Selective Opening Security in the Quantum Random Oracle Model, Revisited

Jiaxin Pan[1,2(✉)] and Runzhi Zeng[2]

[1] University of Kassel, Kassel, Germany
jiaxin.pan@uni-kassel.de
[2] Department of Mathematical Sciences, NTNU – Norwegian University of Science and Technology, Trondheim, Norway
runzhi.zeng@ntnu.no

Abstract. We prove that two variants of the Fujisaki-Okamoto transformations are selective opening (SO) secure against chosen-ciphertext attacks in the quantum random oracle model (QROM), assuming that the underlying public-key encryption scheme is one-wayness against chosen-plaintext attacks (OW-CPA). The two variants we consider are $\mathsf{FO}^{\not\perp}$ (Hofheinz, Hövelmanns, and Kiltz, TCC 2017) and $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ (Jiang et al., CRYPTO 2018). This is the *first* correct proof in the QROM.

The previous work of Sato and Shikata (IMACC 2019) showed the SO security of $\mathsf{FO}^{\not\perp}$ in the QROM. However, we identify a subtle gap in their work. To close this gap, we propose a new framework that allows us to adaptively reprogram a QRO with respect to multiple queries that are computationally hard to predict. This is a property that can be easily achieved by the classical ROM, but is very hard to achieve in the QROM. Hence, our framework brings the QROM closer to the classical ROM.

Under our new framework, we construct the *first tightly* SO secure PKE in the QROM using lossy encryption. Our final application is proving $\mathsf{FO}^{\not\perp}$ and $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ are bi-selective opening (Bi-SO) secure in the QROM. This is a stronger SO security notion, where an adversary can additionally corrupt some users' secret keys.

Keywords: Selective opening security · quantum random oracle model · Fujisaki-Okamoto transformation · tight security

1 Introduction

Public-key encryption (PKE) schemes are a central topic in cryptography. Their widely accepted security notion is indstinguishability against chosen-ciphertext attacks (IND-CCA), which states that confidentiality holds even if an adversary $\mathcal{A}$ can adaptively decrypt ciphertexts of its choice, except the challenge ciphertext. This is a security notion in the single-user, single-challenge setting,

Partially supported by the Research Council of Norway under Project No. 324235.

Q. Tang and V. Teague (Eds.): PKC 2024, LNCS 14603, pp. 92–122, 2024.
https://doi.org/10.1007/978-3-031-57725-3_4

namely, only one user's public key and one challenge ciphertext are exposed to an adversary.

Its multi-user, multi-challenge counterpart is an arguably more realistic setting. Selective opening (SO) security [3,6] is a notion in a multi-challenge setting, where an adversary is given multiple challenge ciphertexts under a single public key and aims at learning some information about the encrypted messages. On top of that, the adversary can open a subset of the challenge ciphertexts and reveal the corresponding messages and randomness used to generate those ciphertexts. SO security guarantees the confidentiality of the remaining unopened challenge ciphertexts. The recent notion, Bi-SO security [28], can be viewed as a stronger variant of the SO security in a multi-user setting, where the adversary is additionally given multiple users' public keys and it can corrupt some of their secret keys.

The aforementioned opening capability is motivated by the fact that cryptographic information is technically hard and expensive to erase in practice and an adversary may break into an encrypter's computer and learn the used randomness. In some applications, such as secure multi-party computation, it is even required to reveal the messages and randomness to make a user's computation publicly verifiable.

Technically speaking, it is challenging to construct a SO secure PKE. At a first glance, one may think that IND-CCA security implies SO security, since each ciphertext is generated using independent randomness. However, this is not true in general. We refer [23] for an overview and useful further reading. We highlight that, from a provable-security point of view, to answer an opening query, a security reduction should be able to 'explain' how it generates a challenge ciphertext by returning the randomness, but in many cases the reduction does not even know the randomness itself. Hybrid arguments are one of the examples, namely, the reduction cannot explain a ciphertext where a challenge is embedded. This is also the inherent reason why the recent updated proof of Sato and Shikata [36] is incorrect. In the recent years, a great amount of effort has been put into defining the right notion of SO security [3,6,23] and construct efficient SO-secure public-key encryption schemes [11,17–20,28].

Notions of Selective Opening Security. Currently, there are two types of notions have been studied in the literature, the indistinguishability-based (IND-based) ones (weak-IND-SO and full-IND-SO) [3,6] and the simulation-based (SIM-based) one (SIM-SO) [3]. They are not polynomial-time equivalent to each other. In this paper we only consider the SIM-based one. Informally, SIM-SO security states that for every SO adversary its output can be efficiently simulated by a simulator that sees only the opened messages. Unlike its IND-based counterpart, SIM-SO does not require the message distribution chosen by the adversary to be efficiently resamplable, conditioned on the opened messages (cf. [3]). Previous work showed that SIM-SO-CCA and full-IND-SO-CCA notions are the strongest SO security [2,6,23]. However, only SIM-SO-CCA has been realized so far [11,17–20]. It is similar for Bi-SO security, and only SIM-based notion is considered so far [28]. For simplicity, we will not write 'SIM' in the following.

Our Goal: Selective Opening Security in the QROM. SO secure PKE schemes are constructed in idealized models [18,19] and in the standard model [3,11,17,20]. Constructions in idealized models are more efficient and hence more relevant to practice. In particular, this paper considers schemes in the random oracle model (ROM).

The increasing threat that quantum computers can break most widely deployed public-key cryptosystems has driven research in the direction of building post-quantum secure public-key primitives, including PKE schemes and key encapsulation mechanisms (KEMs). Currently, the National Institute of Standards and Technology (NIST) in the US has come to a conclusion for the post-quantum standards. Kyber [37], NTRU [8], and Saber [9] were three finalists in the last round for the KEM/PKE category. They all use variants of the Fujisaki-Okamoto (FO) transformation [12–14,21]. It is interesting to consider whether these FO transformations are secure in the SO setting.

The FO transformation turns a relatively weak PKE (e.g. a One-Way CPA secure one) into an IND-CCA secure one. Recently, the FO transformation and its variants have been widely analyzed in both the classical ROM and the quantum (accessible) ROM (QROM) [21,24,27,34,38], but mostly with a focus on establishing IND-CCA security. An exception is the work of Heuer et al. [18] which studied the SO security of the FO transformation in the ROM.

For post-quantum security, proofs in the QROM are more desirable than those in the (classical) ROM, since it models quantum adversaries in a more realistic manner. In this setting, a quantum adversary interacts with a classical network, where "online" primitives (such as encryption) are classical, and computes "offline" primitives (such as hashing) on its own in superposition.

The work of Sato and Shikata [35] proved the SO security of the FO transformation in the QROM. To the best of our knowledge, this is the only work considers SO security in the QROM. However, we identified a subtle gap in their security proof[1]. Even worse, this gap cannot be closed, even if we relax the notion to the weaker, non-adaptive SO security as in [29], where an adversary is not allowed to adaptively open a challenge ciphertext, but commits all its opening indices after seeing the challenge ciphertexts. From a technical point of view, closing the gap in [35] requires new proof techniques in the QROM that allow a security reduction to adaptively reprogram multiple RO-queries in one security game without changing the view of an adversary, where the reprogrammed points are computationally hidden. This is a property not achievable by existing well-known techniques, such as [16,27,39,40]. We provide more discussion about it in Sect. 1.2.

1.1 Our Contributions

We revise the selective opening security in the QROM and prove that two "implicit rejection" variants of the FO transformation (namely, $\mathsf{FO}^{\not\perp}$ [24] and $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ [21]) are SO-CCA secure if the underlying PKE is one-way CPA (OW-CPA)

[1] The authors confirmed this to us.

secure in the QROM. Here we consider PKE schemes, namely, combining KEM $\mathsf{FO}^{\not\perp}$ (or $\mathsf{U}^{\not\perp}_{\mathsf{m}}$) with one-time pad and a message authentication code (MAC). The one with $\mathsf{FO}^{\not\perp}$ is the same scheme considered in [35], but ours is the first correct proof in the QROM. Since the proofs for $\mathsf{FO}^{\not\perp}$ and $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ are similar, we leave the one for $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ in our full version [33], and there we only prove the Bi-SO-CCA for $\mathsf{U}^{\not\perp}_{\mathsf{m}}$, since it implies SO-CCA security.

Our core technical contribution is a computational adaptive reprogramming framework in the QROM that enables a security reduction to *adaptively* and *simultaneously* reprogram polynomially many RO-queries which are computationally hidden from a quantum adversary. This is a property that cannot be provided by previous techniques in the QROM, such as the (adaptive) one-way to hiding (O2H) lemma [39,40], the semi-classical O2H lemma [1], and the measure-rewind-measure O2H lemma [27]. Our framework brings the QROM closer to the classical ROM, and it generalizes and improves the adaptive reprogramming framework by Grilo et al. [16].

Tight SO Security from Lossy Encryption in the QROM. Our second contribution is a tightly SO-CCA secure PKE from lossy encryption [3,22]. This is the *first* tight scheme in the QROM. A recent work of Pan, Wagner, and Zeng has constructed the first tightly multi-user (without corruptions), multi-challenge IND-CCA in the QROM [31], but it did not get extended to the (stronger) SO setting. Another related work is also due to Pan and Zeng [32], where a compact and tightly SO-CCA secure PKE is proposed in the classical random oracle model. However, it is unclear if it can be transformed to the QROM. Our result on tight SO security is established in the QROM, and it improves both aforementioned work.

Bi-SO Security of FO Transformations. As another application of our framework, we prove that the aforementioned variants of FO transformation, namely, $\mathsf{FO}^{\not\perp}$ and $\mathsf{U}^{\not\perp}_{\mathsf{m}}$, are furthermore Bi-SO-CCA secure [28] in the QROM, assuming OW-CPA security of the underlying PKE scheme. This notion is stronger than the SO-CCA security, since it additionally allows secret key corruption for the adversaries. The only known Bi-SO-CCA secure construction is in the classical ROM. Our work is the first one in the QROM.

Impacts on the NIST Finalists. The NIST finalists Kyber and Saber use tweaked verions of transformation $\mathsf{FO}^{\not\perp}$, and NTRU uses $\mathsf{U}^{\not\perp}_{\mathsf{m}}$. Hence, analysis of these FO transformations is more fundamental than directly analyzing these concrete schemes. Although our results strongly indicate that the NIST finalists are SO-CCA secure and Bi-SO-CCA in the QROM, we leave the formal proof of it as a future direction, and we are optimistic that our approaches can be extended naturally in achieving it.

1.2 Technical Details

We provide some details about our technical contribution, computational adaptive reprogramming framework.

Our Starting Point. The work of Heuer et al. [18] is the first one proving that practical PKEs via the OAEP and FO transformation are SO-CCA secure in the (classical) ROM. Their work considered the original FO transformation [14]. Motivated by Heuer et al.'s work, we can show that the combination of $\mathsf{FO}^{\not\perp}$ and one-time pad is SO-CPA secure in the classical ROM by adaptively reprogramming the ROs. Here we describe some key idea. Note that our final goal is SO-CCA, but for the simplicity of our discussion here, we only consider SO-CPA.

A ciphertext of message m in the $\mathsf{FO}^{\not\perp}$ transformation, (e, d), is defined as follow:

$$\begin{aligned} e &:= \mathsf{Enc}_0(\mathsf{pk}, r; G(r)) \quad \text{for} \quad r \xleftarrow{\$} \mathcal{M}' \\ d &:= H(r, e) \oplus m \end{aligned} \tag{1}$$

where Enc_0 is the randomized encryption algorithm of a OW-CPA secure PKE with message space $\mathcal{M}'$, $G(r)$ is the explicit randomness used in Enc_0, and G, H are two hash functions with suitable domains and ranges. Public and secret keys of $\mathsf{FO}^{\not\perp}$ is the same as those of the OW-CPA secure PKE, and the decryption is defined in the straightforward way. We refer Fig. 6 for the full description.

Efficient Openability in the ROM. To show the SO-CPA security, we require "efficient openability" of ciphertexts [3,11]. This property states that one can generate some ciphertexts and later they can be efficiently opened to arbitrary messages by using some trapdoor (in the standard model) or reprogramming ROs (in the ROM) in a suitable way. In the classical ROM, our ciphertexts (defined by Eq. (1)) have efficient openability. More precisely, a security reduction $\mathcal{R}$ can choose random r_i^*, R_i^*, and d_i^* and return the challenge ciphertexts $(\mathsf{Enc}_0(\mathsf{pk}, r_i^*; R_i^*), d_i^*)_{1 \le i \le \mu}$ to the SO-CPA adversary $\mathcal{A}$. For these challenge ciphertexts, the reduction $\mathcal{R}$ can open a ciphertext $(\mathsf{Enc}_0(\mathsf{pk}, r_i^*; R_i^*), d_i^*)$ to arbitrary message m_i by reprogramming $G(r_i^*) := R_i^*$ and $H(r_i^*, e_i^*) := d_i^* \oplus m_i$. Moreover, $\mathcal{R}$ will embed the OW-CPA challenge to one of the unopened ciphertexts. Here, r_i^* are only computationally hidden from the adversary.

For the SO-CPA security, the aforementioned reprogramming is required to be *adaptive*, since an adversary can submit an opening query adaptively. Moreover, a SO-CPA adversary can submit multiple opening queries in one security game or hybrid. Therefore, our reprogramming strategy should be able to reprogram multiple RO-queries in one security game. We call this last requirement as multi-point reprogramming. We stress that hybrid arguments are already not useful for SO security. This is because a standard hybrid argument will embed a OW-CPA challenge into the SO-CPA ciphertexts one-by-one. After it is embedded to the i-th ciphertext, $G(r_i^*)$ cannot be reprogrammed to R_i^*, since R_i^* is unknown to the reduction $\mathcal{R}$. Thus, the opening query cannot be correctly answered.

Existing Approaches in the QROM. Reprogramming a quantum (accessible) RO is highly non-trivial, since a query in superposition can be viewed as a query that might contain all possible input values at once. To correctly reprogram a value to a particular QRO query, it needs to measure and extract classical preimages of a quantum query, which will cause a change in the adversary's

view. Although many works have been done to provide reprogrammability in the QROM [1,16,27,39,40], reprogramming in the QROM is still much more challenging than in the ROM.

For the SO security, the situation is more complicated. Essentially, existing approaches (such as [1,16,27,39,40]) cannot easily achieve the requirements for SO security in the QROM. We use the semi-classical O2H lemma [1] as an example to elaborate on this. Fix a random set $S \subseteq \mathcal{X}$. Let $H, H' : \mathcal{X} \to \mathcal{Y}$ be two different ROs such that, for all $x \in \mathcal{X} \setminus S$, $H(x) = H'(x)$ (denoted by $H \setminus S = H' \setminus S$). The semi-classical O2H lemma states that a quantum adversary $\mathcal{A}$ cannot tell the difference between H and H' by giving only quantum access to them, unless $\mathcal{A}$ finds an element from S. Here set S needs to be defined before defining H and H'.

