\mathsf{pk}, \mathsf{sk}, s\mathcal{k}, q, x_{\mathcal{B}}, x_{\mathcal{C}}, \mathsf{ct}_{\mathcal{B}}, \mathsf{ct}_{\mathcal{C}})$, we have

$$\Pr\left[\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}\right] \geq \frac{1}{2} + \frac{1}{2p(\lambda)}$$

for infinitely many λ where $r_{\mathcal{B}}, r_{\mathcal{C}} \leftarrow \{0,1\}^n, \mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}, b_{\mathcal{B}} := \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \mathsf{coin}_{\mathcal{B}}, b_{\mathcal{C}} := \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle \oplus \mathsf{coin}_{\mathcal{C}}$, $\mathsf{ct}'_{\mathcal{B}} = (\mathsf{ct}_{\mathcal{B}}, r_{\mathcal{B}}, b_{\mathcal{B}})$, $\mathsf{ct}'_{\mathcal{C}} = (\mathsf{ct}_{\mathcal{C}}, r_{\mathcal{C}}, b_{\mathcal{C}})$, $\mathsf{coin}'_{\mathcal{B}} \leftarrow \mathcal{B}(q[\mathsf{R}_{\mathcal{B}}], \mathsf{ct}'_{\mathcal{B}})$, and $\mathsf{coin}'_{\mathcal{C}} \leftarrow \mathcal{C}(q[\mathsf{R}_{\mathcal{C}}], \mathsf{ct}'_{\mathcal{C}})$. Note that choosing $\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}} \leftarrow \{0,1\}$ and then setting $b_{\mathcal{B}} := \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \mathsf{coin}_{\mathcal{B}}$ and $b_{\mathcal{C}} := \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle \oplus \mathsf{coin}_{\mathcal{C}}$ are equivalent to choosing $b_{\mathcal{B}}, b_{\mathcal{C}} \leftarrow \{0,1\}$ and then setting $\mathsf{coin}_{\mathcal{B}} := \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus b_{\mathcal{B}}$ and $\mathsf{coin}_{\mathcal{C}} := \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle \oplus b_{\mathcal{C}}$. Also note that $\mathsf{coin}'_{\mathcal{B}} \oplus \mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{B}} \oplus \mathsf{coin}_{\mathcal{C}}$ is equivalent to $\widetilde{\mathsf{coin}}_{\mathcal{B}} \oplus \widetilde{\mathsf{coin}}_{\mathcal{C}} = \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle$ where $\widetilde{\mathsf{coin}}_{\mathcal{B}} := \mathsf{coin}'_{\mathcal{B}} \oplus b_{\mathcal{B}}$ and $\widetilde{\mathsf{coin}}_{\mathcal{C}} := \mathsf{coin}'_{\mathcal{C}} \oplus b_{\mathcal{C}}$. Thus, with probability at least $1/(2p(\lambda))$ over the choice of $(\mathsf{pk}, \mathsf{sk}, s\mathcal{k}, q, x_{\mathcal{B}}, x_{\mathcal{C}}, \mathsf{ct}_{\mathcal{B}}, \mathsf{ct}_{\mathcal{C}})$, we have

$$\Pr\left[\widetilde{\mathsf{coin}}_{\mathcal{B}} \oplus \widetilde{\mathsf{coin}}_{\mathcal{C}} = \langle r_{\mathcal{B}}, x_{\mathcal{B}}\rangle \oplus \langle r_{\mathcal{C}}, x_{\mathcal{C}}\rangle\right] \geq \frac{1}{2} + \frac{1}{2p(\lambda)}$$

for infinitely many λ where $r_{\mathcal{B}}, r_{\mathcal{C}} \leftarrow \{0,1\}^n$, $\widetilde{\mathsf{coin}}_{\mathcal{B}} \leftarrow \tilde{\mathcal{B}}(q[\mathsf{R}_{\mathcal{B}}], r_{\mathcal{B}})$, and $\widetilde{\mathsf{coin}}_{\mathcal{C}} \leftarrow \tilde{\mathcal{B}}((q[\mathsf{R}_{\mathcal{C}}], r_{\mathcal{C}})$. By Lemma 3.3, with probability at least $1/(2p(\lambda))$ over the choice of $(\mathsf{pk}, \mathsf{sk}, s\mathcal{k}, q, x_{\mathcal{B}}, x_{\mathcal{C}}, \mathsf{ct}_{\mathcal{B}}, \mathsf{ct}_{\mathcal{C}})$,

$$\Pr[\mathcal{E}\mathcal{x}t(\tilde{\mathcal{B}}, q[\mathsf{R}_{\mathcal{B}}]) = x_{\mathcal{B}} \wedge \mathcal{E}\mathcal{x}t(\tilde{\mathcal{C}}, q[\mathsf{R}_{\mathcal{C}}]) = x_{\mathcal{C}}] \geq \frac{1}{p(\lambda)^2}$$

for infinitely many λ. This implies

$$\Pr\left[\mathsf{Exp}^{\mathsf{search\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \geq \frac{1}{2p(\lambda)^3}$$

for infinitely many λ, contradicting $\mathcal{D}$-search anti-piracy security of SDE. □

Remark 9.3. In the above proof, the constructed scheme only supports single-bit messages. However, we show that CPA$^+$anti-piracy security is preserved under parallel composition in Section 10. Thus, we can arbitrarily expand the message length while preserving CPA$^+$anti-piracy security.

Remark 9.4. In the above proof, we assume that the base scheme is $\mathcal{U}$-search anti-piracy secure where the challenge messages are independently and uniformly random. In fact, a similar proof works for a scheme with $\mathcal{D}$-search anti-piracy security as long as the joint distribution of $(m_{\mathcal{B}}, m_{\mathcal{C}})$ generated by $\mathcal{D}$ is a product distribution $D_{\mathcal{B}} \times D_{\mathcal{C}}$ for some distributions $D_{\mathcal{B}}$ and $D_{\mathcal{C}}$.

