Quantum Public-Key Encryption with Tamper-Resilient Public Keys from One-Way Functions

Fuyuki Kitagawa[1], Tomoyuki Morimae[2], Ryo Nishimaki[1],Takashi Yamakawa[1,2]

[1]NTT Social Informatics Laboratories, Tokyo, Japan
{fuyuki.kitagawa,ryo.nishimaki,takashi.yamakawa}@ntt.com
[2]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp

Abstract

We construct quantum public-key encryption from one-way functions. In our construction, public keys are quantum, but ciphertexts are classical. Quantum public-key encryption from one-way functions (or weaker primitives such as pseudorandom function-like states) are also proposed in some recent works [Morimae-Yamakawa, eprint:2022/1336; Coladangelo, eprint:2023/282; Grilo-Sattath-Vu, eprint:2023/345; Barooti-Malavolta-Walter, eprint:2023/306]. However, they have a huge drawback: they are secure only when quantum public keys can be transmitted to the sender (who runs the encryption algorithm) without being tampered with by the adversary, which seems to require unsatisfactory physical setup assumptions such as secure quantum channels. Our construction is free from such a drawback: it guarantees the secrecy of the encrypted messages even if we assume only unauthenticated quantum channels. Thus, the encryption is done with adversarially tampered quantum public keys. Our construction based only on one-way functions is the first quantum public-key encryption that achieves the goal of classical public-key encryption, namely, to establish secure communication over insecure channels.

1 Introduction

1.1 Background

Quantum physics provides several advantages in cryptography. For instance, statistically-secure key exchange, which is impossible in classical cryptography, becomes possible if quantum states are transmitted [BB84]. Additionally, oblivious transfers and multiparty computations are possible only from one-way functions (OWFs) in the quantum world [BCKM21, GLSV21]. Those cryptographic primitives are believed to require stronger structured assumptions in classical cryptography. Furthermore, it has been shown that several cryptographic tasks, such as (non-interactive) commitments, digital signatures, secret-key encryption, quantum money, and multiparty computations, are possible based on new primitives such as pseudorandom states generators, pseudorandom function-like states generators, one-way states generators, and EFI, which seem to be weaker than OWFs [JLS18, Kre21, MY22b, AQY22, BCQ23, AGQY22, CX22, MY22a, KQST22].

Quantum public key encryption from OWFs. Despite these developments, it is still an open problem whether public-key encryption (PKE) is possible with only OWFs (or the above weaker primitives) in the quantum world. PKE from OWFs is impossible (in a black-box way) in the classical cryptography [IR90]. However, it could be possible if quantum states are transmitted or local operations are quantum. In fact, some recent works [MY22a, Col23, BMW23, GSV23] independently constructed quantum PKE (QPKE) with quantum public keys based on OWFs or pseudorandom function-like states generators. However, the constructions proposed in those works have a huge drawback as explained below, and thus we still do not have a satisfactory solution to the problem of "QPKE from OWFs".

How to certify quantum public keys? When we study public key cryptographic primitives, we have to care about how to certify the public keys, that is, how a sender can check if a given public key is a valid public key under which the secrecy of the encrypted messages is guaranteed. When the public keys are classical strings, we can easily certify them using digital signature schemes. However, in the case where the public keys are quantum states, we cannot use digital signature schemes to achieve this goal in general[1], and it is unclear how to certify them.

As stated above, some recent works [MY22a, Col23, BMW23, GSV23] realized QPKE with quantum public keys from OWFs or even weaker assumptions. However, those works did not tackle this quantum public key certification problem very much. In fact, as far as we understand, to use the primitives proposed in those works meaningfully, we need to use secure quantum channels to transmit the quantum public keys so that a sender can use an intact quantum public key. This is a huge drawback since the goal of PKE is to transmit a message *without assuming secure channels*. If the sender can establish a secure channel to obtain the quantum public key, the sender could use it to transmit the message in the first place, and there is no advantage to using the PKE scheme.

QPKE with tamper-resilient quantum public keys. One of our goals in this work is to solve this issue and develop a more reasonable notion of QPKE with quantum public keys. Especially, we consider the setting with the following two natural conditions. First, we assume that every quantum state (that is, quantum public keys in this work) is sent via an unauthenticated channel, and thus it can be tampered with by an adversary. If we do not assume secure quantum channels, we have to take such a tampering attack into account since authentication generally requires secrecy for quantum channels [BCG$^+$02]. Second, we assume that

[1]There is a general impossibility result for signing quantum states [AGM21].

every classical string is sent via an authenticated channel. This is the same assumption in classical PKE and can be achieved using digital signatures. Note that the security of the constructions proposed in the above works [MY22a, Col23, BMW23, GSV23] is broken in this natural setting. In this work, we tackle whether we can realize QPKE with quantum public keys that provides a security guarantee in this natural setting, especially from OWFs.