In the work of Sato and Shikata [35], their security proofs viewed S as the set containing all the randomness used in the opened ciphertexts (cf. the step between Game_1 and Game_2 in [35, Section 3.1] and the one between Game_5 and Game_6 in [35, Section 3.2]). Essentially, S is equivalent to the set of opening indices which are adaptively decided by the adversary $\mathcal{A}$. However, to use the semi-classical O2H lemma, S must be fixed at the beginning of the security game, even before generating the public key. Therefore, this technical gap in their proofs cannot be closed, and it will be the case, even if we consider the weaker, non-adaptive variant of SO security as in [29], namely, an adversary cannot adaptively open challenge ciphertexts, but commits to opening indices after receiving the challenge ciphertexts.

The recent measure-rewind-measure O2H lemma [27] has a similar flavor as the semi-classical O2H lemma, and it does not allow to define S adaptively. The adaptive O2H lemma [39] allow us to reprogram a single query adaptively. However, we require adaptive reprogramming multiple queries for SO security, since if we only reprogram wrt one opening query, an adversary can distinguish the simulation by opening multiple ciphertexts.

Our Approach. To solve the technical difficulties, we propose the computational adaptive reprogramming framework. It is more general than the algorithmic O2H lemma [39] and the adaptive reprogramming framework [16] in the sense that our framework allows a reduction to reprogram polynomial many RO queries in the QROM. Different to the work of Grilo et al., our reprogrammed points can be only computationally hidden from the adversary.

In a nutshell, our framework considers two security games, NonAda and Ada. The RO H' in NonAda will never be reprogrammed, but the RO H in Ada will be adaptively reprogrammed for multiple times according to the adversary's behavior. We require $H' \setminus S = H \setminus S$, but S can be modified adaptively by a security reduction. Intuitively, an adversary $\mathcal{A}$ can distinguish NonAda and Ada if it queries $x \in S$. This event can be detected easily in the classical setting, but is problematic in the quantum setting. Our high-level approach is to bound the probability of this event by randomly measuring $\mathcal{A}$. Details are given in Sect. 3. We stress that our approach is not a "hybrid argument" extension of the existing techniques. In fact, as pointed out by Bellare, Hofheinz, and Yilek [3], it is unknown if a simple hybrid argument is useful in proving SO security.

Very unfortunately, the latest revision[2] of [35] is a concrete example for why it does not work. The proof of their Lemma 1 is essentially a hybrid argument. A counterexample is simply: Imagine an adversary that always opens the first ciphertext, then their first hybrid always fails since the OPEN oracle will abort when the adversary opens the first ciphertext, and thus their hybrid argument cannot prove the SO security.

More Comparison with Related Work. Recently, Grilo et al. proposed the adaptive reprogramming framework [16] and used it to give a QROM proof for Fiat-Shamir's signatures. The main difference between our work and Grilo et al.'s work is that their framework requires the reprogramming points to have high statistical entropy, while our framework requires the reprogramming points are computationally hard to find (which cover the case of statistical entropy). When proving the SO security of the FO transformation, their framework cannot be used since the reprogramming points are computationally hidden by OW-CPA security of some underlying PKEs.

We also compare our framework to the measure-and-reprogram framework of Don, Fehr, and Majenz [10] and the lifting theorem in [41] that are used to prove security of the Fiat-Shamir (FS) signature in the QROM. In a nutshell, the difference between our frameworks is similar to that between the security proofs of the FO encryption and FS signature in the classical setting. More precisely, in the proof of FO encryption, we argue that it is infeasible for an adversary to learn the reprogramming points and thus we can reprogram the random oracle without changing the adversary's view. However, in the proof of FS signature, an adversary can learn the reprogramming points, since they are the hash values of signing messages and some (public) commitments of the Σ protocol. Hence, the measure-and-reprogram framework is conceptually different to us and cannot be used in proving SO or Bi-SO security in the QROM. The lifting theorem (cf. [41, Theorem 4.2]) has a similar flavor as the measure-and-reprogram framework.

Future Work. We leave exploring more applications of our computational adaptive reprogramming framework as a future direction, since reprogramming a (quantum) random oracle on multiple computationally hidden points is an interesting technique and we are optimistic that it may yield new applications. Moreover, we are optimistic that our approach can work for the simulatable DEM framework of SO secure PKEs. We leave a formal treatment of it as another future direction.

2 Preliminaries

Let n be an integer. $[n]$ denotes the set $\{1, ..., n\}$. Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite sets and $f : \mathcal{X} \to \mathcal{Y}$ be a function. $f(\mathcal{X}) := \{f(x)|x \in \mathcal{X}\}$. $x \xleftarrow{\$} \mathcal{X}$ denotes sampling a uniform element x from $\mathcal{X}$ at random. If S is a subset of $\mathcal{X}$, then $\mathcal{X}\backslash S$ denotes the set $\{x \in \mathcal{X}|x \notin S\}$. Let $\mathcal{A}$ be an algorithm. If $\mathcal{A}$ is probabilistic, then $y \leftarrow \mathcal{A}(x)$ means that the variable y is assigned to the output of $\mathcal{A}$ on input

[2] https://eprint.iacr.org/archive/2022/617/20230108:160413.

x. If $\mathcal{A}$ is deterministic, then we write $y := \mathcal{A}(x)$. We write $\mathcal{A}^{\mathcal{O}}$ to indicate that $\mathcal{A}$ has classical access to oracle $\mathcal{O}$. We write $\mathbf{T}(\mathcal{A}_0) \approx \mathbf{T}(\mathcal{A}_1)$ if the running times of $\mathcal{A}_0$ and $\mathcal{A}_1$ are polynomially close to each other. All (quantum) algorithms are (quantum) probabilistic polynomial time, unless we state it.

Games. We use code-based games [4] to define and prove security. We implicitly assume that Boolean flags are initialized to false, numerical types are initialized to 0, sets are initialized to $\emptyset$, while strings are initialized to the empty string ϵ. $\Pr[\mathbf{G}^{\mathcal{A}} \Rightarrow 1]$ denotes the probability that the final output $\mathbf{G}^{\mathcal{A}}$ of game $\mathbf{G}$ running an adversary $\mathcal{A}$ is 1. Let $\mathtt{Ev}$ be an (classical and well-defined) event. We write $\Pr[\mathtt{Ev} : \mathsf{G}]$ to denote the probability that $\mathtt{Ev}$ occurs during the game $\mathbf{G}$.

One-Time Message Authentication Code (MAC). We use MAC schemes that have one-time strong existential unforgeability under chosen message attack (otSUF-CMA) as building block. Let $\mathsf{MAC} := (\mathsf{Tag}, \mathsf{Vrfy})$ be an one-time MAC scheme with key space $\mathcal{K}^{\mathtt{mac}}$. The otSUF-CMA security game is given in Fig. 1.

Definition 1 (otSUF-CMA). *For a forger $\mathcal{F}$, its advantage against otSUF-CMA security of* MAC *is defined as*

$$\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{PKE}}(\mathcal{F}) := \Pr[\mathsf{otSUF\text{-}CMA}^{\mathcal{F}}_{\mathsf{MAC}} \Rightarrow 1]$$

MAC *is otSUF-CMA secure if for all $\mathcal{F}$,* $\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{PKE}}(\mathcal{F}) = \mathsf{negl}(\lambda)$.

One-time MAC schemes can be constructed by using pair-wise independent hash function family, and they are otSUF-CMA secure against *unbounded* adversaries. Here Tag cannot be queried with quantum superposition.

GAME $\mathsf{otSUF\text{-}CMA}^{\mathcal{F}}_{\mathsf{MAC}}$	Tag(m) // Only one query
01 $b := 0, K^{\mathtt{mac}} \xleftarrow{\$} \mathcal{K}^{\mathtt{mac}}$	07 $\tau \leftarrow \mathsf{Tag}(K^{\mathtt{mac}}, m)$
02 $(m^*, \tau^*) \leftarrow \mathcal{F}^{\mathrm{Tag}, \mathrm{Vrfy}}()$	08 $(m_0, \tau_0) := (m, \tau)$
03 **if** $(m^*, \tau^*) \neq (m_0, \tau_0)$	09 **return** τ
04 **and** $\mathsf{Vrfy}(K^{\mathtt{mac}}, m^*, \tau^*) = 1$	Vrfy(m, τ)
05 $b := 1$	10 **return** $\mathsf{Vrfy}(K^{\mathtt{mac}}, m, \tau)$
06 **return** b	

Fig. 1. Security games one-time MAC schemes

2.1 Public-Key Encryption

A Public Key Encryption (PKE) scheme PKE consists of three algorithms (KG, Enc, Dec) and a message space $\mathcal{M}$ that is assumed to be efficiently recognizable. The three algorithms work as follows:

– The key generation algorithm KG, on input the security parameter λ, outputs a public and secret key pair $(\mathsf{pk}, \mathsf{sk})$. pk also defines a finite randomness space $\mathcal{R} := \mathcal{R}(\mathsf{pk})$ and a ciphertext space $\mathcal{C} := \mathcal{C}(\mathsf{pk})$. For sake of simplicity, in this paper, we ignore the input λ and simply write the process as $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}$.

- The encryption algorithm Enc, on input pk and a message $m \in \mathcal{M}$, outputs a ciphertext $c \in \mathcal{C}$. We also write $c := \mathsf{Enc}(\mathsf{pk}, m; r)$ to indicate the randomness $r \in \mathcal{R}$ explicitly.
- The (deterministic) decryption algorithm Dec, on input sk and a ciphertext c, outputs a message $m' \in \mathcal{M}$ or a rejection symbol $\perp \notin \mathcal{M}$.

Definition 2 (PKE Correctness). *A PKE scheme* $\mathsf{PKE} := (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *is* $(1-\delta)$*-correct if*

$$\mathbb{E}\left[\max_{m \in \mathcal{M}} \Pr\left[\mathsf{Dec}(\mathsf{sk}, c) \neq m : c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)\right]\right] \leq \delta,$$

where the expectation is taken over $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}$ *and randomness of* Enc. PKE *has perfect correctness if* $\delta = 0$.

Definition 3 (Collision Probability of Key Generation). *Let*

$$\eta_{\mathsf{PKE}} := \max\left[\Pr\left[\mathsf{pk}_0 = \mathsf{pk}_1 : (\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{KG}, (\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KG}\right]\right]$$

be the collision probability of KG *of* PKE. *The maximum is taken over all* $\mathsf{pk}_0, \mathsf{pk}_1$. *In this paper, we assume that for any OW-CPA-secure* PKE, $\eta_{\mathsf{PKE}} = \mathsf{negl}(\lambda)$

Let $\mathsf{PKE} := (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ be a PKE scheme with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$. We focus on two security notions for PKE: onewayness under chosen-plaintext attacks (OW-CPA) and selective-opening security under chosen-ciphertext-attacks (SO-CCA).

Definition 4 ($\mathsf{OW\text{-}CPA}$). *For an adversary* $\mathcal{A}$, *its advantage against* $\mathsf{OW\text{-}CPA}$ *security of* PKE *is defined as*

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{A}) := \Pr\Big[m' = m^* : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}, m^* \xleftarrow{\$} \mathcal{M}, c^* \leftarrow \mathsf{Enc}(\mathsf{pk}, m^*), m' \leftarrow \mathcal{A}(\mathsf{pk}, c^*)\Big].$$

PKE *is* $\mathsf{OW\text{-}CPA}$ *secure if for all PPT adversaries* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{A}) = \mathsf{negl}(\lambda)$.

(Adaptive) Selective Opening Security. Selective Opening (SO) security preserves confidentiality even if an adversary opens the randomnesses of some ciphertexts. We use simulation-based approach to define SO security as in [18]. We consider the SO security against Chosen-Plaintext Attacks (SO-CPA) and Chosen-Ciphertext Attacks (SO-CCA), respectively.

We note that a non-adaptive variant of SO security has been used in [29], where an adversary must declare the opening index set I after receiving the challenge ciphertexts, while our SO security is *adaptive* in the sense that Open can be asked adaptively. Intuitively, our adaptive security is harder to achieve, since an adversary can change its opening queries after seeing the answers of previous ones.

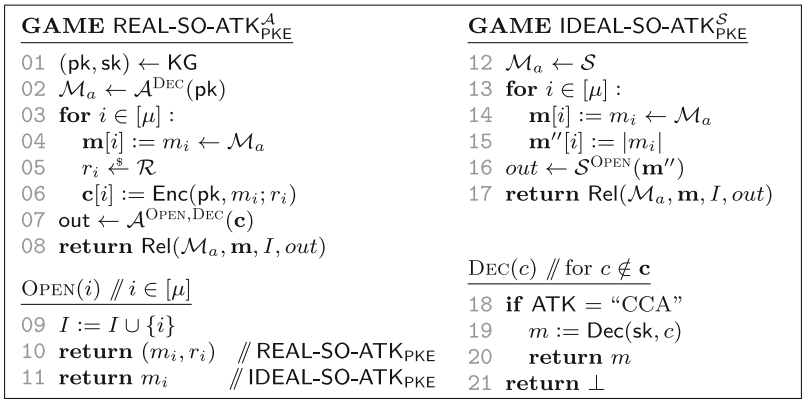

Fig. 2. The SO security games for PKE schemes.

Definition 5 (SO security). *Let* PKE *be a PKE scheme with message space* $\mathcal{M}$ *and randomness space* $\mathcal{R}$ *and* $\mathcal{A}$ *be an adversary against* PKE. *For security parameter* λ, $\mu := \mu(\lambda) > 0$ *is a polynomially bounded function. Let* Rel *be a relation. We consider two games defined in Fig. 2, where* $\mathcal{A}$ *is run in* REAL-SO-ATK$_{\mathsf{PKE}}$ *and a SO simulator* $\mathcal{S}$ *in* IDEAL-SO-ATK$_{\mathsf{PKE}}$. $\mathcal{M}_a$ *is a distribution over* $\mathcal{M}$ *chosen by* $\mathcal{A}$, *and* $\mathcal{A}$ *is not allowed to issue* Open *queries before it outputs* $\mathcal{M}_a$ *and receives challenge ciphertexts* $\mathbf{c}$. *Messages sampled from* $\mathcal{M}_a$ *may be dependent on each other.* Dec *is not available in SO-CPA security.*

We define the SO-ATK (ATK = 'CPA' or 'CCA') advantage function

$$\mathsf{Adv}^{\mathsf{SO\text{-}ATK}}_{\mathsf{PKE}}(\mathcal{A},\mathcal{S},\mu,\mathsf{Rel}) := \left|\Pr\left[\mathsf{REAL\text{-}SO\text{-}ATK}^{\mathcal{A}}_{\mathsf{PKE}} \Rightarrow 1\right] - \Pr\left[\mathsf{IDEAL\text{-}SO\text{-}ATK}^{\mathcal{S}}_{\mathsf{PKE}} \Rightarrow 1\right]\right|,$$

PKE *is SO-ATK secure if, for every adversary* $\mathcal{A}$ *and every PPT relation* Rel, *there exists a simulator* $\mathcal{S}$ *such that* $\mathsf{Adv}^{\mathsf{SO\text{-}ATK}}_{\mathsf{PKE}}(\mathcal{A},\mathcal{S},\mu,\mathsf{Rel}) \leq \mathsf{negl}(\lambda)$.