10 Parallel Composition Theorem

We prove that CPA$^+$anti-piracy security and strong anti-piracy security (which are shown to be equivalent in Theorem 6.23) are preserved under parallel composition.

Let $\mathsf{SDE} = (\mathsf{SDE.Setup}, \mathsf{SDE}.\mathcal{KG}, \mathsf{SDE.Enc}, \mathsf{SDE}.\mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M}$. For $\ell = \mathrm{poly}(\lambda)$, let $\mathsf{SDE}^{(\ell)} = (\mathsf{SDE}^{(\ell)}.\mathsf{Setup}, \mathsf{SDE}^{(\ell)}.\mathcal{KG}, \mathsf{SDE}^{(\ell)}.\mathsf{Enc}, \mathsf{SDE}^{(\ell)}.\mathcal{D}ec)$ be an SDE scheme with message space $\mathcal{M}^\ell$ defined as follows.

$\mathsf{SDE}^{(\ell)}.\mathsf{Setup}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$**:** On input the security parameter 1^λ, run $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{SDE.Setup}(1^\lambda)$ and output $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{SDE}^{(\ell)}.\mathcal{KG}(\mathsf{sk}) \to s\mathcal{k}$**:** On input a classical secret key sk, run $s\mathcal{k} \leftarrow \mathsf{SDE}.\mathcal{KG}(\mathsf{sk})$ and output $s\mathcal{k}$.

$\mathsf{SDE}^{(\ell)}.\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{SDE}^{(\ell)}.\mathsf{ct}$**:** On input a public key pk and a message $m = (m_1, \dots, m_\ell) \in \mathcal{M}^\ell$, generate $\mathsf{SDE}.\mathsf{ct}_i \leftarrow \mathsf{SDE}.\mathsf{Enc}(\mathsf{pk}, m_i)$ for $i \in [\ell]$ and output a ciphertext $\mathsf{SDE}^{(\ell)}.\mathsf{ct} := (\mathsf{SDE}.\mathsf{ct}_i)_{i\in[\ell]}$.

$\mathsf{SDE}^{(\ell)}.\mathcal{D}ec(s\mathcal{k}, \mathsf{SDE}^{(\ell)}.\mathsf{ct}) \to \tilde{m}$**:** On input a quantum secret key $s\mathcal{k}$ and a ciphertext $\mathsf{SDE}^{(\ell)}.\mathsf{ct} = (\mathsf{SDE}.\mathsf{ct}_i)_{i\in[\ell]}$, compute $\tilde{m}_i \leftarrow \mathsf{SDE}.\mathcal{D}ec(s\mathcal{k}, \mathsf{SDE}.\mathsf{ct}_i)$ for $i \in [\ell]$,[15] and output $\tilde{m} := (\tilde{m}_1, \dots, \tilde{m}_\ell)$.

The correctness of $\mathsf{SDE}^{(\ell)}$ immediately follows from that of SDE.

Theorem 10.1. *If* SDE *satisfies strong anti-piracy security, then* $\mathsf{SDE}^{(\ell)}$ *also satisfies strong anti-piracy security.*

Combining Theorems 6.23 and 10.1, we obtain the following corollary.

Corollary 10.2. *If* SDE *satisfies CPA*$^+$*anti-piracy security, then* $\mathsf{SDE}^{(\ell)}$ *also satisfies CPA*$^+$*anti-piracy security.*

Proof of Theorem 10.1. Toward contradiction, suppose that $\mathsf{SDE}^{(\ell)}$ is not strong anti-piracy secure. That is, suppose that $\mathsf{SDE}^{(\ell)}$ is not strong γ-anti-piracy secure for some inverse polynomial γ. Then, there is a QPT adversary $\mathsf{SDE}^{(\ell)}.\mathcal{A}$ such that $\mathsf{Adv}^{\mathsf{strong\text{-}anti\text{-}piracy}}_{\mathsf{SDE}^{(\ell)},\mathsf{SDE}^{(\ell)}.\mathcal{A}}(\lambda, \gamma(\lambda))$ is non-negligible. Let $\epsilon = \frac{\gamma}{6}$ and $\delta = 2^{-\lambda}$. We construct an adversary $\mathsf{SDE}.\mathcal{A}$ against strong $\frac{\gamma}{4\ell}$-anti-piracy security of SDE as follows.

$\mathsf{SDE}.\mathcal{A}(\mathsf{pk}, s\mathcal{k})$**:** Do the following:

- Run $\mathsf{SDE}^{(\ell)}.\mathcal{A}(\mathsf{pk}, s\mathcal{k})$ to obtain $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1}) \in (\mathcal{M}^\ell)^4$ of messages and two (possibly entangled) quantum decryptors $\mathcal{D}_\mathcal{B} = (q[\mathsf{R}_\mathcal{B}], \boldsymbol{U}_\mathcal{B})$ and $\mathcal{D}_\mathcal{C} = (q[\mathsf{R}_\mathcal{C}], \boldsymbol{U}_\mathcal{C})$ for $\mathsf{SDE}^{(\ell)}$, where q is a quantum state over registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$, and $\boldsymbol{U}_\mathcal{B}$ and $\boldsymbol{U}_\mathcal{C}$ are unitary quantum circuits. For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$ and $\mathsf{coin} \in \{0,1\}$, parse $m_{\mathcal{X},\mathsf{coin}} = (m^{(1)}_{\mathcal{X},\mathsf{coin}}, \dots, m^{(\ell)}_{\mathcal{X},\mathsf{coin}})$.
- For $\mathcal{X} \in \{\mathcal{B}, \mathcal{C}\}$, let $\mathcal{P}_{\mathcal{X},D_\mathcal{X}}$ be a mixture of projective measurements associated to a function $D_\mathcal{X}$ and a family $\mathcal{P}_\mathcal{X} = \{\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{SDE}^{(\ell)}.\mathsf{ct})}\}_{\mathsf{coin},\mathsf{SDE}^{(\ell)}.\mathsf{ct}}$ of projective measurements defined as follows:
  - $D_\mathcal{X}$ takes $\mathsf{coin} \in \{0,1\}$ and a randomness r_{Enc} for $\mathsf{SDE}^{(\ell)}.\mathsf{Enc}$ as input and outputs coin and $\mathsf{SDE}^{(\ell)}.\mathsf{ct} = \mathsf{SDE}^{(\ell)}.\mathsf{Enc}(\mathsf{pk}, m_{\mathcal{X},\mathsf{coin}}; r_{\mathsf{Enc}})$.
  - $\mathcal{P}_{\mathcal{X},(\mathsf{coin},\mathsf{SDE}^{(\ell)}.\mathsf{ct})}$ is a projective measurement corresponding to the following procedure: On a quantum state $\widetilde{q}$ on register $\mathsf{R}_\mathcal{X}$, run $\mathsf{coin}' \leftarrow \widetilde{\mathcal{D}}_\mathcal{X}(\mathsf{ct})$ where $\widetilde{\mathcal{D}}_\mathcal{X} = (\widetilde{q}, \boldsymbol{U}_\mathcal{X})$. If $\mathsf{coin}' = \mathsf{coin}$, output 1, otherwise output 0.