1.2 Our Results

We affirmatively answer the above question. We realize the first QPKE scheme based only on OWFs that achieves the goal of classical PKE, which is to establish secure communication over insecure channels. We define the notions of QPKE that can be used in the above setting where unauthenticated quantum channels and classical authenticated channels are available. Then, we propose constructions satisfying the definitions from OWFs. Below, we state each result in detail.

Definitional work. We redefine the syntax of QPKE. The difference from the previous definitions is that the key generation algorithm outputs a classical verification key together with the secret key. Also, this verification key is given to the encryption algorithm with a quantum public key and a message so that the encryption algorithm can check the validity of the given quantum public key. We then define a security notion for QPKE that we call *indistinguishability against public key tempering attacks (IND-pkTA security)*. Roughly speaking, it guarantees that indistinguishability holds even if messages are encrypted by a public key tampered with by an adversary. More specifically, it guarantees that no efficient adversary can guess the challenge bit b with a probability significantly better than random guessing given $\mathsf{Enc}(\mathsf{vk}, \mathsf{pk}', \mathsf{msg}_b)$, where vk is the correct verification key and $(\mathsf{pk}', \mathsf{msg}_0, \mathsf{msg}_1)$ are generated by the adversary who is given the verification key vk and multiple copies of the correctly generated quantum public keys. IND-pkTA security captures the setting where the classical verification key is sent via a classical authenticated channel. Thus, everyone can obtain the correct verification key. However, a quantum public key is sent via an unauthenticated quantum channel and thus can be tampered with by an adversary.

Moreover, we define a security notion related to the correctness notion. In our setting, a decryption error could frequently occur as a result of tampering attacks on the quantum public key. To address this issue, we introduce a security notion that we call *decryption error detectability*. It roughly guarantees that a legitimate receiver of a ciphertext can notice if the decrypted message is different from the message intended by the sender.

Constructions from OWFs. We propose a QPKE scheme satisfying IND-pkTA security from a digital signature scheme that can be constructed from OWFs. Our construction is inspired by the duality between distinguishing and swapping shown by Aaronson, Atia, and Susskind [AAS20] and its cryptographic applications by Hhan, Morimae, and Yamakawa [HMY22]. Our construction has quantum public keys and classical ciphertexts. We also propose a general transformation that adds decryption error detectability. The transformation uses only a digital signature scheme.

Recyclable variant. Our above definitions for QPKE assume each quantum public key is used to encrypt only a single message and might be consumed. We also introduce a notion of *recyclable QPKE* where the encryption algorithm given a quantum public key outputs a ciphertext together with a classical state that can be used to encrypt a message many times. Then, we show that any standard QPKE scheme with classical ciphertext can be transformed into a recyclable one. The transformation uses only a CPA secure classical symmetric key encryption scheme that is implied by OWFs. Thus, by combining the transformation with the above results, we obtain a recyclable QPKE scheme from OWFs.

1.3 Discussion: Pure State Public Keys vs. Mixed State Public Keys

The quantum public keys of our QPKE schemes are mixed states. Some recent works [BMW23, GSV23] that studied QPKE explicitly require that a quantum public key of QPKE be a pure quantum state. The reason is related to the quantum public key certification problem, which is this work's main focus. Those works claimed that a sender can check the validity of given quantum public keys by using SWAP test if they are pure states, but not if they are mixed states. However, as far as we understand, this claim implicitly requires that at least one intact quantum public key be transmitted via secure quantum channels where an adversary cannot touch it at all[2], which is an unsatisfactory assumption that makes QPKE less valuable. It is unclear how a sender can check the validity of a given quantum public key in the constructions proposed in [BMW23, GSV23] without assuming such secure transmission of intact quantum public keys.

We believe that it is not important whether the quantum public keys are pure states or mixed states, and what is really important is whether a sender can check the validity of given quantum public keys without assuming unsatisfactory setups such as quantum secure channels. Although our QPKE schemes have mixed state quantum public keys, they provide such a validity checking of quantum public keys by a sender without assuming any unsatisfactory setups. In addition, we can easily extend our construction into one with pure state quantum public keys. We provide the variant in Appendix A.

1.4 Technical Overview

In this subsection, we overview our technical contributions.