(Adaptive) Bi-Selective-Opening Security. In this paper, we also consider a stronger SO security definition: Bi-SO-ATK [28]. This security definition considers a multi-user setting and allows the adversary to corrupt some users (namely, obtains their secret keys) adaptively. The Bi-SO-ATK definition in [28] is non-adaptive, that is, the SO adversary is required to tell the game simulator which users it wants to corrupted and which challenge ciphertexts it wants to open at once. In this paper, we enhance the security definition to be adaptive. The adversary can adaptively issues Open queries and Corrupt queries in any order. The enhanced definition is also simulation-based. If $\mathcal{A}$ corrupts a user j, then the messages of challenge ciphertexts that encrypted by j are also revealed (see Items 15 and 16).

Definition 6 (Bi-SO security). *Let* PKE *be a PKE scheme and* $\mathcal{A}$ *be a Bi-SO adversary against* PKE. *For security parameter* λ, *let* $\mu := \mu(\lambda)$ *and* $p := p(\lambda)$

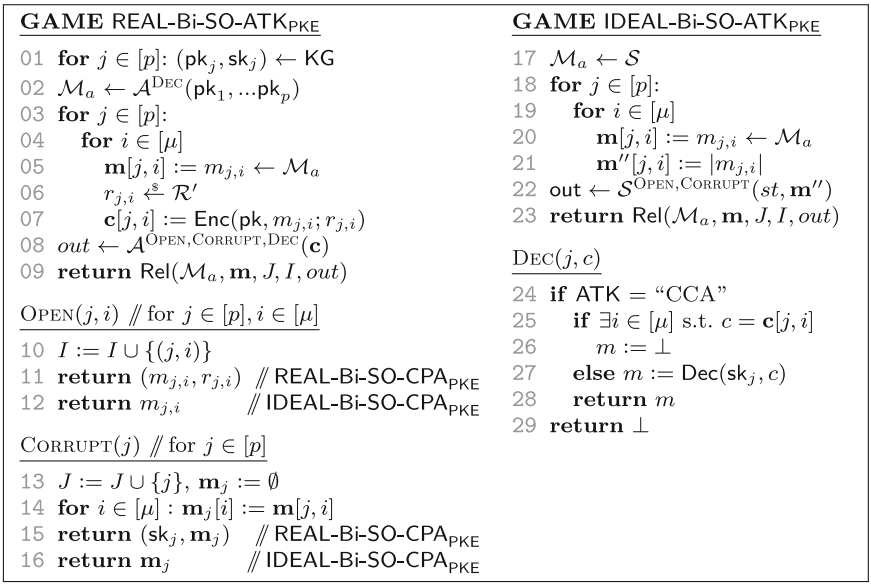

Fig. 3. The Bi-SO-ATK security game for PKE schemes

that are both polynomially bounded. Let Rel *be a relation. We consider two games defined in Fig. 3, where* $\mathcal{A}$ *is run in* REAL-Bi-SO-ATK$_{\mathsf{PKE}}$ *and a Bi-SO simulator* $\mathcal{S}$ *in* IDEAL-Bi-SO-ATK$_{\mathsf{PKE}}$. $\mathcal{M}_a$ *is a distribution over* $\mathcal{M}$ *chosen by* $\mathcal{A}$*, and* $\mathcal{A}$ *is not allowed to issue* OPEN *or* CORRUPT *queries before it outputs* $\mathcal{M}_a$ *and receives challenge ciphertexts* $\mathbf{c}$*. Messages sampled from* $\mathcal{M}_a$ *may be dependent on each other.* DEC *is not available in Bi-SO-CPA security.*

We define the Bi-SO-ATK (ATK = 'CPA' or 'CCA') advantage function

$$\mathsf{Adv}^{\text{Bi-SO-ATK}}_{\mathsf{PKE}}(\mathcal{A}, \mathcal{S}, p, \mu, \mathsf{Rel}) := \left| \Pr\left[\text{REAL-Bi-SO-ATK}^{\mathcal{A}}_{\mathsf{PKE}} \Rightarrow 1\right] - \Pr\left[\text{IDEAL-Bi-SO-ATK}^{\mathcal{S}}_{\mathsf{PKE}} \Rightarrow 1\right] \right|.$$

PKE *is adaptive Bi-SO-ATK secure if, for any adversary* $\mathcal{A}$ *and PPT relation* Rel*, there exists a simulator* $\mathcal{S}$ *such that* $\mathsf{Adv}^{\text{Bi-SO-ATK}}_{\mathsf{PKE}}(\mathcal{A}, \mathcal{S}, p, \mu, \lambda) = \mathsf{negl}(\lambda)$.

SECURITY IN THE QUANTUM RANDOM ORACLE MODEL. The (Bi-)SO security of PKE schemes containing hash functions can be analyzed in the quantum random oracle model (cf. Sect. 2.2). If we model a hash function H as quantum random oracle, then the adversary $\mathcal{A}$ has quantum access to H during the SO security games (e.g., Fig. 7).

2.2 Quantum Computation

We refer to [30] for detailed background about quantum mechanism. Here we only recall some necessary notations and lemmas.

Pure quantum states can be described by qubits. For a λ-bit-string x, $|x\rangle \in \mathbb{C}^{2^\lambda}$ denotes the (pure) quantum state of x encoded in the standard computational basis. Quantum register is used to store multiple qubits. In this paper, we assume that any polynomially long object x can be encoded as a (unique) bit string, and if we "store" x in a quantum register X, $|x\rangle$ is the quantum state of this register. A λ-qubits quantum superposition state $|\phi\rangle$ can be written as $\sum_{x\in\{0,1\}^\lambda} \alpha_x|x\rangle$ where $\sum_{x\in\{0,1\}^\lambda} |\alpha_x|^2 = 1$.

By performing measurement on a quantum state, we obtain classical information about the state, and the state collapses after measurement. Let $|x\rangle$ be an quantum state, $x' \leftarrow \mathsf{Measure}(|x\rangle)$ denote the process that $|x\rangle$ is measured and the measurement outcome is x'. We assume that all measurement are performed with respect to the standard computational basis.

Let $\mathcal{O} : \mathcal{X} \to \mathcal{Y}$ be an random oracle with sets $\mathcal{X}, \mathcal{Y}$. We implicitly assume that the elements in $\mathcal{X}$ and $\mathcal{Y}$ are expressed as bit strings. In quantum random oracle model (QROM) [7], the oracle $\mathcal{O}$ are described as the unitary transformation $U_\mathcal{O} : |x\rangle|y\rangle \to |x, y \oplus \mathcal{O}(x)\rangle$, and the adversary can query random oracles on quantum states. For an quantum adversary $\mathcal{A}$, the notation $\mathcal{A}^{|\mathcal{O}\rangle}$ indicates that $\mathcal{A}$ has quantum access to the $U_\mathcal{O}$. Without loss of generality, we directly write $\mathcal{O}$ to denote the unitary $U_\mathcal{O}$.

In this paper, we say an event is classical if it can be determined by only using classical algorithm (namely, without using any quantum mechanism).

Lemma 1 gives a probabilistic bound for adversary (has a quantum access to oracles) to distinguish $h(s, \cdot)$ and h', where s is secret, h and h' are QRO and have the same image set. When the image is large enough, the adversary cannot distinguish these two oracles.

Lemma 1 (Lemma 2.2 in [34]). *Let k be an integer. Let $h : \mathcal{X}' \times \mathcal{X} \to \mathcal{Y}$ and $h' : \mathcal{X} \to \mathcal{Y}$ be two independent random oracles. If an unbounded time quantum adversary $\mathcal{A}$ that queries h at most q_h times, then we have*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}^{|h\rangle,|h(s,\cdot)\rangle}() \middle| s \xleftarrow{\$} \mathcal{X}'\right] - \Pr\left[1 \leftarrow \mathcal{A}^{|h\rangle,|h'\rangle}()\right]\right| \leq 2q_h/\sqrt{|\mathcal{X}'|}$$

3 Computational Adaptive Reprogramming in the QROM

We propose a computational adaptive reprogramming framework in the QROM. In our full version [33], we review Unruh's adaptive O2H lemma [39] and discuss why our lemma (namely, Lemma 2) cannot be proved by using hybrid arguments of Unruh's adaptive O2H lemma.

Let $\mathcal{A}$ be an adversary that has quantum access to $\mathcal{H} : \mathcal{X} \to \mathcal{Y}$ and takes in_0 as input and terminates by outputting out_n. During its execution, $\mathcal{A}$ outputs some out_i and then takes in_{i+1} as input ($0 \leq i \leq n-1$). We view $\mathcal{A}$ as a $(n+1)$-stage adversary, $(\mathcal{A}_0, ..., \mathcal{A}_n)$, where $\mathcal{A}_i$ takes in_i as input and outputs out_i. Here $\mathsf{in}_0, \mathsf{out}_0, \mathsf{in}_1, ..., \mathsf{in}_n$, and out_n can be arbitrary classical information. In this paper, we consider post-quantum setting where adversaries have quantum access to hash functions. The classical information $\mathsf{in}_0, \mathsf{out}_0, \mathsf{in}_1, ..., \mathsf{in}_n, \mathsf{out}_n$ capture the

interaction between $\mathcal{A}$ and the security game simulator, and they will be specified in a concrete use of our framework.

We write $\mathcal{A} = (\mathcal{A}_0, ..., \mathcal{A}_n)$ to divide $\mathcal{A}$ into $n+1$ stages for better analysis. By writing $\mathsf{out}_i \leftarrow \mathcal{A}_i(\mathsf{in}_i)$ we mean that at stage i $\mathcal{A}$ receives input in_i and outputs out_i at the end of the stage. The index indicates the stage number of $\mathcal{A}$. So, all $\mathcal{A}_i$ are the same adversary $\mathcal{A}$ in different stages, and they share the quantum registers of $\mathcal{A}$. The same notation (of dividing $\mathcal{A}$ into different stages) is also used in Unruh's adaptive O2H lemma [39].

Games NonAda and Ada (as in Fig. 4) are used to define our framework. $\mathcal{A}$ has quantum access to $\mathcal{H}$ which is either H or H_i. In NonAda, H will never get reprogrammed, while in Ada different stages of $\mathcal{A}$ will have access to different ROs H_i. That is, $\mathcal{A}_i$ queries H_i, and according to $\mathcal{A}_i$'s output out_i H_i will be reprogrammed and become H_{i+1} (cf. Items 07, 17 and 18). To formalize this, we define three algorithms $\mathtt{INIT}$, $\mathsf{F}_\mathbf{s}$, and $\mathsf{Repro}_\mathbf{s}$ in Fig. 4 as:

- $\mathtt{INIT}$ outputs $((\mathbf{s}, \mathsf{in}_0), \mathsf{H}, \mathsf{H}_0)$ (cf. Items 01 and 11), where $\mathbf{s}$ is some parameter that used in a security reduction, in_0 is the initial input to $\mathcal{A}$, and H and H_0 are two random oracles. Here the tuple $((\mathbf{s}, \mathsf{in}_0), \mathsf{H}, \mathsf{H}_0)$ may have an arbitrary joint distribution.
- $\mathsf{F}_\mathbf{s}$ takes out_i as input and computes $(\mathsf{in}_{i+1}, \mathsf{in}'_{i+1})$, where in_{i+1} is the input to $\mathcal{A}_{i+1}$ and in'_{i+1} is the information for reprogramming H_i. Here in'_{i+1} is used to capture the fact that $\mathcal{H}$ can be reprogrammed according to $\mathcal{A}_i$'s behavior, and the algorithm $\mathsf{Repro}_\mathbf{s}$ (described below) will take it as input. To make our lemma general and useful for a wider class of applications, we only require that $\mathsf{F}_\mathbf{s}$ does not have access to random oracles.
- $\mathsf{Repro}_\mathbf{s}$ is defined to reprogram $\mathcal{H}$ in Ada (cf. Item 17). $\mathsf{Repro}_\mathbf{s}$ takes in'_i and H_{i-1} as input. It returns a random oracle H_i which is from reprogramming H_{i-1}. The concrete reprogramming operation of $\mathsf{Repro}_\mathbf{s}$ depends on the concrete use of our framework. Here we only require $\mathsf{Repro}_\mathbf{s}$ to be deterministic.

Let S_i be a set such that $\mathsf{H} \backslash S_i = \mathsf{H}_i \backslash S_i$ (namely, for all $x \in \mathcal{X}$, if $x \in S_i$, then $\mathsf{H}(x) \neq \mathsf{H}_i(x)$). $\mathcal{A}$ can only distinguish Ada and NonAda, if it queries a $x \in S_i$ (where $i \in \{0, ..., n\}$). Since $\mathcal{A}$'s QRO queries are superposition states, we need to define extractor $\mathcal{B}_i$ as in Fig. 5 to bound the difference between NonAda and Ada. This follows the works in [27,34,39]. Lemma 2 formalizes our framework. Its proof is postponed to our full version [33].