  Apply $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{B},D_\mathcal{B},1/2+\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{C},D_\mathcal{C},1/2+\gamma-\epsilon}$ on q where the first and second $\mathcal{ATI}$ act on registers $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$, respectively. If either of them results in outcome 0, abort. Otherwise (i.e., if the both measurements result in outcome 1), let q' be the resulting state on $\mathsf{R}_\mathcal{B}$ and $\mathsf{R}_\mathcal{C}$. Let $\mathcal{D}'_\mathcal{B} = (q'[\mathsf{R}_\mathcal{B}], \boldsymbol{U}_\mathcal{B})$ and $\mathcal{D}'_\mathcal{C} = (q'[\mathsf{R}_\mathcal{C}], \boldsymbol{U}_\mathcal{C})$.
- For $\mathcal{B} \in \{\mathcal{B}, \mathcal{C}\}$, choose $i_\mathcal{X} \leftarrow [\ell]$ and define a quantum decryptor $\widetilde{\mathcal{D}}_{\mathcal{X},i_\mathcal{X}}$ for SDE that works as follows.

  $\widetilde{\mathcal{D}}_{\mathcal{X},i_\mathcal{X}}(\mathsf{SDE}.\mathsf{ct})$**:** On input $\mathsf{SDE}.\mathsf{ct}$, do the following. For $i \in [\ell]$, generate $\mathsf{SDE}.\mathsf{ct}_i$ as follows:
  - If $i \le i_\mathcal{X} - 1$, generate $\mathsf{SDE}.\mathsf{ct}_i \leftarrow \mathsf{SDE}.\mathsf{Enc}(\mathsf{pk}, m^{(i)}_{\mathcal{X},0})$
  - If $i = i_\mathcal{X}$, set $\mathsf{SDE}.\mathsf{ct}_i := \mathsf{SDE}.\mathsf{ct}$.
  - If $i \ge i_\mathcal{X} + 1$, generate $\mathsf{SDE}.\mathsf{ct}_i \leftarrow \mathsf{SDE}.\mathsf{Enc}(\mathsf{pk}, m^{(i)}_{\mathcal{X},1})$.

  Let $\mathsf{SDE}^{(\ell)}.\mathsf{ct} := (\mathsf{SDE}.\mathsf{ct}_i)_{i\in[\ell]}$. Run $\mathsf{coin}' \leftarrow \mathcal{D}'_j(\mathsf{SDE}^{(\ell)}.\mathsf{ct})$ and output coin'.
- Output a pair $(\widetilde{m}_{\mathcal{B},0}, \widetilde{m}_{\mathcal{B},1}, \widetilde{m}_{\mathcal{C},0}, \widetilde{m}_{\mathcal{C},1}) = (m^{(i_\mathcal{B})}_{\mathcal{B},0}, m^{(i_\mathcal{B})}_{\mathcal{B},1}, m^{(i_\mathcal{C})}_{\mathcal{C},0}, m^{(i_\mathcal{C})}_{\mathcal{C},1})$ of messages and two (possibly entangled) quantum decryptors $\widetilde{\mathcal{D}}_{\mathcal{B},i_\mathcal{B}}$ and $\widetilde{\mathcal{D}}_{\mathcal{C},i_\mathcal{C}}$ defined above.

[15] We can use the same $s\mathcal{k}$ for decrypting many (honestly generated) ciphertexts by the gentle measurement lemma.

In the following, we show that $\mathsf{SDE}.\mathcal{A}$ breaks strong $\frac{\gamma}{4\ell}$-anti-piracy security of SDE. Let E be the event that $\mathsf{SDE}.\mathcal{A}(\mathsf{pk}, s\mathcal{k})$ does not abort where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{SDE.Setup}(1^\lambda)$ and $s\mathcal{k} \leftarrow \mathsf{SDE}.\mathcal{KG}(\mathsf{sk})$. We prove the following lemmas.

Lemma 10.3. $\Pr[E]$ *is non-negligible.*

Proof of Lemma 10.3. The probability that $\mathsf{SDE}.\mathcal{A}(\mathsf{pk}, s\mathcal{k})$ does not abort can be written as

$$\mathrm{Tr}\left[(\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{B},D_\mathcal{B},\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_C,D_C,\gamma-\epsilon})q\right].$$

By the first item of Lemma 3.16,

$$\mathrm{Tr}\left[(\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{B},D_\mathcal{B},\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_C,D_C,\gamma-\epsilon})q\right] \geq \mathrm{Tr}[(\mathcal{TI}_\gamma(\mathcal{P}_{\mathcal{B},D_\mathcal{B}}) \otimes \mathcal{TI}_\gamma(\mathcal{P}_{C,D_C}))q] - 2\delta.$$