Duality between distinguishing and swapping. Our construction is inspired by the duality between distinguishing and swapping shown by Aaronson, Atia, and Susskind [AAS20] and its cryptographic applications by Hhan et al. [HMY22].[3] We first review their idea. Let $|\psi\rangle$ and $|\phi\rangle$ be orthogonal states. [AAS20] showed that $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$ are computationally indistinguishable[4] if and only if one cannot efficiently "swap" $|\psi\rangle$ and $|\phi\rangle$ with a non-negligible advantage, i.e., for any efficiently computable unitary U, $|\langle\phi| U |\psi\rangle + \langle\psi| U |\phi\rangle|$ is negligible. Based on the above result, [HMY22] suggested to use $|\psi\rangle + (-1)^b |\phi\rangle$ as an encryption of a plaintext $b \in \{0,1\}$. By the result of [AAS20], its security is reduced to the hardness of swapping $|\psi\rangle$ and $|\phi\rangle$.

Basic scheme. Based on the above idea, we first construct a QPKE scheme that is secure in a very restricted setting where an adversary is not given any quantum public key at all and only given one ciphertext. In particular the adversary cannot tamper with the quantum public key. Of course, constructing a secure QPKE scheme in such a setting is trivial since one could simply send a secret key for the one-time pad as a "public key". But we construct it in an alternative way for convenience of the later extension.

A quantum public key is

$$|0\rangle |x_0\rangle + |1\rangle |x_1\rangle \tag{1}$$

[2]More precisely, their model seems to require a physical setup assumption that enables a sender to obtain at least one intact quantum public key, such as secure quantum channels or tamper-proof quantum hardware.

[3]In the main body, we do not explicitly use any result of [AAS20, HMY22] though our analysis is similar to theirs.

[4]We often omit normalization factors.

for uniformly random bit strings $x_0, x_1 \in \{0,1\}^\lambda$, a secret key is (x_0, x_1), and an encryption of a plaintext $b \in \{0,1\}$ is

$$|0\rangle |x_0\rangle + (-1)^b |1\rangle |x_1\rangle . \tag{2}$$

Security of the above scheme in the restricted setting is somewhat obvious because the adversary has no information of x_0 or x_1 besides the ciphertext, but let us analyze it using the idea of [AAS20] to get more insights. Suppose that the above scheme is insecure, i.e., $|0\rangle |x_0\rangle + |1\rangle |x_1\rangle$ and $|0\rangle |x_0\rangle - |1\rangle |x_1\rangle$ are computationally distinguishable with a non-negligible advantage. Then, by the result of [AAS20], there is an efficient unitary U that swaps $|0\rangle |x_0\rangle$ and $|1\rangle |x_1\rangle$ with a non-negligible advantage. By using this unitary, let us consider the following procedure:

1. Given a state $|0\rangle |x_0\rangle \pm |1\rangle |x_1\rangle$, measure it in the computational basis to get $|\alpha\rangle |x_\alpha\rangle$ for random $\alpha \in \{0,1\}$.

2. Apply the unitary U to $|\alpha\rangle |x_\alpha\rangle$ and measure it in the computational basis.

Since U swaps $|0\rangle |x_0\rangle$ and $|1\rangle |x_1\rangle$ with a non-negligible advantage, the probability that the outcome of the second measurement is $|\alpha \oplus 1\rangle |x_{\alpha\oplus 1}\rangle$ is non-negligible. This yields the following observation: If one can efficiently distinguish $|0\rangle |x_0\rangle + |1\rangle |x_1\rangle$ and $|0\rangle |x_0\rangle - |1\rangle |x_1\rangle$, then one can efficiently compute both x_0 and x_1 from $|0\rangle |x_0\rangle \pm |1\rangle |x_1\rangle$. On the other hand, it is easy to show that one cannot compute both x_0 and x_1 from $|0\rangle |x_0\rangle \pm |1\rangle |x_1\rangle$ with a non-negligible probability by a simple information theoretical argument. Thus, the above argument implies security of the above scheme in the restricted setting where no public key and one ciphertext is given to the adversary.

Dealing with public key tampering. We extend the above basic scheme to resist public key tampering attacks. Specifically, we consider the setting where the adversary receives a single copy of the quantum public key from the receiver, sends a tampered quantum public key to the sender, and receives a ciphertext generated under the tampered quantum public key. First, we remark that the basic scheme is insecure if the public key is tampered with since the adversary can replace the public key with $|0\rangle |x'_0\rangle + |1\rangle |x'_1\rangle$ for x'_0, x'_1 of its choice. Indeed, it is impossible to prevent such a man-in-the-middle attack if only untrusted quantum channels are available. Thus, we assume that authenticated classical channels are available similarly to classical PKE.