Lemma 2. *Let $\mathcal{A}$ be an adversary that can be divided into $(n+1)$ stages as in Fig. 4 and has quantum access to random oracle $\mathcal{H}$ ($= \mathsf{H}$ in NonAda or H_i in Ada). Let Ev be a classical event that may be raised by $\mathcal{A}$ in NonAda or Ada. Suppose that $\mathcal{A}$ queries $\mathcal{H}$ at most q_i times in its i-th stage and at most $q := q_0 + \cdots q_n$ times in total during the game. Then for all algorithms $\mathtt{INIT}$, $\mathsf{F}_\mathbf{s}$, and $\mathsf{Repro}_\mathbf{s}$ (as described earlier), there exists adversaries $\mathcal{B}_i$ for $i \in \{0, ..., n\}$ (shown in Fig. 5) such that*

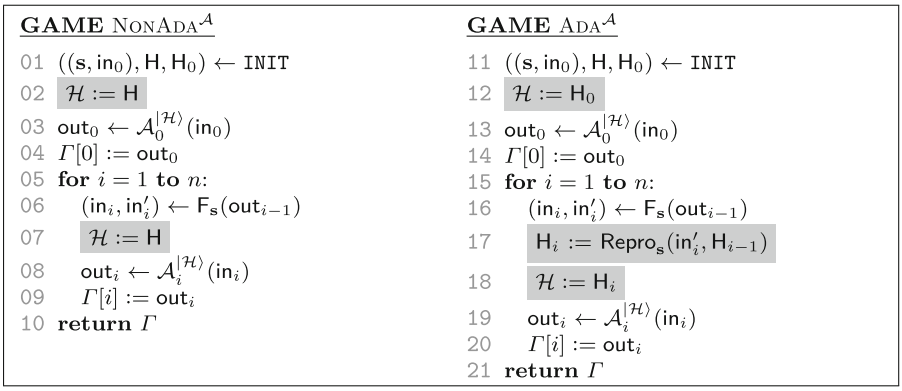

Fig. 4. Games NonAda and Ada used in Lemma 2. The main difference between two games is highlighted with gray box. In both games, $\mathcal{A}$ is divided into $n+1$ stages, namely, $(\mathcal{A}_0, ..., \mathcal{A}_n)$. The input and output of $\mathcal{A}$ in each stage are classical information because we consider post-quantum settings. The list Γ stores $\mathcal{A}$'s outputs in each stage. F_s is a deterministic algorithm that provides inputs for each stage of $\mathcal{A}$. $\mathsf{Repro}_\mathsf{s}$ is a deterministic algorithm that reprograms QROs. For a concise presentation, we assume that $\mathcal{A}_i$ takes $\mathcal{A}_{i-1}$'s final state as its initial state. In our framework, H_0 can be different to H.

$$\left|\Pr\left[\mathsf{Ev} : \text{NonAda}^{\mathcal{A}}\right] - \Pr\left[\mathsf{Ev} : \text{Ada}^{\mathcal{A}}\right]\right| \leq \sum_{k=0}^{n}\sum_{i=0}^{k} 2q_i\sqrt{\Pr\left[x' \leftarrow \mathcal{B}_i^{\mathcal{H}} \ s.t.\ x' \in S_i : \text{Ada}^{\mathcal{B}_i}\right]}, \quad (2)$$

where S_i is a set such that $\mathsf{H}\backslash S_i = \mathsf{H}_i\backslash S_i$. Such an S_i is defined by the operations in $\mathsf{Repro}_\mathsf{s}$. $\Pr\left[\mathsf{Ev} : \text{NonAda}^{\mathcal{A}}\right]$ *and* $\Pr\left[\mathsf{Ev} : \text{Ada}^{\mathcal{A}}\right]$ *are the probabilities that $\mathcal{A}$ triggers Ev in* NonAda *and in* Ada*, respectively.*

Discussions on Lemma 2. In Ada, reprogramming the RO is captured by algorithm $\mathsf{Repro}_\mathsf{s}$. How the reprogramming is done will be specified in a concrete use of Lemma 2. This is to make our framework general. The difference between NonAda and Ada is that between H and H_i caused by $\mathsf{Repro}_\mathsf{s}$.

Concretely, in i-th stage, $\mathsf{Repro}_\mathsf{s}$ will define a set S_i such that $\mathsf{H}\setminus S_i = \mathsf{H}_i \setminus S_i$. For any $k \in \{0, ..., n\}$, if $\mathcal{A}$ queries $\mathcal{H}$ with an $x \in \cup_{0\le i\le k} S_k$ before the end of its k-th stage, then $\mathcal{A}$ can distinguish NonAda and Ada. To bound this in the quantum setting, our approach is to randomly measure $\mathcal{A}$'s queries to $\mathcal{H}$, which is captured by $\mathcal{B}_i$ (in Fig. 5). The advantage of $\mathcal{A}$ distinguishing NonAda and Ada is bounded by the probability that $\mathcal{B}_i$'s output falls into S_i.

More Discussions on F and Repro in Fig. 4. When defining our framework, we do not make any requirement on the efficiencies of F_s and $\mathsf{Repro}_\mathsf{s}$. However, when we use this framework to construct (efficient) reduction, F_s and $\mathsf{Repro}_\mathsf{s}$ are required to be efficient (namely, running in quantum probabilistic polynomial time) and the description of QRO is polynomially bounded [7,25,42]. For

$\mathcal{B}_i^{|\mathcal{H}\rangle}(\mathsf{in}_0)$: // $\mathcal{H}$ is defined as in ADA

$t^* \xleftarrow{\$} [q_i]$
for $j = 0$ **to** $i-1$:
  $\mathsf{out}_j \leftarrow \mathcal{A}_j^{|\mathcal{H}\rangle}(\mathsf{in}_j)$
  Output out_j to ADA
  Receive in_{j+1} from ADA
Run $\mathcal{A}_i^{|\mathcal{H}\rangle}(\mathsf{in}_i)$ until it issues t^*-th quantum query to $\mathcal{H}$
Let $|\varphi\rangle$ be the t^*-th quantum query to $\mathcal{H}$
$x' \leftarrow \mathsf{Measure}(|\varphi\rangle)$
return x'

Fig. 5. Algorithm $\mathcal{B}_i$ (used in Lemma 2) plays Game ADA (where $i \in [n]$). $\mathcal{B}_i$ proceeds identically with $(\mathcal{A}_1, ..., \mathcal{A}_i)$, except that $\mathcal{B}_i$ measures the t^*-th QRO query issued by $\mathcal{A}_i$ and then outputs the measurement outcome.

instance, we can use a $2q$-independent hash function [42] and the list of reprogramming points (which are inputs to the hash and polynomial-bounded) to describe this QRO.

WHY OUR FRAMEWORK COVERS THE WORK OF GRILO ET AL. By specifying $\mathsf{F}_\mathbf{s}$ and $\mathsf{Repro}_\mathbf{s}$, we can describe Grilo et al.'s framework using our framework (though the bound of our framework is less tight than Grilo et al.'s one). In Grilo et al.'s framework [16], the i-th output of $\mathcal{A}$ is a distribution $\mathsf{out}_i := p_i$. $\mathsf{F}_\mathbf{s}$ can be defined as, on input p_i, it samples a reprogramming point (x_i, x_i') from p_i and an independently random y_i and outputs $(\mathsf{in}_{i+1} := (x_i, x_i'), \mathsf{in}'_{i+1} := (x_i, x_i', y_i))$[3]. $\mathsf{Repro}_\mathbf{s}$ can be defined as, on input $\mathsf{in}'_{i+1} := (x_i, x_i', y_i)$, it reprograms the QRO $\mathcal{H} := \mathcal{H}[(x_i, x_i') \to y_i]$ and returns the reprogrammed QRO. Their framework implicitly requires that the probability bound for $\mathcal{A}$ to learn x_i, x_i' (before seeing them) is information-theoretic. Namely, p_i should have enough entropy. Some important advantage of our framework, compared with Grilo et al.'s [16], are as follows:

- Grilo et al.'s framework requires the reprogramming points have high entropy and it is hard to find them even for unbounded adversary, while our framework does not have such restrictions. If $\mathcal{A}$ is a QPPT adversary, our framework provides efficient extractors $\mathcal{B}_i$'s to bound the difference of $\mathcal{A}$ in NONADA and ADA. In our proofs, we need to instantiate $\mathtt{INIT}, \mathsf{F}_\mathbf{s}$, and $\mathsf{Repro}_\mathbf{s}$ efficiently. This $\mathcal{B}_i$ can be used to do a reduction in breaking some computational hard problem, for instance, the OW-CPA security. However, the Grilo et al. framework cannot be used to do any efficient reduction.
- Our framework allows NONADA and ADA to start from different QROs, while the Grilo et al. framework starts from the same QRO. Starting from different QROs allows us to consider more complicated cases of adaptive reprogramming. All security proofs in this paper are examples for this, and for SO and Bi-SO security we require this.

[3] The randomness for sampling can be included in $\mathbf{s}$, since it is captured by the game simulator.

– Our framework also supports delayed analysis. In some complicated proofs, the difference between non-reprogramming and reprogramming games cannot be immediately bounded, and we may need extra game sequences to postpone such a bound. Our framework supports delayed analysis, since we can use extra game sequences to bound the winning probability of $\mathcal{B}_i$ (i.e. $\mathcal{B}_i$ outputs $x \in S_i$). In particular, our tightly-secure SO-CCA PKE scheme in Sect. 5 requires delayed analysis.

4 Selective Opening Security of Fujisaki-Okamoto's PKE in the QROM

We prove the selective-opening (SO) security of two Fujisaki-Okamoto(FO)-style PKE schemes in the QROM. As a warm-up, our first scheme is SO secure against chosen-plaintext attacks (SO-CPA), and the scheme follows the idea of hybrid encryption. It offers a simple example about how to use our framework. Our second scheme is SO secure against chosen-ciphertext attacks (SO-CCA). It is the same scheme as in [35, Section 3.2], but our proof is showing adaptive SO-CCA security, while the original proof in [35] has a subtle gap and the gap still exists even if we consider the non-adaptive security notion (cf. discussion in Introduction).

In both schemes, let $\mathsf{PKE} := (\mathsf{KG}_0, \mathsf{Enc}_0, \mathsf{Dec}_0)$ be a $(1-\delta)$-correct PKE scheme with message space $\mathcal{M}'$, ciphertext space $\mathcal{C}'$, and randomness space $\mathcal{R}'$. Let $G : \mathcal{M}' \to \mathcal{R}'$ be a hash function.

4.1 Selective Opening Security Against Chosen-Plaintext Attacks

Let $H : \mathcal{M}' \times \mathcal{C}' \to \mathcal{M}$ be a hash function. Our first PKE scheme $\mathsf{wPKE} = (\mathsf{wKG}, \mathsf{wEnc}, \mathsf{wDec})$ (where 'w' stands for weak) with message space $\mathcal{M}$ and is defined as in Fig. 6. Theorem 1 states that wPKE is adaptive SO-CPA secure when modeling G and H as QROs.

$\underline{\mathsf{wKG}}$	$\underline{\mathsf{wEnc}(\mathsf{pk}, m \in \mathcal{M})}$	$\underline{\mathsf{wDec}(\mathsf{sk}, (e,d))}$
01 $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KG}_0$	03 $r \xleftarrow{\$} \mathcal{M}'$	08 $r' := \mathsf{Dec}_0(\mathsf{sk}, e)$
02 **return** $(\mathsf{pk},\mathsf{sk})$	04 $e := \mathsf{Enc}_0(\mathsf{pk}, r; G(r))$	09 $K := H(r', e)$
	05 $K := H(r, e)$	10 $m := K \oplus d$
	06 $d := K \oplus m$	11 **return** m
	07 **return** (e, d)	

Fig. 6. A SO-CPA secure PKE scheme $\mathsf{wPKE} = (\mathsf{wKG}, \mathsf{wEnc}, \mathsf{wDec})$

Theorem 1. *If* PKE *is OW-CPA secure, then* wPKE *in Fig. 6 is adaptive SO-CPA secure (Definition 5). Concretely, for security parameter* λ *and*

Game $\mathbf{G}_0$-$\mathbf{G}_3$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}_0$
$\mathcal{M}_a \leftarrow \mathcal{A}^{|G \times H\rangle}(\mathsf{pk})$
for $i \in [\mu]$
  $\mathbf{m}[i] := m_i \leftarrow \mathcal{M}_a, r_i \xleftarrow{\$} \mathcal{R}'$
  $R_i := G(r_i)$
  $R_i \xleftarrow{\$} \mathcal{R}'$ // $\mathbf{G}_2$-$\mathbf{G}_3$
  $e_i := \mathsf{Enc}_0(\mathsf{pk}, r_i; R_i)$
  $K_i := H(r_i, e_i)$ // $\mathbf{G}_0$-$\mathbf{G}_1$
  $K_i \xleftarrow{\$} \mathcal{M}$ // $\mathbf{G}_2$
  $d_i := K_i \oplus m_i$ // $\mathbf{G}_0$-$\mathbf{G}_2$
  $d_i \xleftarrow{\$} \mathcal{M} \backslash \{d_1, ..., d_{i-1}\}$ // $\mathbf{G}_3$
  $\mathbf{c}[i] := (e_i, d_i)$
if $\exists i \neq j$ s.t. $K_i = K_j$ // $\mathbf{G}_1$-$\mathbf{G}_2$
  abort // $\mathbf{G}_1$-$\mathbf{G}_2$
$out \leftarrow \mathcal{A}^{\textsc{Open}, |G \times H\rangle}(\mathbf{c})$
return $\mathsf{Rel}(\mathcal{M}_a, \mathbf{m}, I, out)$

$\textsc{Open}(i)$
$I := I \cup \{i\}$
return (m_i, r_i)

$H(r, e)$
if $\exists i \in I$ s.t. $(r, e) = (r_i, e_i)$ // $\mathbf{G}_2$-$\mathbf{G}_3$
  return K_i // $\mathbf{G}_2$
  return $d_i \oplus m_i$ // $\mathbf{G}_3$
return $h(r, e)$

$G(r)$
if $\exists i \in I$ s.t. $r = r_i$ // $\mathbf{G}_2$-$\mathbf{G}_3$
  return R_i // $\mathbf{G}_2$-$\mathbf{G}_3$
return $g(r)$

Fig. 7. Games $\mathbf{G}_0$-$\mathbf{G}_3$ for proving Theorem 1.

$\mu := \mu(\lambda)$ (polynomially bounded), for any SO-CPA adversary $\mathcal{A}$ and relation Rel*, there exist a simulator $\mathcal{S}$ and an adversary $\mathcal{B}'$ such that $\mathbf{T}(\mathcal{S}) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}')$ and*

$$\mathsf{Adv}^{\mathsf{SO\text{-}CPA}}_{\mathsf{wPKE}}(\mathcal{A}, \mathcal{S}, \mu, \mathsf{Rel}) \leq 2(n_{\mathrm{O}}+1)^2 q \sqrt{2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}')} + \frac{\mu^2}{|\mathcal{M}|} + \frac{\mu^2}{|\mathcal{M}'|} + \frac{2\mu q}{\sqrt{|\mathcal{M}'|}},$$

where μ, q_G, q_H, and n_{O} are the maximum numbers of $\mathcal{A}$'s challenge ciphertexts, $\mathcal{A}$'s queries to G, H, and Open*, respectively. $q = q_G + q_H$.*

Proof. Let $h : \mathcal{M}' \times \mathcal{C}' \to \mathcal{M}$ and $g : \mathcal{M}' \to \mathcal{R}'$ be two internal quantum-accessible random oracles that are used to respond queries to H and G, respectively. Following the convention in [25,34], in our proof we simulate H and G using two internal quantum-accessible random oracles $h : \mathcal{M}' \times \mathcal{C}' \to \mathcal{M}$ and $g : \mathcal{M}' \to \mathcal{R}'$, respectively.