By the assumption that $\mathsf{SDE}^{(\ell)}.\mathcal{A}$ breaks strong γ-anti-piracy security of $\mathsf{SDE}^{(\ell)}$, $\mathrm{Tr}[(\mathcal{TI}_\gamma(\mathcal{P}_{\mathcal{B},D_\mathcal{B}}) \otimes \mathcal{TI}_\gamma(\mathcal{P}_{C,D_C}))q]$ is non-negligible. Since $\delta = \mathsf{negl}(\lambda)$, Lemma 10.3 follows. □

Lemma 10.4. *Conditioned that E occurs,*

$$\mathrm{Tr}\left[(\mathcal{TI}_{1/2+\gamma-3\epsilon}(\mathcal{P}_{\mathcal{B},D_\mathcal{B}}) \otimes \mathcal{TI}_{1/2+\gamma-3\epsilon}(\mathcal{P}_{C,D_C}))q'\right] \geq 1 - 4\delta$$

Proof of Lemma 10.4. When E occurs, $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{B},D_\mathcal{B},\gamma-\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_C,D_C,\gamma-\epsilon}$ results in outcome 1 for both registers. Thus, this lemma immediately follows from the second item of Lemma 3.16. □

Let q'' be the (normalized) state obtained by applying $\mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_\mathcal{B},D_\mathcal{B},1/2+\gamma-3\epsilon} \otimes \mathcal{ATI}^{\epsilon,\delta}_{\mathcal{P}_C,D_C,1/2+\gamma-3\epsilon}$ to q' where both measurement outcomes are post-selected to 1. Lemma 6.15 implies that both $\mathcal{D}''_\mathcal{B} = (q''[\mathsf{R}_\mathcal{B}], \boldsymbol{U}_\mathcal{B})$ and $\mathcal{D}''_C = (q''[\mathsf{R}_C], \boldsymbol{U}_C)$ are $(\gamma - 3\epsilon) = \frac{\gamma}{2}$-good quantum decryptors with respect to $(\mathsf{pk}, (m_{\mathcal{B},0}, m_{\mathcal{B},1}))$ and $(\mathsf{pk}, (m_{C,0}, m_{C,1}))$, respectively. By Lemma 6.15, the gentle measurement lemma (Lemma 3.2), and $\delta = 2^{-\lambda}$, the trace distance between q' and q'' is negligible when E occurs. Moreover, Lemma 10.3 ensures that $\Pr[E]$ is non-negligible. Thus, for proving that $\mathsf{SDE}.\mathcal{A}$ breaks strong $\frac{\gamma}{4\ell}$-anti-piracy security of SDE, it suffices to prove that it breaks it assuming that both $\mathcal{D}'_\mathcal{B} = (q'[\mathsf{R}_\mathcal{B}], \boldsymbol{U}_\mathcal{B})$ and $\mathcal{D}'_C = (q'[\mathsf{R}_C], \boldsymbol{U}_C)$ are $\frac{\gamma}{2}$-good quantum decryptors with respect to $(\mathsf{pk}, (m_{\mathcal{B},0}, m_{\mathcal{B},1}))$ and $(\mathsf{pk}, (m_{C,0}, m_{C,1}))$, respectively. In particular, it suffices to prove the following lemma.

Lemma 10.5. *If both $\mathcal{D}'_\mathcal{B}$ and $\mathcal{D}'_C$ are $\frac{\gamma}{2}$-good quantum decryptors with respect to $(\mathsf{pk}, (m_{\mathcal{B},0}, m_{\mathcal{B},1}))$ and $(\mathsf{pk}, (m_{C,0}, m_{C,1}))$, respectively, then*

$$\Pr\left[\widetilde{\mathcal{D}}_{\mathcal{B},i_\mathcal{B}} \textit{ passes test}_\mathcal{B} \wedge \widetilde{\mathcal{D}}_{C,i_C} \textit{ passes test}_C\right] \geq \frac{\gamma^2}{16\ell^2}$$

where $i_\mathcal{B}, i_C \leftarrow [\ell]$ and $\textit{test}_X$ means the test for $\frac{\gamma}{4\ell}$-good quantum decryptors with respect to pk and $(\widetilde{m}_{X,0}, \widetilde{m}_{X,1}) = (m^{(i_X)}_{X,0}, m^{(i_X)}_{X,1})$ (as per Definition 6.14).

When both $\mathcal{D}'_\mathcal{B}$ and $\mathcal{D}'_C$ are $\frac{\gamma}{2}$-good quantum decryptors, suppose that we apply an arbitrary measurement on register $\mathsf{R}_\mathcal{B}$. Lemma 6.16 implies that $\mathcal{D}'_C$ is still a $\frac{\gamma}{2}$-good quantum decryptor conditioned on any outcome for the measurement on register $\mathcal{D}'_\mathcal{B}$. Therefore, we can reduce Lemma 10.5 to Lemma 10.6 stated below.

Lemma 10.6. *The following hold where $i_\mathcal{B}, i_C \leftarrow [\ell]$ and $\textit{test}_X$ is as in Lemma 10.5.*

- *If $\mathcal{D}'_\mathcal{B}$ is a $\frac{\gamma}{2}$-good quantum decryptor with respect to $(\mathsf{pk}, (m_{\mathcal{B},0}, m_{\mathcal{B},1}))$, then*

$$\Pr\left[\widetilde{\mathcal{D}}_{\mathcal{B},i_\mathcal{B}} \textit{ passes test}_\mathcal{B}\right] \geq \frac{\gamma}{4\ell}$$

- *If $\mathcal{D}'_C$ is a $\frac{\gamma}{2}$-good decryptor $(\mathsf{pk}, (m_{C,0}, m_{C,1}))$, then*

$$\Pr\left[\widetilde{\mathcal{D}}_{C,i_C} \textit{ passes test}_C\right] \geq \frac{\gamma}{4\ell}$$