Our proof consists a sequence of games defined in Fig. 7. We will use our framework in Sect. 3 to finish the proof. To fit into the syntax of our framework, we combine G and H as one random oracle $G \times H$ such that $G \times H(r', r, e) := (G(r'), H(r, e))$. If $\mathcal{A}$ only queries $G(r')$, we view it as querying $G \times H(r', r, e)$ for some dummy (r, e) and ignoring $H(r, e)$ in the response. $\mathcal{A}$ can query $G \times H$ at most $q = q_H + q_G$ times. This was also used in [24]. $\mathbf{G}_0$ is equivalent to $\mathsf{REAL\text{-}SO\text{-}CPA}_{\mathsf{wPKE}}$, thus

$$\Pr\left[\mathsf{REAL\text{-}SO\text{-}CPA}^{\mathcal{A}}_{\mathsf{wPKE}} \Rightarrow 1\right] = \Pr\left[\mathbf{G}_0^{\mathcal{A}} \Rightarrow 1\right]$$

Game $\mathbf{G}_1$: If in the challenge ciphertexts there exist K_i and K_j for $i \neq j$ such that $K_i = K_j$, then we abort the game. Such K_i and K_j collide only if r_i and r_j collide or $H(r_i, e_i)$ and $H(r_j, e_j)$ collide with different r_i and r_j. By birthday bounds, and we have

$$\left|\Pr\left[\mathbf{G}_0^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathbf{G}_1^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \frac{\mu^2}{|\mathcal{M}|} + \frac{\mu^2}{|\mathcal{M}'|}$$

Game $\mathbf{G}_2$: R_i and K_i in the challenge ciphertexts are chosen randomly, instead of using G and H. If $\mathcal{A}$ queries $\textsc{Open}(i)$, then we reprogram G and H such that $G(r_i) := R_i$ and $H(r_i, e_i) := K_i$.

In the following, we use Lemma 2 to bound the difference between $\mathbf{G}_1$ and $\mathbf{G}_2$. In $\mathbf{G}_2$, $\mathcal{A}$'s $\textsc{Open}$ queries will make QRO $G \times H$ reprogrammed, while in $\mathbf{G}_1$, QRO $G \times H$ does not get reprogrammed. So, we can view $\mathbf{G}_1$ and $\mathbf{G}_2$ as concrete cases of NonAda and Ada, respectively. For simplicity, we denote $\mathcal{A} := (\mathcal{A}_0, (\mathcal{A}_{1,0}, ..., \mathcal{A}_{1,n_O}))$, where $\mathcal{A}_0$ is the initial stage of $\mathcal{A}$ and cannot query $\textsc{Open}$, and $(\mathcal{A}_{1,0}, ..., \mathcal{A}_{1,n_O})$ is the stage that $\mathcal{A}$ receives the challenge ciphertexts $\mathbf{c}$ and can query $\textsc{Open}$. Let $\mathcal{A}_1 := (\mathcal{A}_{1,0}, ..., \mathcal{A}_{1,n_O})$. $\mathcal{A}_1$'s initial state is the final state of $\mathcal{A}_0$. $\mathcal{A}_{1,k}$ is defined with respect to $\textsc{Open}$ queries:

- Before any $\textsc{Open}$ query (i.e., at the 0-th stage), $\mathcal{A}_{1,0}$ takes $\mathsf{in}_0 := \mathbf{c}$ as input and outputs the first opening index $\mathsf{out}_0 := (i_1)$.
- At k-th stage ($1 \leq k \leq n_O - 1$), $\mathcal{A}_{1,k}$ receives $\mathsf{in}_k = (m_{i_k}, r_{i_k})$ As the result of the $(k-1)$-th $\textsc{Open}$ query and finishes the stage by outputting the $(k+1)$-th opening index $\mathsf{out}_k := (i_{k+1})$
- Finally, at the n_O stage, $\mathcal{A}_{1,n_O}$ receives $\mathsf{in}_{n_O} = (m_{i_{n_O}}, r_{i_{n_O}})$ and terminates by outputting $\mathsf{out}_{n_O} = out$ (the final output of SO adversary).

To formally show why $\mathbf{G}_1$ and $\mathbf{G}_2$ are concrete cases of NonAda and Ada, respectively, in Fig. 8, we define $\texttt{INIT}$, $\mathsf{F_s}$, $\mathsf{Repro_s}$, $\mathbf{G}'_1$ and $\mathbf{G}'_2$. Games $\mathbf{G}'_1$ and $\mathbf{G}'_2$ are only defined to show how our proof follows the syntax of our framework. They have the same forms as NonAda and Ada.

Now we argue that $\mathbf{G}_1$ and $\mathbf{G}_2$ are concrete cases of NonAda and Ada, respectively. Namely, $\mathbf{G}_1$ and $\mathbf{G}_2$ in Fig. 7 are equivalent to $\mathbf{G}'_1$ and $\mathbf{G}'_2$ in Fig. 8, respectively. Firstly, algorithm $\texttt{INIT}$ in Fig. 8 run the codes from Item 01 to Item 12 in Fig. 7. Since in $\mathcal{A}_0$'s view, $\mathbf{G}_1$ is the same as $\mathbf{G}_2$ (it does not see any challenge ciphertexts), the distribution of $\mathcal{M}_a$ and $\mathbf{m}$ in $\mathbf{G}_1$ is the same as the one in $\mathbf{G}_2$, and thus the output of $\texttt{INIT}$ and the final state of $\mathcal{A}_0$ in $\texttt{INIT}$ in $\mathbf{G}'_1$ are the same as those in $\mathbf{G}'_2$. Secondly, $\mathsf{F_s}$ simulates the $\textsc{Open}$ oracle and $\mathsf{Repro_s}$ simulates the reprogramming operations on G and H. In $\mathbf{G}'_1$, G and H will not be reprogrammed, but in $\mathbf{G}'_2$, G and H will be reprogrammed, according to $\mathcal{A}$'s output. This is the same as in $\mathbf{G}_2$.

Moreover, when running $\mathcal{A}_{1,k}$, our $\mathsf{Repro_s}$ defines a set

$$S_k := \{(r, (r', e')) \mid \exists i \in [\mu] \backslash I_k \text{ s.t. } r = r_i \text{ or } (r', e') = (r_i, e_i)\} \tag{3}$$

where $I_k := \{i_1, ..., i_k\}$ is the opening index set I in $\mathcal{A}_1$'s k-th stage. Answers of $G \times H$ on S_k are only different in $\mathbf{G}_1$ (i.e., NonAda) and $\mathbf{G}_2$ (i.e., Ada). For $k = 0$, S_0 is defined at line 35 and $I_0 = \emptyset$.

Now we consider the probability that $\mathsf{Rel}(\mathcal{M}_a, \mathbf{m}, I, out) = 1$. I and out are determined by $\mathcal{A}_1$. $\mathcal{M}_a$ is output by $\mathcal{A}_0$, and $\mathbf{m}$ is determined by $\mathcal{M}_a$. Since in $\mathcal{A}_0$'s view, $\mathbf{G}_1$ is the same as $\mathbf{G}_2$ (since it does not see challenge ciphertexts),

Game $\mathbf{G}'_1$-$\mathbf{G}'_2$

$((\mathbf{s}, \mathsf{in}_0), \mathsf{H}, \mathsf{H}_0) \leftarrow \texttt{INIT}$
Initialize $\mathcal{A}_{1,0}$ with
  the final state of $\mathcal{A}_0$ in INIT
$\mathcal{H} := \mathsf{H}$ // $\mathbf{G}'_1$
$\mathcal{H} := \mathsf{H}_0$ // $\mathbf{G}'_2$
$\mathsf{out}_0 \leftarrow \mathcal{A}_{1,0}^{\vert\mathcal{H}\rangle}(\mathsf{in}_0)$
$\Gamma[0] := \mathsf{out}_0$
for $i = 1$ **to** n_{O}:
  $(\mathsf{in}_i, \mathsf{in}'_i) := \mathsf{F}_{\mathbf{s}}(\mathsf{out}_{i-1})$
  $\mathsf{H}_i := \mathsf{Repro}_{\mathbf{s}}(\mathsf{in}'_i, \mathsf{H}_{i-1})$ // $\mathbf{G}'_2$
  $\mathcal{H} := \mathsf{H}_i$ // $\mathbf{G}'_2$
  $\mathsf{out}_i \leftarrow \mathcal{A}_{1,i}^{\vert\mathcal{H}\rangle}(\mathsf{in}_i)$
  $\Gamma[i] := \mathsf{out}_i$
return $\mathsf{Rel}(\mathcal{M}_a, \mathbf{m}, I, \Gamma[n_{\mathrm{O}}])$

INIT

$I := \emptyset$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}_0$
$\mathcal{M}_a \leftarrow \mathcal{A}_0^{\vert g \times h\rangle}(\mathsf{pk})$
Let g' and h' be internal QROs.
for $i \in [\mu]$:
  $\mathbf{m}[i] := m_i \leftarrow \mathcal{M}_a, \mathbf{r}[i] := r_i \xleftarrow{\$} \mathcal{M}'$
  $R_i := g(r_i)$, $\mathbf{R}[i] := R_i$
  $e_i := \mathsf{Enc}_0(\mathsf{pk}, r_i; R_i)$
  $K_i := h(r_i, e_i)$, $d_i := K_i \oplus m_i$ // By $\mathbf{G}_1$, all K_i's are different.
  $\mathbf{c}[i] := (e_i, d_i)$
$\mathbf{s} := (\mathcal{M}_a, \mathbf{m}, \mathbf{r}, \mathbf{R}, \mathbf{c})$, $\mathsf{in}_0 := \mathbf{c}$
$S_0 := \{r_i\}_{i\in[\mu]} \times \{(r_i, e_i)\}_{i\in[\mu]}$
$G := g, H := h$
Let $G_0 \times H_0$ be a QRO such that $G_0 \times H_0(x) := \begin{cases} g \times h(x), & (x \notin S_0) \\ g' \times h'(x), & (\text{else}) \end{cases}$
  // Namely, $(G_0 \times H_0)\backslash S_0 = (G \times H)\backslash S_0$
return $((\mathbf{s}, \mathsf{in}_0), (G \times H), (G_0 \times H_0))$

$\mathsf{F}_{\mathbf{s}}(\mathsf{out})$

parse $i := \mathsf{out}$
parse $(\mathcal{M}_a, \mathbf{m}, \mathbf{r}, \mathbf{R}, \mathbf{c}) := \mathbf{s}$
$I := I \cup \{i\}$
$r_i := \mathbf{r}[i], m_i := \mathbf{m}[i], (e_i, d_i) := \mathbf{c}[i]$
$\mathsf{in} := (m_i, r_i)$, $\mathsf{in}' := (m_i, r_i, e_i, d_i)$
return $(\mathsf{in}, \mathsf{in}')$

$\mathsf{Repro}_{\mathbf{s}}(\mathsf{in}', (G \times H))$

parse $(m, r, e, d) := \mathsf{in}'$
$G' := G[r \to R]$
$H' := H[(r, e) \to d \oplus m]$
  // Namely, we set $H(r_i, e_i) := K_i$
  // and denote the new oracle as H'
return $G' \times H'$

Fig. 8. Constructions of INIT, $\mathsf{F}_{\mathbf{s}}$, and $\mathsf{Repro}_{\mathbf{s}}$ and games $\mathbf{G}'_1$ and $\mathbf{G}'_2$. $G' := G[r_i \to R_i]$ (similarly, $H' := H[(r_i, e_i) \to K_i]$) means that we set $G'(r_i) := R_i$ and $G'(r) := G(r)$ for $r \neq r_i$. Oracles $g, g' : \mathcal{M}' \to \mathcal{R}'$, and $h, h' : \mathcal{M}' \times \mathcal{C}' \to \mathcal{M}$ are four independent internal quantum-accessible random oracles.

thus the distribution of $\mathcal{M}_a$ and $\mathbf{m}$ in $\mathbf{G}_1$ is the same as the one in $\mathbf{G}_2$. Therefore, the probability difference between the classical event that $\mathsf{Rel}(\mathcal{M}_a, \mathbf{m}, I, out) = 1$ in $\mathbf{G}_1$ and the similar event in $\mathbf{G}_2$, is determined by the probability difference between the event that $\mathcal{A}_1$ outputs a particular (I, out) (i.e., Γ in Fig. 8) in $\mathbf{G}_1$ and the similar event in $\mathbf{G}_2$. Therefore, we have

$$\left|\Pr\left[\mathbf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathbf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \left|\Pr\left[\mathbf{G}_1'^{\mathcal{A}_1} \Rightarrow 1\right] - \Pr\left[\mathbf{G}_2'^{\mathcal{A}_1} \Rightarrow 1\right]\right| + \frac{2\mu q}{\sqrt{|\mathcal{M}'|}} \tag{4}$$

$\underline{\mathcal{B}'_i(\mathsf{pk}^*, e^*)}$ // (pk^*, e^*) is a OW-CPA challenge of PKE

01 $I := \emptyset$
02 $((\mathbf{s}, \mathsf{in}_0), (G \times H), (G_0 \times H_0)) \leftarrow \mathtt{INIT}$ // INIT is defined in Figure 8 and // it uses pk^* instead of KG_0
03 **parse** $(\mathcal{M}_a, \mathbf{m}, \mathbf{r}, \mathbf{R}, \mathbf{c}) := \mathbf{s}$
04 **parse** $\mathbf{c} := \mathsf{in}_0$
05 $t^* \xleftarrow{\$} [\mu], (e_{t^*}, d_{t^*}) := \mathbf{c}[t^*]$
06 $\mathbf{c}[t^*] := (e^*, d_{t^*})$, $\mathsf{in}_0 := \mathbf{c}$ // embed the challenge
07 Initialize $\mathcal{B}_i$ with $\mathcal{A}_0$'s final state in INIT.
08 **if** $i = 0$: **goto** line 18
09 $\mathsf{out}_0 \leftarrow \mathcal{B}_i^{|G_0 \times H_0\rangle}(\mathsf{in}_0)$
10 **if** $\mathsf{out}_0 = t^*$: **abort**
11 $(\mathsf{in}_1, \mathsf{in}'_1) := \mathsf{F}_{\mathbf{s}}(\mathsf{out}_0)$ // $\mathsf{F}_{\mathbf{s}}$ is defined in Figure 8
12 $(G_1 \times H_1) := \mathsf{Repro}_{\mathbf{s}}(\mathsf{in}'_1, (G_0 \times H_0))$ // $\mathsf{Repro}_{\mathbf{s}}$ is defined in Figure 8
13 **for** $j = 1$ **to** $i - 1$:
14 $\quad \mathsf{out}_j \leftarrow \mathcal{B}_i^{|G_j \times H_j\rangle}(\mathsf{in}_j)$
15 $\quad$ **if** $\mathsf{out}_j = t^*$: **abort**
16 $\quad (\mathsf{in}_{j+1}, \mathsf{in}'_{j+1}) := \mathsf{F}_{\mathbf{s}}(\mathsf{out}_j)$
17 $\quad (G_{j+1} \times H_{j+1}) := \mathsf{Repro}_{\mathbf{s}}(\mathsf{in}'_{j+1}, (G_j \times H_j))$
18 $(r'_0, (r'_1, e')) \leftarrow \mathcal{B}_i^{|G_i \times H_i\rangle}(\mathsf{in}_i)$ // perform measurement
19 $b \xleftarrow{\$} \{0, 1\}, r^* := r'_b$ // randomly choose a solution
20 **return** r^*

Fig. 9. The constructions of OW-CPA adversaries $\mathcal{B}'_i$ for $i \in \{0, ..., n_{\mathrm{O}}\}$. $\mathcal{B}'_i$ simulates $\mathbf{G}'_2$ (which is a concrete case of ADA in Fig. 4) for $\mathcal{B}_i$ to break PKE. F and Repro are defined as in Fig. 8.