Proof of Lemma 10.6. Since both items can proven similarly, we only prove the first item here. Since $\mathcal{D}'_{\mathcal{B}}$ is a $\frac{\gamma}{2}$-good quantum decryptor with respect to pk and $(m_{\mathcal{B},0}, m_{\mathcal{B},1})$, it is straightforward to see that

$$\Pr\left[\mathcal{D}'_{\mathcal{B}}(\mathsf{SDE}^{(\ell)}.\mathsf{ct}) = \mathsf{coin}\right] \geq \frac{1}{2} + \frac{\gamma}{2}$$

where $\mathsf{coin} \leftarrow \{0,1\}$ and $\mathsf{SDE}^{(\ell)}.\mathsf{ct} \leftarrow \mathsf{SDE}^{(\ell)}.\mathsf{Enc}(\mathsf{pk}, m_{\mathsf{coin}})$. For $\mathsf{coin} \in \{0,1\}$ and $i_{\mathcal{B}} \in [\ell]$, define $m^{(i_{\mathcal{B}})}_{\mathcal{B},\mathsf{coin}} \in \mathcal{M}^{\ell}$ as follows: the first $i_{\mathcal{B}} - 1$ coordinates are identical to those of $m_{\mathcal{B},0}$, and the remaining $\ell - i_{\mathcal{B}} + 1$ coordinates are identical to those of $m_{\mathcal{B},1}$. Note that $m^{(1)}_{\mathcal{X},0} = m_{\mathcal{X},0}$ and $m^{(\ell)}_{1} = m_1$. Thus, by the triangle inequality, we have

$$\Pr\left[\mathcal{D}'_{\mathcal{B}}(\mathsf{SDE}^{(\ell)}.\mathsf{ct}^{(i_{\mathcal{B}})}) = \mathsf{coin}\right] \geq \frac{1}{2} + \frac{\gamma}{2\ell}$$

where $\mathsf{coin} \leftarrow \{0,1\}$, $i_{\mathcal{B}} \leftarrow [\ell]$, and $\mathsf{SDE}^{(\ell)}.\mathsf{ct}^{(i_{\mathcal{B}})} \leftarrow \mathsf{SDE}^{(\ell)}.\mathsf{Enc}(\mathsf{pk}, m^{(i_{\mathcal{B}})}_{\mathcal{B},\mathsf{coin}})$. By the definition of $\widetilde{\mathcal{D}}_{\mathcal{B},i_{\mathcal{B}}}$, this means that

$$\Pr\left[\widetilde{\mathcal{D}}_{\mathcal{B},i_{\mathcal{B}}}(\mathsf{SDE}.\mathsf{ct}) = \mathsf{coin}\right] \geq \frac{1}{2} + \frac{\gamma}{2\ell}$$

where $\mathsf{coin} \leftarrow \{0,1\}$, $i_{\mathcal{B}} \leftarrow [\ell]$, and $\mathsf{SDE}.\mathsf{ct} \leftarrow \mathsf{SDE}.\mathsf{Enc}(\mathsf{pk}, m^{(i_{\mathcal{B}})}_{\mathcal{B},\mathsf{coin}})$. Thus, by an averaging argument, the probability that $\widetilde{\mathcal{D}}_{\mathcal{B},i_{\mathcal{B}}}$ passes $\mathsf{test}_{\mathcal{B}}$ is at least $\frac{\gamma}{4\ell}$. □

As already explained, Lemmata 6.16 and 10.6 imply Lemma 10.5, and Lemmata 10.3 to 10.5 together imply that $\mathsf{SDE}.\mathcal{A} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ breaks strong $\frac{\gamma}{4\ell}$-anti-piracy security of SDE, which contradicts the assumption. This completes the proof of Theorem 10.1. □

11 CPA Anti-Piracy under Arbitrarily Correlated Challenge Bits

In this section, we first define correlated-challenge-bits CPA anti-piracy security that captures arbitrary correlation between the challenge bits for the second stage adversaries. We then show that correlated-challenge-bits CPA anti-piracy security is equivalent to $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security.

Definition 11.1 (Correlated-Challenge-Bits CPA Anti-Piracy Security). *Let* $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ *be an SDE scheme. Let* $\mathcal{D}_{\mathsf{challbits}}$ *be any distribution over* $\{0,1\} \times \{0,1\}$*. We consider the correlated-challenge-bits CPA anti-piracy game* $\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}_{\mathsf{sde}}}(\lambda)$ *between the challenger and an adversary* $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ *below.*

1. *The challenger generates* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^{\lambda})$.
2. *The challenger generates* $sk \leftarrow \mathcal{KG}(\mathsf{sk})$ *and sends* $(1^{\lambda}, \mathsf{pk}, sk)$ *to* $\mathcal{A}$.
3. $\mathcal{A}$ *chooses two pairs of messages* $(m_{\mathcal{B},0}, m_{\mathcal{B},1}) \in \mathcal{M}^2$ *and* $(m_{\mathcal{C},0}, m_{\mathcal{C},1}) \in \mathcal{M}^2$ *such that* $|m_{\mathcal{B},0}| = |m_{\mathcal{B},1}|$ *and* $|m_{\mathcal{C},0}| = |m_{\mathcal{C},1}|$*, and creates a bipartite state* q *over registers* $\mathsf{R}_{\mathcal{B}}$ *and* $\mathsf{R}_{\mathcal{C}}$*. Then,* $\mathcal{A}$ *sends* $(m_{\mathcal{B},0}, m_{\mathcal{B},1}, m_{\mathcal{C},0}, m_{\mathcal{C},1})$ *to the challenger, register* $\mathsf{R}_{\mathcal{B}}$ *to* $\mathcal{B}$*, and register* $\mathsf{R}_{\mathcal{C}}$ *to* $\mathcal{C}$.
4. *The challenger generates* $(\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}}) \leftarrow \mathcal{D}_{\mathsf{challbits}}$ *and generates* $\mathsf{ct}_{\mathcal{B}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{B},\mathsf{coin}_{\mathcal{B}}})$ *and* $\mathsf{ct}_{\mathcal{C}} \leftarrow \mathsf{Enc}(\mathsf{pk}, m_{\mathcal{C},\mathsf{coin}_{\mathcal{C}}})$*. Then, the challenger sends* $\mathsf{ct}_{\mathcal{B}}$ *and* $\mathsf{ct}_{\mathcal{C}}$ *to* $\mathcal{B}$ *and* $\mathcal{C}$*, respectively.*
5. $\mathcal{B}$ *and* $\mathcal{C}$ *respectively output* $\mathsf{coin}'_{\mathcal{B}}$ *and* $\mathsf{coin}'_{\mathcal{C}}$*. The challenger outputs* 1 *if* $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ *and* $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$ *and otherwise outputs* 0.