This bound includes a term $\frac{2\mu q}{\sqrt{|\mathcal{M}'|}}$, since $\mathcal{A}_0$ also has quantum access to $|G \times H\rangle$, and this term is the probability that the first stage (i.e., $\mathcal{A}_{1,0}$) of $\mathcal{A}_1$ learns r_i before seeing challenge ciphertexts. Such probability is only information-theoretic.

We now use Lemma 2 to bound Eq. (4). Since $\mathbf{G}'_1$ is a NONADA game and $\mathbf{G}'_2$ is an ADA game, by Lemma 2, there exist adversaries $\mathcal{B}_i$ $(0 \le i \le n_{\mathrm{O}})$, which take $\mathsf{in}_0 = \mathbf{c}$ as its input and output $x \in S_k$ where the set S_i is defined in (3), such that

$$\left|\Pr\left[\mathbf{G}'^{\mathcal{A}_1}_1 \Rightarrow 1\right] - \Pr\left[\mathbf{G}'^{\mathcal{A}_1}_2 \Rightarrow 1\right]\right| \le \sum_{k=0}^{n_{\mathrm{O}}} \sum_{i=0}^{k} 2q_i \sqrt{\Pr\left[x \leftarrow \mathcal{B}_i \text{ s.t. } x \in S_i : \mathbf{G}'^{\mathcal{B}_i}_2\right]} \tag{5}$$

Here $\mathcal{B}_i$ proceeds the same as $(\mathcal{A}_{1,0}, ..., \mathcal{A}_{1,i})$ except that it randomly measures a QRO query issued by $\mathcal{A}_{1,i}$. Moreover, since $\mathcal{A}_{1,0}$'s initial state is the final state of $\mathcal{A}_0$, $\mathcal{B}_i$ starts with state of $\mathcal{A}_0$ (cf. Item 07).

Based on $\mathcal{B}_i$, we construct an adversary $\mathcal{B}'_i$ (in Fig. 9) to break OW-CPA security of PKE. By the construction of $\mathcal{B}'_i$, if $\mathcal{A}_1$ does not open t^*, and r or r' equals the solution of e^*, then $\mathcal{B}'_i$ wins. So the winning probability for $\mathcal{B}'_i$ to break the OW-CPA challenge is:

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}'_i) = \frac{1}{2}\frac{\mu - n_{\mathrm{O}}}{\mu}\frac{1}{\mu - n_{\mathrm{O}}} \Pr\left[x \leftarrow \mathcal{B}_i \text{ s.t. } x \in S_i\right],$$

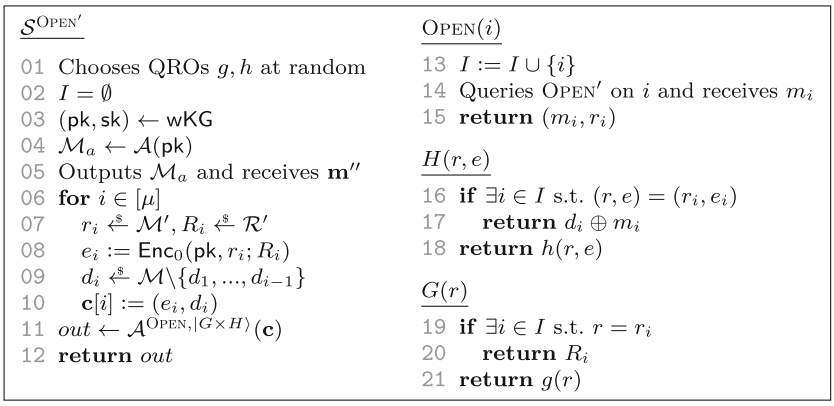

Fig. 10. The simulator $\mathcal{S}$ of the proof of Theorem 1.

and thus we have

$$\Pr\left[x \leftarrow \mathcal{B}_i \text{ s.t. } x \in S_i : \mathbf{G}_2'^{\mathcal{B}_i}\right] \leq 2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}_i') \tag{6}$$

Let $\mathcal{B}'$ be the adversary that has highest advantage against PKE among $\{\mathcal{B}_i'\}_{i \in \{0,\ldots,n\}}$. Then Eq. (6) can be written as:

$$\Pr\left[x \leftarrow \mathcal{B}_i \text{ s.t. } x \in S_i : \mathbf{G}_2'^{\mathcal{B}_i}\right] \leq 2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}'), \text{ for } \forall i \in [\mu] \tag{7}$$

By combining Eqs. (4) to (7), we have

$$\left|\Pr\left[\mathbf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathbf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 2(n_{\mathrm{O}} + 1)^2 q \sqrt{2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}')} + \frac{2\mu q}{\sqrt{|\mathcal{M}'|}}$$

Game $\mathbf{G}_3$: We change the generation of K_i and d_i. Now we firstly sample d_i uniformly at random, and replace all K_i as $d_i \oplus m_i$. This change is conceptual since in $\mathbf{G}_2$, all K_i are independently and uniformly random. In $\mathbf{G}_1$, we excluded any collision of K_i, so, in $\mathbf{G}_3$, it is equivalent to sample d_i in a collision-free way. Therefore, we have

$$\Pr\left[\mathbf{G}_2^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathbf{G}_3^{\mathcal{A}} \Rightarrow 1\right]$$

CONSTRUCTION OF SO SIMULATOR. We construct a SO simulator $\mathcal{S}$ that is simulating $\mathbf{G}_3$ for $\mathcal{A}$ and interacts with the $\mathsf{IDEAL\text{-}SO\text{-}CPA}^{\mathcal{S}}_{\mathsf{wPKE}}$ game. The simulation process is shown in Fig. 10. Obviously, $\mathcal{S}$ can perfectly simulates $\mathbf{G}_3$. So, we have

$$\Pr[\mathbf{G}_3^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{IDEAL\text{-}SO\text{-}CPA}^{\mathcal{S}}_{\mathsf{wPKE}} \Rightarrow 1]$$

In conclusion, for any SO-CPA adversary $\mathcal{A}$, there exists efficient simulator $\mathcal{S}$ such that

$$\begin{aligned}&\left|\Pr[\mathsf{REAL\text{-}SO\text{-}CPA}^{\mathcal{A}}_{\mathsf{wPKE}} \Rightarrow 1] - \Pr[\mathsf{IDEAL\text{-}SO\text{-}CPA}^{\mathcal{S}}_{\mathsf{wPKE}} \Rightarrow 1]\right| \\ &\leq 2(n_{\mathrm{O}} + 1)^2 q \sqrt{2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}')} + \frac{\mu^2}{|\mathcal{M}|} + \frac{\mu^2}{|\mathcal{M}'|} + \frac{2\mu q}{\sqrt{|\mathcal{M}'|}}.\end{aligned}$$

4.2 Selective Opening Security Against Chosen-Ciphertext Attacks

Let $\mathsf{MAC} = (\mathsf{Tag}, \mathsf{Vrfy})$ be a MAC scheme with key space $\mathcal{K}^{\mathtt{mac}}$, and let $H : \mathcal{R}' \times \mathcal{C}' \to \mathcal{M} \times \mathcal{K}^{\mathtt{mac}}$ be a hash function, where $\mathcal{C}$ is the ciphertext space of PKE. The second PKE scheme $\mathsf{sPKE} = (\mathsf{sKG}, \mathsf{sEnc}, \mathsf{sDec})$ (Fig. 11) is a combination of a modular Fujisaki-Okamoto's transformation $\mathsf{FO}^{\not\perp}[\mathsf{PKE}, G, H]$ [21,24], one-time pad, and the one-time MAC scheme MAC. It has similar structure with the scheme in [18,35].

$\underline{\mathsf{sKG}}$	$\underline{\mathsf{sEnc}(\mathsf{pk}, m \in \mathcal{M})}$	$\underline{\mathsf{sDec}((\mathsf{sk}, k), (e, d, \tau))}$
01 $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}_0$	06 $r \xleftarrow{\$} \mathcal{M}'$	12 $r' := \mathsf{Dec}_0(\mathsf{sk}, e)$
02 $k \xleftarrow{\$} \mathcal{R}'$	07 $e := \mathsf{Enc}_0(\mathsf{pk}, r; G(r))$	13 **if** $r' = \perp$
03 $\mathsf{pk}' := \mathsf{pk}$	08 $(K, K^{\mathtt{mac}}) := H(r, e)$	14 **or** $e \neq \mathsf{Enc}_0(\mathsf{pk}, r'; G(r'))$
04 $\mathsf{sk}' := (\mathsf{sk}, k)$	09 $d := K \oplus m$	15 $(K, K^{\mathtt{mac}}) := H(k, e)$
05 **return** $(\mathsf{pk}', \mathsf{sk}')$	10 $\tau := \mathsf{Tag}(K^{\mathtt{mac}}, d)$	16 **else** $(K, K^{\mathtt{mac}}) := H(r', e)$
	11 **return** (e, d, τ)	17 **if** $\mathsf{Vrfy}(K^{\mathtt{mac}}, \tau) = 1$
		18 $m := K \oplus d$
		19 **else** $m := \perp$
		20 **return** m

Fig. 11. A SO-CCA secure PKE scheme $\mathsf{sPKE} = (\mathsf{sKG}, \mathsf{sEnc}, \mathsf{sDec})$

This scheme is adaptive SO-CCA secure when modeling G and H as QROs, as stated in Theorem 2. The main difference between the proof of Theorem 2 and the one of Theorem 1 is that the simulator needs to simulate the decryption oracle for the adversary. We use the encrypt-then-hash technique (widely used in CCA proof of PKE [24,27,34]) to simulate the decryption oracle without using the secret key and add a MAC verification in the decryption so that the adversary cannot forge valid MAC codes for any unopened cipheretext. We postpone the proof of Theorem 2 to our full version [33].

Theorem 2. *If* PKE *is OW-CPA secure and* δ*-correct, and* MAC *is otSUF-CMA secure, then the PKE scheme* sPKE *in Fig. 11 is adaptive SO-CCA secure (Definition 5). Concretely, for security parameter* λ *and integer* $\mu := \mu(\lambda)$ *(polynomially bounded) for any SO-CCA adversary* $\mathcal{A}$ *and relation* Rel*, there exist a simulator* $\mathcal{S}$ *and adversaries* $\mathcal{B}'$ *and* $\mathcal{F}$ *such that* $\mathbf{T}(\mathcal{S}) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}') \approx \mathbf{T}(\mathcal{F})$ *and*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{SO\text{-}CCA}}_{\mathsf{sPKE}}(\mathcal{A}, \mathcal{S}, \mu, \mathsf{Rel}) \leq\ & 6(n_{\mathrm{O}}+1)^2 q \sqrt{2\mu \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}') + \mu \mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F})} \\ & + 3\mu \mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F}) + \frac{2q_H}{\sqrt{2^k}} + 16(\mu + n_{\mathrm{D}} + q + 1)^2 \delta \\ & + \frac{\mu^2}{|\mathcal{M}|} + \frac{\mu^2}{|\mathcal{K}^{\mathtt{mac}}|} + \frac{6\mu q}{\sqrt{|\mathcal{M}'|}} + \frac{\mu n_{\mathrm{D}}}{|\mathcal{C}'| - n_{\mathrm{D}}} + \frac{(2+\mu)q}{\sqrt{|\mathcal{M}'|}}\end{aligned}$$

where μ*,* q_G, q_H, n_{O}*, and* n_{D} *are the maximum numbers of* $\mathcal{A}$*'s challenge ciphertexts,* $\mathcal{A}$*'s queries to* $G, H,$ OPEN*, and* DEC*, respectively.* $q = q_G + q_H$*.*

5 Tight SO-CCA Security from Lossy Encryption

In this section, we show that if the underlying PKE is a lossy encryption [3,22], then the construction in Fig. 11 is tightly SO-CCA secure. We recall the notion of lossy encryption from [22].

Definition 7 (Lossy Encryption [22]). *Let* $\mathsf{PKE}_1 := (\mathsf{KG}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ *be a PKE scheme with message space* $\mathcal{M}'$ *and randomness space* $\mathcal{R}'$. PKE_1 *is lossy if it has the following properties:*

- PKE_1 *is correct according to Definition 2.*
- *Key indistinguishability: We say* PKE_1 *has key indistinguishability if there is an algorithm* LKG_1 *such that, for any adversary* $\mathcal{B}$*, the advantage function*

$$\mathsf{Adv}^{\mathsf{ind\text{-}key}}_{\mathsf{PKE}_1}(\mathcal{B}) := |\Pr[\mathcal{B}(\mathsf{pk}_1) \Rightarrow 1] - \Pr[\mathcal{B}(\mathsf{lpk}_1) \Rightarrow 1]|$$

  is negligible, where $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KG}_1$ *and* $(\mathsf{lpk}_1, \mathsf{lsk}_1) \leftarrow \mathsf{LKG}_1$.
- *Lossiness: Let* $(\mathsf{lpk}_1, \mathsf{lsk}_1) \leftarrow \mathsf{LKG}_1$ *and* m, m' *be arbitrary messages in* $\mathcal{M}'$*, the statistical distance between* $\mathsf{Enc}_1(\mathsf{lpk}_1, m)$ *and* $\mathsf{Enc}_1(\mathsf{lpk}_1, m')$ *is negligible.*
- *Weak Openability: Let* $(\mathsf{lpk}_1, \mathsf{lsk}_1) \leftarrow \mathsf{KG}_1$*,* m *and* m' *be arbitrary messages, and* r *be arbitrary randomness. For ciphertext* $c := \mathsf{Enc}_1(\mathsf{lpk}_1, m; r)$*, there exists an algorithm* open_1 *such that* $\mathsf{open}_1(\mathsf{lsk}_1, \mathsf{lpk}_1, c, r, m')$ *outputs* r' *where* $c = \mathsf{Enc}_1(\mathsf{lpk}_1, m'; r')$ *and* r' *is distributed uniformly.* open_1 *can be inefficient.*

The lossiness definition can be extended to a multi-challenge version using a hybrid argument. Since it is only a statistical property, the hybrid argument will not affect tightness of the computational advantage.

Definition 8 (Multi-challenge Lossiness). *For any arbitrary messages* $m_1, m'_1, ..., m_\mu, m'_\mu \in \mathcal{M}'$*, the statistical distance between the following distributions* D *and* D' *is at most* $\epsilon^{\mathsf{m\text{-}ind\text{-}enc}}_{\mathsf{PKE}_1}$*, where* $\epsilon^{\mathsf{m\text{-}ind\text{-}enc}}_{\mathsf{PKE}_1}$ *is negligible:*

$$D := \left\{ (\mathsf{lpk}_1, c_1, ..., c_\mu) \;\middle|\; \begin{array}{l} (\mathsf{lpk}_1, \mathsf{lsk}_1) \leftarrow \mathsf{LKG}_1 \\ c_1 \leftarrow \mathsf{Enc}_1(\mathsf{lpk}_1, m_1), ..., c_\mu \leftarrow \mathsf{Enc}_1(\mathsf{lpk}_1, m_\mu) \end{array} \right\},$$

$$D' := \left\{ (\mathsf{lpk}_1, c'_1, ..., c'_\mu) \;\middle|\; \begin{array}{l} (\mathsf{lpk}_1, \mathsf{lsk}_1) \leftarrow \mathsf{LKG}_1 \\ c'_1 \leftarrow \mathsf{Enc}_1(\mathsf{lpk}_1, m'_1), ..., c'_\mu \leftarrow \mathsf{Enc}_1(\mathsf{lpk}_1, m'_\mu) \end{array} \right\}.$$

5.1 Construction

Let $\mathsf{PKE}_1 = (\mathsf{KG}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ be a lossy encryption with message space $\mathcal{M}'$, randomness space $\mathcal{R}'$, ciphertext space $\mathcal{C}'$, and an opening algorithm open_1. Let $\mathsf{MAC} = (\mathsf{Tag}, \mathsf{Vrfy})$ be a MAC scheme with key space $\mathcal{K}^{\mathtt{mac}}$, and $G : \mathcal{M}' \to \mathcal{R}', H : \mathcal{M}' \times \mathcal{C}' \to \mathcal{M} \times \mathcal{K}^{\mathtt{mac}}$ be two hash functions. Our PKE scheme $\mathsf{sPKE} = (\mathsf{sKG}, \mathsf{sEnc}, \mathsf{sDec})$ is defined in Fig. 12, which has the same structure with the scheme in Fig. 11.

Theorem 3 shows that sPKE is tightly SO-CCA secure when modeling G and H as QROs. Although there is a loss μ to the otSUF-CMA security of the underlying MAC, if one can use a perfectly otSUF-CMA secure MAC (e.g., the efficient one implicitly in [26]), it will not affect the security loss of sPKE and thus sPKE is tight.

$\underline{\mathsf{sKG}}$	$\underline{\mathsf{sEnc}(\mathsf{pk}=\mathsf{pk}_1, m\in\mathcal{M})}$	$\underline{\mathsf{sDec}((\mathsf{sk}_1,k),(e,d,\tau))}$
01 $(\mathsf{pk}_1,\mathsf{sk}_1)\leftarrow\mathsf{KG}_1$	06 $r\xleftarrow{\$}\mathcal{M}'$	12 $r':=\mathsf{Dec}_1(\mathsf{sk}_1,e)$
02 $k\xleftarrow{\$}\mathcal{M}'$	07 $e:=\mathsf{Enc}_1(\mathsf{pk}_1,r;G(r))$	13 **if** $r'=\bot$
03 $\mathsf{pk}:=\mathsf{pk}_1$	08 $(K,K^{\mathtt{mac}}):=H(r,e)$	**or** $e\neq\mathsf{Enc}_1(\mathsf{pk}_1,r';G(r'))$
04 $\mathsf{sk}:=(\mathsf{sk}_1,k)$	09 $d:=K\oplus m$	14 $(K,K^{\mathtt{mac}}):=H(k,e)$
05 **return** $(\mathsf{pk},\mathsf{sk})$	10 $\tau\leftarrow\mathsf{Tag}(K^{\mathtt{mac}},(e,d))$	15 **else** $(K,K^{\mathtt{mac}}):=H(r',e)$
	11 **return** (e,d,τ)	16 **if** $\mathsf{Vrfy}(K^{\mathtt{mac}},(e,d),\tau)=1$
		17 $m:=K\oplus d$
		18 **else** $m:=\bot$
		19 **return** m

Fig. 12. A PKE scheme $\mathsf{sPKE}=(\mathsf{sKG},\mathsf{sEnc},\mathsf{sDec})$ based on lossy encryption PKE_1.

Theorem 3. *If* PKE_1 *is a lossy encryption scheme and* $(1-\delta)$*-correct, and* MAC *is otSUF-CMA secure, then the PKE scheme* sPKE *in Fig. 12 is adaptive SO-CCA secure (Definition 5). Concretely, for security parameter* λ *and integer* $\mu:=\mu(\lambda)$ *(which is polynomially bounded) for any SO-CCA adversary* $\mathcal{A}$ *and relation* Rel*, there exist a simulator* $\mathcal{S}$ *and an adversary* $\mathcal{F}$ *with* $\mathbf{T}(\mathcal{S})\approx\mathbf{T}(\mathcal{A})$, $\mathbf{T}(\mathcal{F})\approx\mathbf{T}(\mathcal{A})$*, and*

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{SO\text{-}CCA}}_{\mathsf{sPKE}}(\mathcal{A},\mathcal{S},\mu,\mathsf{Rel})\\
&\quad\le \mathsf{Adv}^{\mathsf{ind\text{-}key}}_{\mathsf{PKE}_1}(\mathcal{A})+3\mu\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F})\\
&\qquad+6(n_{\mathrm{O}}+1)^2q\sqrt{\epsilon^{\mathsf{m\text{-}ind\text{-}enc}}_{\mathsf{PKE}_1}+\frac{\mu q}{|\mathcal{M}'|}}+16(\mu+n_{\mathrm{D}}+q+1)^2\delta\\
&\qquad+\frac{(2+\mu)q}{\sqrt{|\mathcal{M}'|}}+\frac{6\mu q}{\sqrt{|\mathcal{M}'|}}+\frac{\mu^2}{|\mathcal{M}'|}+\frac{\mu^2}{|\mathcal{R}'|}+\frac{\mu^2}{|\mathcal{K}^{\mathtt{mac}}|}+\frac{\mu n_{\mathrm{D}}}{|\mathcal{C}'-n_{\mathrm{D}}|}+\frac{\mu^2}{|\mathcal{M}|}
\end{aligned}$$

where μ, q_G,q_H,n_{O}*, and* n_{D} *are the maximum numbers of* $\mathcal{A}$*'s challenge ciphertexts,* $\mathcal{A}$*'s queries to* $G,H,$ Open*, and* Dec*, respectively.* $q=q_G+q_H$*.*

For simplicity, here we only sketch the proof idea and the formal proof of Theorem 3 is postponed to our full version [33]. Roughly, we firstly use the encrypt-then-hash technique [24,27,34] to change security games so that the simulator can simulate decryption oracle without using secret key. Then, we switch the public key of PKE_1 to the lossy mode. By the key indistinguishability of PKE_1, the adversary cannot detect such modification, and the simulation of decryption oracle still works. However, although the public key is switched to lossy mode, we cannot use the lossiness of PKE_1 directly, since there are several correlations between challenge ciphertexts and the QROs. Therefore, at the end of the proof, we use our adaptive reprogramming framework in Sect. 3 and delayed analysis to derelate QROs and challenge ciphertexts, and argue that the adversary cannot learn any information of unopened challenge ciphertexts.

Instantiation from LWE. The Regev encryption scheme as defined in [15] is essentially a lossy encryption, and we can use it to instantiate our generic

$\underline{\mathsf{sKG}_{\mathsf{bi}}}$
01 $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}_0$
02 $k \xleftarrow{\$} \mathcal{M}'$
03 $\mathsf{pk}' := \mathsf{pk}$
04 $\mathsf{sk}' := (\mathsf{pk}, \mathsf{sk}, k)$
05 **return** $(\mathsf{pk}', \mathsf{sk}')$

$\underline{\mathsf{sEnc}_{\mathsf{bi}}(\mathsf{pk}, m \in \mathcal{M})}$
06 $r \xleftarrow{\$} \mathcal{M}'$
07 $e := \mathsf{Enc}_0(\mathsf{pk}, r; G(\mathsf{pk}, r))$
08 $(K, K^{\mathtt{mac}}) := H(\mathsf{pk}, r, e)$
09 $d := K \oplus m$
10 $\tau \leftarrow \mathsf{Tag}(K^{\mathtt{mac}}, d)$
11 **return** (e, d, τ)

$\underline{\mathsf{sDec}_{\mathsf{bi}}((\mathsf{pk}, \mathsf{sk}, k), (e, d, \tau))}$
12 $r' := \mathsf{Dec}_0(\mathsf{sk}, e)$
13 **if** $r' = \bot$
14 **or** $e \neq \mathsf{Enc}_0(\mathsf{pk}, r'; G(\mathsf{pk}, r'))$
15 $(K, K^{\mathtt{mac}}) := H'(\mathsf{pk}, k, e)$
16 **else** $(K, K^{\mathtt{mac}}) := H(\mathsf{pk}, r', e)$
17 **if** $\mathsf{Vrfy}(K^{\mathtt{mac}}, \tau) = 1$
18 $m := K \oplus d$
19 **else** $m := \bot$
20 **return** m

Fig. 13. A Bi-SO-CCA secure PKE scheme $\mathsf{sPKE}_{\mathsf{bi}} = (\mathsf{sKG}, \mathsf{sEnc}, \mathsf{sDec})$

construction in Fig. 12. For completeness, we describe the lossy encryption in our full version [33]. Our resulting LWE-based SO-CCA secure PKE is unfortunately only almost tight, since the LWE-based lossy encryption loses a factor depending on the security parameter.

6 Bi-sO Security in the QROM

In this section, we show that two PKE schemes are Bi-sO-CCA secure in the QROM. The first scheme is based on a modular FO transformation $\mathsf{FO}^{\not\perp}$ [21,24] (Sect. 6.1). The second scheme is based on another modular FO transformation $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ [21] (Sect. 6.2).

6.1 Bi-sO Security of $\mathsf{FO}^{\not\perp}$

We show that a multi-user version of sPKE (Fig. 11) is Bi-SO-CCA-secure in the QROM. Using the same building blocks $\mathsf{PKE} = (\mathsf{KG}_0, \mathsf{Enc}_0, \mathsf{Dec}_0)$ and MAC as sPKE, we propose $\mathsf{sPKE}_{\mathsf{bi}}$ (in Fig. 13). This scheme can be viewed as a combination of a modular FO transformation $\mathsf{FO}^{\not\perp}[\mathsf{PKE}, G, H]$ in [21,24], one-time pad, and the a MAC scheme MAC. Moreover, in $\mathsf{sPKE}_{\mathsf{bi}}$, each user includes its public key as an input to the hash functions G, H, H'.

Theorem 4 shows that $\mathsf{sPKE}_{\mathsf{bi}}$ is Bi-SO-CCA secure when modeling G and H as QROs. The proof of Theorem 4 is more complicated than the proofs of Theorem 2, since we also need to simulate CORRUPT oracle. But the proof idea is similar: we change the games so that the game simulator can use the encrypt-then-hash technique to simulate DEC (as we did in the proof of Theorem 2). To use our framework, we divide $\mathcal{A}_1$ with respect to CORRUPT and DEC, since the operations of CORRUPT also reprograms $G \times H$. The proof of Theorem 4 is postponed to our full version [33].

Theorem 4. *If* PKE *is OW-CPA secure, then the PKE scheme* $\mathsf{sPKE}_{\mathsf{bi}}$ *in Fig. 13 is adaptive Bi-SO-CCA secure (Definition 6). Concretely, for any adversary* $\mathcal{A}$ *and relation* Rel*, there exist a simulator* $\mathcal{S}$ *and adversaries* $\mathcal{B}'$ *and* $\mathcal{F}$ *such that* $\mathbf{T}(\mathcal{S}) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}') \approx \mathbf{T}(\mathcal{F})$ *and*

$$\mathsf{Adv}^{\mathsf{Bi\text{-}SO\text{-}CCA}}_{\mathsf{sPKE}_{\mathsf{bi}}}(\mathcal{A},\mathcal{S},p,\mu,\mathsf{Rel})$$
$$\leq 6(n_{\mathrm{C}}+n_{\mathrm{O}}+1)^2 q\sqrt{2p\mu\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathcal{B}^{ow})+p\mu\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F})}+p\eta_{\mathsf{KG}_0}$$
$$+3p\mu\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F})+\frac{p\mu n_{\mathrm{D}}}{|\mathcal{C}'|-n_{\mathrm{D}}}+\frac{p^2\mu^2+p^2}{|\mathcal{M}'|}+\frac{p^2\mu^2}{|\mathcal{R}'|}+\frac{p^2\mu^2}{|\mathcal{M}|}+\frac{p^2\mu^2}{|\mathcal{K}^{\mathtt{mac}}|}$$
$$+\frac{6p\mu q}{\sqrt{|\mathcal{M}'|}}+16p(\mu+n_{\mathrm{D}}+q+q_{H'}+1)^2\delta+\frac{2(n_{\mathrm{C}}+1)^2\sqrt{pq_{H'}}+2pq_{H'}+p\mu q}{\sqrt{|\mathcal{M}'|}}$$

where p,μ, $q_G,q_H,q_{H'},n_{\mathrm{O}},n_{\mathrm{C}}$, *and* n_{D} *are the number of user in the games and the maximal numbers of challenge ciphertexts per users,* $\mathcal{A}$*'s queries to* G,H,H', Open, Corrupt, *and* Dec, *respectively.* $q=q_G+q_H$.

6.2 Bi-sO Security of $\mathsf{U}^{\not\perp}_{\mathsf{m}}$

Let $\mathsf{PKE}=(\mathsf{KG}_0,\mathsf{Enc}_0,\mathsf{Dec}_0)$ be a deterministic PKE scheme with public space $\mathcal{PK}'$, plaintext space $\mathcal{M}'$, ciphertext space $\mathcal{C}'$, and plaintext distribution $\mathcal{D}_{\mathcal{M}'}$. Lett MAC be a one-time MAC as in $\mathsf{sPKE}_{\mathsf{bi}}$. Let $H:\mathcal{PK}'\times\mathcal{M}'\to\mathcal{M}\times\mathcal{K}^{\mathtt{mac}}$ and $H':\mathcal{PK}'\times\mathcal{M}'\times\mathcal{C}'\to\mathcal{M}\times\mathcal{K}^{\mathtt{mac}}$ be two hash functions. We define $\mathsf{sPKE}^{\mathsf{m}}_{\mathsf{bi}}$ as in Fig. 14. $\mathsf{sPKE}^{\mathsf{m}}_{\mathsf{bi}}$ can be viewed as a combination of $\mathsf{U}^{\not\perp}_{\mathsf{m}}$ [21], one-time pad and one-time MAC. Similar to $\mathsf{sPKE}_{\mathsf{bi}}$, each user includes its public key into the input of hash functions.