We say that SDE *satisfies correlated-challenge-bits CPA anti-piracy security if for any QPT adversary* $\mathcal{A}_{\mathsf{sde}}$ *and any distribution* $\mathcal{D}_{\mathsf{challbits}}$*, it holds that*

$$\Pr\left[\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] \leq p^{\mathsf{triv}}_{\mathcal{D}_{\mathsf{challbits}}} + \mathsf{negl}(\lambda),$$

where $p^{\mathsf{triv}}_{\mathcal{D}_{\mathsf{challbits}}} = \max\{\Pr[\mathsf{coin}_{\mathcal{B}} = 0], \Pr[\mathsf{coin}_{\mathcal{B}} = 1], \Pr[\mathsf{coin}_{\mathcal{C}} = 0], \Pr[\mathsf{coin}_{\mathcal{C}} = 1]\}$.

Note that $p^{\mathsf{triv}}_{\mathcal{D}_{\mathsf{challbits}}}$ is the trivial success probability with respect to $\mathcal{D}_{\mathsf{challbits}}$ that is achieved when $\mathcal{A}$ just passes sk to one of the second stage adversaries, the second stage adversary decrypts the given challenge with sk, and the other second stage adversary does random guessing.

Remark 11.2 (On real-or-random style anti-piracy from [CHV23]). Before our work, [CHV23] considered a special case of our correlated-challenge-bits CPA anti-piracy security, called real-or-random style anti-piracy security, where the joint distribution of $(\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}})$ assigns probability $1/3$ to each of $(0,1)$, $(1,0)$, and $(1,1)$, and probability 0 to $(0,0)$. [CHV23] informally suggested that the proof of strong anti-piracy security for the SDE construction of [CLLZ21], based on the ATI framework, could be extended to this correlated-challenge-bits setting. However, based on personal communication with the authors of [CHV23], it appears that directly establishing correlated-challenge-bits security within the ATI-based proof framework is nontrivial, and we are currently not aware of a direct proof in that framework.

$\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security is a special case of correlated-challenge-bits CPA anti-piracy security, corresponding to the joint distribution over the challenge bits that assigns probability $1/2$ to each of $(0,0)$ and $(1,1)$, and probability 0 to $(0,1)$ and $(1,0)$. We now show that the converse implication also holds.

Theorem 11.3. *Let* $\mathsf{SDE} = (\mathsf{Setup}, \mathcal{KG}, \mathsf{Enc}, \mathcal{D}ec)$ *be an SDE scheme. If* SDE *satisfies* $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$*-CPA anti-piracy security, then it also satisfies correlated-challenge-bits CPA anti-piracy security.*

Proof. Let $\mathcal{D}_{\mathsf{challbits}}$ be any distribution over $\{0,1\} \times \{0,1\}$. Let p_{ab} be the probability that $\mathcal{D}_{\mathsf{challbits}}$ outputs (a,b) for every (a,b). Let $\mathcal{A}_{\mathsf{sde}} = (\mathcal{A}, \mathcal{B}, \mathcal{C})$ be any adversary for the correlated-challenge-bits CPA anti-piracy security of SDE. We define the following events.

E_{suc}**:** $\mathsf{coin}'_{\mathcal{B}} = \mathsf{coin}_{\mathcal{B}}$ and $\mathsf{coin}'_{\mathcal{C}} = \mathsf{coin}_{\mathcal{C}}$ hold.

E_{ab}**:** $(\mathsf{coin}_{\mathcal{B}}, \mathsf{coin}_{\mathcal{C}}) = (a,b)$ holds for any $(a,b) \in \{0,1\} \times \{0,1\}$.

We have

$$\Pr\left[\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] = (p_{00}+p_{11}) \cdot \Pr[E_{\mathsf{suc}} | E_{00} \vee E_{11}] + (p_{01}+p_{10}) \cdot \Pr[E_{\mathsf{suc}} | E_{01} \vee E_{10}]. \quad (1)$$

We prove the following two lemmas.

Lemma 11.4. *If* SDE *satisfies* $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$*-CPA anti-piracy security, we have*

$$\Pr[E_{\mathsf{suc}} | E_{00} \vee E_{11}] \leq \max\left\{\frac{p_{00}}{(p_{00}+p_{11})}, \frac{p_{11}}{(p_{00}+p_{11})}\right\} + \mathsf{negl}.$$

Proof. Let $q_{00} = \frac{p_{00}}{(p_{00}+p_{11})}$ and $q_{11} = \frac{p_{11}}{(p_{00}+p_{11})}$. We consider the case where $q_{00} \geq q_{11}$. The other case can be proven similarly. We define E_{fail} as the event that $\mathsf{coin}'_{\mathcal{B}} \neq \mathsf{coin}_{\mathcal{B}}$ or $\mathsf{coin}'_{\mathcal{C}} \neq \mathsf{coin}_{\mathcal{C}}$ holds. We have

$$\begin{aligned}
\Pr[E_{\mathsf{suc}} | E_{00} \vee E_{11}] - q_{00} &= q_{00} \cdot \Pr[E_{\mathsf{suc}} | E_{00}] + q_{11} \cdot \Pr[E_{\mathsf{suc}} | E_{11}] - q_{00} \\
&= q_{11} \cdot \Pr[E_{\mathsf{suc}} | E_{11}] - q_{00} \cdot \Pr[E_{\mathsf{fail}} | E_{00}] \\
&\leq q_{11} \cdot (\Pr[E_{\mathsf{suc}} | E_{11}] - \Pr[E_{\mathsf{fail}} | E_{00}]) \\
&\leq \mathsf{negl}(\lambda).
\end{aligned}$$