$\underline{\mathsf{sKG}^{\mathsf{m}}_{\mathsf{bi}}}$	$\underline{\mathsf{sEnc}^{\mathsf{m}}_{\mathsf{bi}}(\mathsf{pk},m\in\mathcal{M})}$	$\underline{\mathsf{sDec}^{\mathsf{m}}_{\mathsf{bi}}((\mathsf{pk},\mathsf{sk},k),(e,d,\tau))}$
01 $(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{KG}_0$	06 $r\leftarrow\mathcal{D}_{\mathcal{M}'}$	12 $r'=\mathsf{Dec}_0(\mathsf{sk},e)$
02 $k\xleftarrow{\$}\mathcal{M}'$	07 $e:=\mathsf{Enc}_0(\mathsf{pk},r)$	13 **if** $r'=\perp$
03 $\mathsf{pk}':=\mathsf{pk}$	08 $(K,K^{\mathtt{mac}}):=H(\mathsf{pk},r)$	14 $\quad(K,K^{\mathtt{mac}}):=H'(\mathsf{pk},k,e)$
04 $\mathsf{sk}':=(\mathsf{pk},\mathsf{sk},k)$	09 $d:=K\oplus m$	15 **else** $(K,K^{\mathtt{mac}}):=H(\mathsf{pk},r')$
05 **return** $(\mathsf{pk}',\mathsf{sk}')$	10 $\tau\leftarrow\mathsf{Tag}(K^{\mathtt{mac}},d)$	16 **if** $\mathsf{Vrfy}(K^{\mathtt{mac}},\tau)=1$
	11 **return** (e,d,τ)	17 $\quad m=K\oplus d$
		18 **else** $m=\perp$
		19 **return** m

Fig. 14. A Bi-SO-CCA secure PKE scheme $\mathsf{sPKE}^{\mathsf{m}}_{\mathsf{bi}}=(\mathsf{sKG}^{\mathsf{m}}_{\mathsf{bi}},\mathsf{sEnc}^{\mathsf{m}}_{\mathsf{bi}},\mathsf{sDec}^{\mathsf{m}}_{\mathsf{bi}})$

Here we consider a variant of OW-CPA security: $\mathcal{D}_{\mathcal{M}'}$-OW-CPA security, namely, OW-CPA security with challenge messages chosen following $\mathcal{D}_{\mathcal{M}'}$. For simplicity, the definition of of $\mathcal{D}_{\mathcal{M}'}$-OW-CPA is given in our full version [33]. Moreover, we require that PKE is *rigid* correct [5], namely, for all $(\mathsf{pk},\mathsf{sk})$ generated from KG_0, ciphertext e, and plaintext r, $(e=\mathsf{Enc}_0(\mathsf{pk},r))$ if and only if $(\mathsf{Dec}_0(\mathsf{sk},e)=r)$. Theorem 5 shows that $\mathsf{sPKE}^{\mathsf{m}}_{\mathsf{bi}}$ is Bi-sO-CCA secure when modeling G, H, and H' as QROs. The proof of Theorem 5 is similar to Theorem 4, and is postponed to our full version [33].

Theorem 5. *Let* PKE *be a deterministic PKE with perfect correctness and rigidity. If* PKE *is* $\mathcal{D}_{\mathcal{M}'}$*-OW-CPA secure, then the PKE scheme* $\mathsf{sPKE}^{\mathsf{m}}_{\mathsf{bi}}$ *in Fig. 14*

is adaptive Bi-SO-CCA secure (Definition 6). Concretely, for any Bi-SO-CCA adversary $\mathcal{A}$ and relation Rel*, there exist a simulator $\mathcal{S}$ and adversaries $\mathcal{B}^{ow}$ and $\mathcal{F}$ such that $\mathbf{T}(\mathcal{S}) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}') \approx \mathbf{T}(\mathcal{F})$ and*

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{Bi\text{-}SO\text{-}CCA}}_{\mathsf{sPKE}_{\mathsf{bi}}}(\mathcal{A},\mathcal{S},p,\mu,\mathsf{Rel}) \\
&\leq 6(n_{\mathrm{C}}+n_{\mathrm{O}}+1)^2 q\sqrt{2p\mu\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{D}_{\mathcal{M}'}}(\mathcal{B}^{ow})+p\mu\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F})} \\
&\quad + 3p\mu\mathsf{Adv}^{\mathsf{otSUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{F}) + \frac{6p\mu q}{2^{\epsilon_{\mathcal{D}_{\mathcal{M}'}}}} + \frac{p\mu n_{\mathrm{D}}}{|\mathcal{C}'|-n_{\mathrm{D}}} + \frac{p^2\mu^2+p^2}{|\mathcal{M}'|} + \frac{p^2\mu^2}{|\mathcal{M}|} \\
&\quad + p\eta_{\mathsf{KG}_0} + \frac{p^2\mu^2}{|\mathcal{K}^{\mathtt{mac}}|} + \frac{2(n_{\mathrm{C}}+1)^2\sqrt{pq_{H'}}+2pq_{H'}+p\mu q}{\sqrt{|\mathcal{M}'|}}
\end{aligned}$$

where p, μ, $q_H, q_{H'}, n_{\mathrm{O}}, n_{\mathrm{C}}$, and n_{D} are the maximum numbers of user in the games and $\mathcal{A}$'s challenge ciphertexts per users, $\mathcal{A}$'s queries to $H, H',$ Open*,* Corrupt*, and* Dec*, respectively. $\epsilon_{\mathcal{D}_{\mathcal{M}'}}$ is the minimum entropy of $\mathcal{D}_{\mathcal{M}'}$.*

Supporting Material

A Review of Adaptive One-Way-to-Hiding

Let $\mathcal{HF} := \{\{0,1\}^* \to \{0,1\}^n\}$ be a set containing all functions that have $\{0,1\}^*$ as domain and $\{0,1\}^n$ as codomain. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ be an adversary that has quantum access to a QRO $\mathcal{H}$ and queries it at most $q_0 + q_1$ times. Unruh's adaptive OW2H lemma [39, Lemma 15] can be described as follows: let

$$\begin{aligned}
P_0^{\mathcal{A}} &:= \Pr\left[b'=1 : \mathcal{H} \xleftarrow{\$} \mathcal{HF}, m \leftarrow \mathcal{A}_0^{\mathcal{H}}(), x \xleftarrow{\$} \{0,1\}^l, b' \leftarrow \mathcal{A}_1^{\mathcal{H}}(x, \mathcal{H}(x||m))\right] \\
P_1^{\mathcal{A}} &:= \Pr\Big[b'=1 : \mathcal{H} \xleftarrow{\$} \mathcal{HF}, m \leftarrow \mathcal{A}_0^{\mathcal{H}}(), x \xleftarrow{\$} \{0,1\}^l, \\
&\qquad\qquad B \xleftarrow{\$} \{0,1\}^n, b' \leftarrow \mathcal{A}_1^{\mathcal{H}}(x,B)\Big] \\
P_C &:= \Pr\Big[(x'||m') = (x||m) : \mathcal{H} \xleftarrow{\$} \mathcal{HF}, m \leftarrow \mathcal{A}_0^{\mathcal{H}}(), x \xleftarrow{\$} \{0,1\}^l, \\
&\qquad\qquad B \xleftarrow{\$} \{0,1\}^n, j \xleftarrow{\$} [q_0], x'||m' \xleftarrow{\$} C^{\mathcal{H}}(j,x,B)\Big]
\end{aligned}$$

where q_0, q_1 are the numbers of time $\mathcal{A}_0, \mathcal{A}_1$ queries $\mathcal{H}$ respectively. C is an algorithm that has quantum access to $\mathcal{H}$ and on input (j, B, x), runs $\mathcal{A}_1^{\mathcal{H}}(x, B)$ until its j-th query, measures the QRO query in the computational basis, output the measurement outcome. Then

$$\left|P_0^{\mathcal{A}} - P_1^{\mathcal{A}}\right| \leq 2q_1\sqrt{P_C} + q_0 2^{-l/2+2}$$

The bound given in this adaptive OW2H lemma includes two parts: the first part is roughly the search bound of quantum adversaries to find a uniformly random x given $\mathcal{H}(x||m)$ (i.e., $q_0 2^{-l/2+2}$), and the second part is the advantage of $\mathcal{A}_1$ to distinguish two QROs: $\mathcal{H}_{(x||m)\to B}$ and $\mathcal{H}$, where $\mathcal{H}_{(x||m)\to B}$ is the same as $\mathcal{H}$ except that $\mathcal{H}_{(x||m)\to B}(x||m) = B$. Note that this advantage is described by the extracting algorithm C.

Unruh's adaptive OW2H lemma cannot be used to prove the bound of our reprogramming framework Fig. 4 via hybrid arguments. This is because:

- The initial oracles of Ada and NonAda in our framework are not necessarily the same. In this case, our framework considers a stronger QROM adaptive reprogramming setting than the adaptive OW2H (and the adaptive reprogramming framework in [16]).
- Even if the initial oracles are the same, in our framework, sets S_i may not independent to each other, and thus each intermediate hybrid games in the hybrid argument may not independent. This makes it hard to modify the adaptive OW2H lemma to fit in our framework and use hybrid argument. More details will be given in our full version [33].

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 269–295. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-030-26951-7_10
2. Bellare, M., Dowsley, R., Waters, B., Yilek, S.: Standard security does not imply security against selective-opening. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 645–662. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_38
3. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_1
4. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_25
5. Bernstein, D.J., Persichetti, E.: Towards KEM unification. Cryptology ePrint Archive, Report 2018/526 (2018). https://ia.cr/2018/526
6. Böhl, F., Hofheinz, D., Kraschewski, D.: On definitions of selective opening security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 522–539. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_31
7. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_3
8. Chen, C., et al.: NTRU. Technical report, National Institute of Standards and Technology (2020). https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
9. D'Anvers, J.P., et al.: SABER. Technical report, National Institute of Standards and Technology (2020). https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

10. Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: multi-round fiat-shamir and more. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part III. LNCS, vol. 12172, pp. 602–631. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-56877-1_21
11. Fehr, S., Hofheinz, D., Kiltz, E., Wee, H.: Encryption schemes secure against chosen-ciphertext selective opening attacks. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 381–402. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_20
12. Fujisaki, E., Okamoto, T.: How to enhance the security of public-key encryption at minimum cost. In: Imai, H., Zheng, Y. (eds.) PKC 1999. LNCS, vol. 1560, pp. 53–68. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-49162-7_5
13. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (Aug (1999). https://doi.org/10.1007/3-540-48405-1_34
14. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. J. Cryptol. **26**(1), 80–101 (2013)
15. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC, pp. 197–206. ACM Press (2008)
16. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the QROM. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 637–667. Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-030-92062-3_22
17. Hemenway, B., Libert, B., Ostrovsky, R., Vergnaud, D.: Lossy encryption: constructions from general assumptions and efficient selective opening chosen ciphertext security. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 70–88. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_4
18. Heuer, F., Jager, T., Kiltz, E., Schäge, S.: On the selective opening security of practical public-key encryption schemes. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 27–51. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_2
19. Heuer, F., Poettering, B.: Selective opening security from simulatable data encapsulation. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 248–277. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_9
20. Hofheinz, D.: All-but-many lossy trapdoor functions. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 209–227. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_14
21. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017, Part I. LNCS, vol. 10677, pp. 341–371. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-70500-2_12
22. Hofheinz, D., Jager, T., Rupp, A.: Public-key encryption with simulation-based selective-opening security and compact ciphertexts. In: Hirt, M., Smith, A.D. (eds.) TCC 2016-B, Part II. LNCS, vol. 9986, pp. 146–168. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_6
23. Hofheinz, D., Rupp, A.: Standard versus selective opening security: separation and equivalence results. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 591–615. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_25

24. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part III. LNCS, vol. 10993, pp. 96–125. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-96878-0_4
25. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 552–586. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-78372-7_18
26. Kiltz, E., Pan, J., Wee, H.: Structure-preserving signatures from standard assumptions, revisited. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 275–295. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_14
27. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.: Measure-rewind-measure: tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part III. LNCS, vol. 12107, pp. 703–728. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-45727-3_24
28. Lai, J., Yang, R., Huang, Z., Weng, J.: Simulation-based bi-selective opening security for public key encryption. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part II. LNCS, vol. 13091, pp. 456–482. Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-030-92075-3_16
29. Lyu, L., Liu, S., Han, S., Gu, D.: Tightly SIM-SO-CCA secure public key encryption from standard assumptions. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part I. LNCS, vol. 10769, pp. 62–92. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-76578-5_3
30. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press, Cambridge (2016)
31. Pan, J., Wagner, B., Zeng, R.: Tighter security for generic authenticated key exchange in the QROM. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023. LNCS, vol. 14441, pp. 401–433. Springer, Heidelberg (2023). https://eprint.iacr.org/2023/1380
32. Pan, J., Zeng, R.: Compact and tightly selective-opening secure public-key encryption schemes. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022, Part III. LNCS, vol. 13793, pp. 363–393. Springer, Heidelberg (2022). https://doi.org/10.1007/978-3-031-22969-5_13
33. Pan, J., Zeng, R.: Selective opening security in the quantum random oracle model, revisited. Cryptology ePrint Archive (2023). https://ia.cr/2023/1682
34. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 520–551. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-78372-7_17
35. Sato, S., Shikata, J.: SO-CCA secure PKE in the quantum random oracle model or the quantum ideal cipher model. In: Albrecht, M. (ed.) IMACC 2019. LNCS, vol. 11929, pp. 317–341. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-030-35199-1_16
36. Sato, S., Shikata, J.: SO-CCA secure PKE in the quantum random oracle model or the quantum ideal cipher model. Cryptology ePrint Archive, Paper 2022/617 (2022). https://eprint.iacr.org/2022/617. Accessed 21 July 2022
37. Schwabe, P., et al.: CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology (2020). https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

38. Targhi, E.E., Unruh, D.: Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In: Hirt, M., Smith, A.D. (eds.) TCC 2016-B, Part II. LNCS, vol. 9986, pp. 192–216. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_8
39. Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 1–18. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44381-1_1
40. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 129–146. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_8
41. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part II. LNCS, vol. 12697, pp. 568–597. Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-030-77886-6_20
42. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_44