The final inequality holds from the $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security of SDE since we have

$$\begin{aligned}
\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\mathcal{A}_{\mathsf{sde}}}(\lambda) = 1\right] - \frac{1}{2} &= \frac{1}{2} \cdot (\Pr[E_{\mathsf{suc}} | E_{11}] - \Pr[E_{\mathsf{fail}} | E_{00}]) \\
&\leq \mathsf{negl}(\lambda).
\end{aligned}$$

This completes the proof of Lemma 11.4. □

Lemma 11.5. *If* SDE *satisfies* $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$*-CPA anti-piracy security, we have*

$$\Pr[E_{\mathsf{suc}}|E_{01}\vee E_{10}]\leq \max\left\{\frac{p_{01}}{(p_{01}+p_{10})},\frac{p_{10}}{(p_{01}+p_{10})}\right\}+\mathsf{negl}.$$

Proof. Let $q_{01}=\frac{p_{01}}{(p_{01}+p_{10})}$ and $q_{10}=\frac{p_{10}}{(p_{10}+p_{10})}$. We consider the case where $q_{01}\geq q_{10}$. The other case can be proven similarly. Similarly to the proof of Lemma 11.4, we have

$$\Pr[E_{\mathsf{suc}}|E_{01}\vee E_{10}]-q_{01}\leq q_{10}\cdot(\Pr[E_{\mathsf{suc}}|E_{01}]-\Pr[E_{\mathsf{fail}}|E_{10}]).$$

To complete the proof, we show that $\Pr[E_{\mathsf{suc}}|E_{01}]-\Pr[E_{\mathsf{fail}}|E_{10}]\leq\mathsf{negl}(\lambda)$ based on the $\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}}$-CPA anti-piracy security of SDE. We define $\mathcal{A}'$ as the first stage adversary that runs in the same way as $\mathcal{A}$, except that $\mathcal{A}'$ sets the challenge message tuple as $(m'_{\mathcal{B},0},m'_{\mathcal{B},1},m'_{\mathcal{C},0},m'_{\mathcal{C},1})=(m_{\mathcal{B},0},m_{\mathcal{B},1},m_{\mathcal{C},1},m_{\mathcal{C},0})$. (Namely, the order of $m_{\mathcal{C},0}$ and $m_{\mathcal{C},1}$ is flipped.) We define the events $E'_{\mathsf{suc}},E'_{\mathsf{fail}},E'_{00},E'_{11}$ in $\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}'_{\mathsf{sde}}}(\lambda)$ similarly to the corresponding events in $\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}_{\mathsf{sde}}}(\lambda)$, where $\mathcal{A}'_{\mathsf{sde}}=(\mathcal{A}',\mathcal{B},\mathcal{C})$. Then, we have

$$\begin{aligned}\Pr\left[\mathsf{Exp}^{\mathsf{cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{iden\text{-}bit,ind\text{-}msg}},\mathcal{A}'_{\mathsf{sde}}}(\lambda)=1\right]-\frac{1}{2}&=\frac{1}{2}\cdot(\Pr[E'_{\mathsf{suc}}|E'_{00}]-\Pr[E'_{\mathsf{fail}}|E'_{11}])\\&=\frac{1}{2}\cdot(\Pr[E_{\mathsf{suc}}|E_{01}]-\Pr[E_{\mathsf{fail}}|E_{10}])\\&\leq\mathsf{negl}(\lambda).\end{aligned}$$

This completes the proof of Lemma 11.5. □

By combining Equation (1), Lemma 11.4, and Lemma 11.5, we obtain

$$\begin{aligned}\Pr\left[\mathsf{Exp}^{\mathsf{corrbits\text{-}cpa\text{-}anti\text{-}piracy}}_{\mathsf{SDE},\mathcal{D}_{\mathsf{challbits}},\mathcal{A}_{\mathsf{sde}}}(\lambda)=1\right]&\leq(p_{00}+p_{11})\cdot\max\left\{\frac{p_{00}}{(p_{00}+p_{11})},\frac{p_{11}}{(p_{00}+p_{11})}\right\}+\mathsf{negl}(\lambda)\\&\quad+(p_{01}+p_{10})\cdot\max\left\{\frac{p_{01}}{(p_{01}+p_{10})},\frac{p_{10}}{(p_{10}+p_{01})}\right\}+\mathsf{negl}(\lambda)\\&=\max\{p_{00},p_{11}\}+\max\{p_{10},p_{01}\}+\mathsf{negl}(\lambda)\\&=\max\{p_{00}+p_{01},p_{10}+p_{11},p_{00}+p_{10},p_{01}+p_{11}\}+\mathsf{negl}(\lambda)\\&=\max\{\Pr[\mathsf{coin}_{\mathcal{B}}=0],\Pr[\mathsf{coin}_{\mathcal{B}}=1],\Pr[\mathsf{coin}_{\mathcal{C}}=0],\Pr[\mathsf{coin}_{\mathcal{C}}=1]\}+\mathsf{negl}(\lambda)\\&=p^{\mathsf{triv}}_{\mathcal{D}_{\mathsf{challbits}}}+\mathsf{negl}(\lambda).\end{aligned}$$

This completes the proof of Theorem 11.3. □

Acknowledgment

We thank Prabhanjan Ananth and Fatih Kaleoglu for answering questions on [AKL23]. We also thank Quoc-Huy Vu for answering questions on [CHV23].

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 229–242. IEEE Computer Society, 2009. (Cited on page 3.)

[AB24] Prabhanjan Ananth and Amit Behera. A modular approach to unclonable cryptography. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 3–37. Springer, Cham, August 2024. (Cited on page 3, 5, 6, 7, 21, 22, 23.)

[ABH+25] Prabhanjan Ananth, Amit Behera, Zikuan Huang, Fuyuki Kitagawa, and Takashi Yamakawa. Copy-protection from unclonable puncturable obfuscation, revisited. In *EUROCRYPT 2025 (to appear)*, 2025. (Cited on page 7.)

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, volume 2285 of *Lecture Notes in Computer Science*, pages 323–334. Springer, 2002. (Cited on page 12.)

[AGKZ20] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *52nd ACM STOC*, pages 255–268. ACM Press, June 2020. (Cited on page 3.)

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 269–295. Springer, Cham, August 2019. (Cited on page 30.)

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 212–241. Springer, Cham, August 2022. (Cited on page 8, 10, 11, 13, 16.)

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 66–98. Springer, Cham, August 2023. (Cited on page 7, 10, 11, 12, 22, 31, 35, 38, 47.)

[AKY25] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous haar indistinguishability with applications to unclonable cryptography. In *ITCS 2025*, 2025. (Cited on page 7, 8, 10, 12, 13, 25.)

[ALL+21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 526–555, Virtual Event, August 2021. Springer, Cham. (Cited on page 5, 13, 14.)

[AP20] Shweta Agrawal and Alice Pellet-Mary. Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear FE. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 110–140. Springer, Cham, May 2020. (Cited on page 12.)

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. (Cited on page 37, 39.)

[BGI+12] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6:1–6:48, 2012. (Cited on page 12.)

[BGMZ18] James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry. Return of GGH15: Provable security against zeroizing attacks. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part II*, volume 11240 of *LNCS*, pages 544–574. Springer, Cham, November 2018. (Cited on page 12.)

[BHH+19] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of CCA security in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 61–90. Springer, Cham, December 2019. (Cited on page 31.)

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, June 9-12, 2020, Riga, Latvia*, volume 158 of *LIPIcs*, pages 4:1–4:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. (Cited on page 3, 6, 31.)

[BNZ25] John Bostanci, Barak Nehoran, and Mark Zhandry. A general quantum duality for representations of groups with applications to quantum money, lightning, and fire. In *STOC 2025*, 2025. (Cited on page 4.)

[BPW16] Nir Bitansky, Omer Paneth, and Daniel Wichs. Perfect structure on the edge of chaos - trapdoor permutations from indistinguishability obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 474–502. Springer, Berlin, Heidelberg, January 2016. (Cited on page 17.)

[ÇG24] Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part III*, volume 15366 of *LNCS*, pages 225–256. Springer, Cham, December 2024. (Cited on page 7.)

[ÇGLZR24] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Unbounded leakage-resilience and intrusion-detection in a quantum world. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part II*, volume 15365 of *LNCS*, pages 159–191. Springer, Cham, December 2024. (Cited on page 3.)

[CHV23] Céline Chevalier, Paul Hermouet, and Quoc-Huy Vu. Semi-quantum copy-protection and more. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 155–182. Springer, Cham, November / December 2023. (Cited on page 46, 47.)

[CHVW19] Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, and Hoeteck Wee. Matrix PRFs: Constructions, attacks, and applications to obfuscation. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 55–80. Springer, Cham, December 2019. (Cited on page 12.)

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584, Virtual Event, August 2021. Springer, Cham. (Cited on page 3, 4, 5, 6, 8, 12, 13, 15, 16, 17, 21, 22, 23, 24, 46.)

[CLPY25] Rohit Chatterjee, Xiao Liang, Omkant Pandey, and Takashi Yamakawa. The round complexity of black-box post-quantum secure computation. In *CRYPTO 2025*, 2025. (Cited on page 14.)

[CMP24] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, May 2024. (Cited on page 31.)

[CV22] Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6:791, sep 2022. (Cited on page 8, 17.)

[DQV+21] Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Succinct LWE sampling, random polynomials, and obfuscation. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part II*, volume 13043 of *LNCS*, pages 256–287. Springer, Cham, November 2021. (Cited on page 12.)

[FGH+12] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter W. Shor. Quantum money from knots. In Shafi Goldwasser, editor, *ITCS 2012*, pages 276–289. ACM, January 2012. (Cited on page 4.)

[GKW17] Rishab Goyal, Venkata Koppula, and Brent Waters. Lockable obfuscation. In Chris Umans, editor, *58th FOCS*, pages 612–621. IEEE Computer Society Press, October 2017. (Cited on page 5.)

[GZ20] Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Report 2020/877, 2020. (Cited on page 3, 6, 10, 15, 23.)

[KN23] Fuyuki Kitagawa and Ryo Nishimaki. One-out-of-many unclonable cryptography: Definitions, constructions, and more. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 246–275. Springer, Cham, November / December 2023. (Cited on page 7.)

[KSS21] Daniel M. Kane, Shahed Sharif, and Alice Silverberg. Quantum money from quaternion algebras. Cryptology ePrint Archive, Paper 2021/1294, 2021. (Cited on page 4.)

[LLQZ22] Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 294–323. Springer, Cham, November 2022. (Cited on page 3, 7.)

[LMZ23] Jiahui Liu, Hart Montgomery, and Mark Zhandry. Another round of breaking and making quantum money: How to not build it from lattices, and more. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 611–638. Springer, Cham, April 2023. (Cited on page 4.)

[MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding, 2021. (Cited on page 31.)

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. (Cited on page 3.)

[Win99] Andreas J. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999. (Cited on page 12.)

[WZ17] Daniel Wichs and Giorgos Zirdelis. Obfuscating compute-and-compare programs under LWE. In Chris Umans, editor, *58th FOCS*, pages 600–611. IEEE Computer Society Press, October 2017. (Cited on page 5.)

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Berlin, Heidelberg, August 2012. (Cited on page 40.)

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 408–438. Springer, Cham, May 2019. (Cited on page 4.)

[Zha20] Mark Zhandry. Schrödinger's pirate: How to trace a quantum decoder. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 61–91. Springer, Cham, November 2020. (Cited on page 5, 13, 14.)

[Zha22] Mark Zhandry. Personal communication. 2022. (Cited on page 23.)

[Zha23] Mark Zhandry. Quantum money from abelian group actions. Cryptology ePrint Archive, Paper 2023/1097, 2023. (Cited on page 4.)