Our idea is to partially authenticate a quantum public key by using classical digital signatures where its verification key is sent through the authenticated classical channel. Namely, our idea is to set $x_\alpha := \sigma(\alpha)$ for $\alpha \in \{0,1\}$ in the basic construction where $\sigma(\alpha)$ is a signature for $\alpha \in \{0,1\}$, i.e., a quantum public key is

$$|0\rangle |\sigma(0)\rangle + |1\rangle |\sigma(1)\rangle. \tag{3}$$

A secret key is the signing key of the digital signature scheme. Here, we assume that the signature scheme has a deterministic signing algorithm and satisfies strong unforgeability, i.e., given message-signature pairs $(\mathsf{msg}_1, \sigma_1), ..., (\mathsf{msg}_n, \sigma_n)$, no efficient adversary can output $(\mathsf{msg}^*, \sigma^*)$ such that $(\mathsf{msg}^*, \sigma^*) \neq (\mathsf{msg}_i, \sigma_i)$ for all $i \in [n]$.[5] Before encryption, the sender coherently verifies the validity of the signature in the second register of the public key and aborts if the verification rejects. By strong unforgeability of the signature scheme, no matter how the adversary tampers with the public key, the state after passing the verification is negligibly close to a state in the form of

$$c_0 |0\rangle |\sigma(0)\rangle |\Psi_0\rangle + c_1 |1\rangle |\sigma(1)\rangle |\Psi_1\rangle \tag{4}$$

[5]At this point, two-time security (where $n = 2$) suffices but we finally need to allow n to be an arbitrary polynomial.

with some complex coefficients c_0 and c_1, and some states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ over the adversary's register (except for a negligible probability). The encryption of a plaintext $b \in \{0,1\}$ is to apply Z^b on the first qubit of Equation (4). The cipertext generated under the tampered public key is therefore

$$c_0 |0\rangle |\sigma(0)\rangle |\Psi_0\rangle + (-1)^b c_1 |1\rangle |\sigma(1)\rangle |\Psi_1\rangle . \tag{5}$$

By a slight extension of the analysis of the basic scheme, we show that if one can efficiently distinguish $c_0 |0\rangle |\sigma(0)\rangle |\Psi_0\rangle + c_1 |1\rangle |\sigma(1)\rangle |\Psi_1\rangle$ and $c_0 |0\rangle |\sigma(0)\rangle |\Psi_0\rangle - c_1 |1\rangle |\sigma(1)\rangle |\Psi_1\rangle$, then one can efficiently compute both $\sigma(0)$ and $\sigma(1)$. On the other hand, recall that the adversary is only given one copy of the public key $|0\rangle |\sigma(0)\rangle + |1\rangle |\sigma(1)\rangle$. We can show that it is impossible to compute both $\sigma(0)$ and $\sigma(1)$ from this state by the strong unforgeability as follows. By [BZ13, Lemma 2.1], the probability to output both $\sigma(0)$ and $\sigma(1)$ is only halved even if $|0\rangle |\sigma(0)\rangle + |1\rangle |\sigma(1)\rangle$ is measured in the computational basis before given to the adversary. After the measurement, the adversary's input collapses to a classical state $|\alpha\rangle |\sigma(\alpha)\rangle$ for random $\alpha \in \{0,1\}$, in which case the adversary can output $\sigma(\alpha \oplus 1)$ only with a negligible probability by the strong unforgeability. Combining the above, security of the above scheme under tampered public keys is proven.

Multiple public keys. In the previous paragraph, we give only one copy of the quantum public key to the adversary. It is clear that the security is broken if two copies of the public key are available to the adversary: by measuring each public key, the adversary can learn both $\sigma(0)$ and $\sigma(1)$ with probability 1/2. The construction in the previous paragraph therefore cannot achieve an important advantage of PKE, namely, many public keys corresponding to a single secret key can be distributed. In order to extend the above scheme to ensure security even if the adversary can obtain multiple public keys, we introduce a classical randomness for each public key generation. Specifically, a public key is

$$(r, |0\rangle |\sigma(0,r)\rangle + |1\rangle |\sigma(1,r)\rangle) \tag{6}$$

where $r \in \{0,1\}^\lambda$ is chosen uniformly at random for every execution of the public key generation algorithm, and $\sigma(\alpha, r)$ is a signature for $\alpha \| r$.[6] A secret key is the signing key of the digital signature scheme, and an encryption of a plaintext $b \in \{0,1\}$ is

$$(r, |0\rangle |\sigma(0,r)\rangle + (-1)^b |1\rangle |\sigma(1,r)\rangle). \tag{7}$$

Since each quantum public key uses different r, security of this scheme holds even if the adversary obtains arbitrarily many public keys. Note that the receiver does not need to remember each r. What the receiver has to record is only a single secret key that is the same for all public keys.

Making ciphertext classical and recycling public key. Finally, we extend the scheme so that one quantum public key can be used to encrypt many plaintexts. Toward the goal, we first observe that the ciphertext of the above scheme can be made classical. In the above construction, the ciphertext contains a quantum state $|0\rangle |\sigma(r,0)\rangle + (-1)^b |1\rangle |\sigma(r,1)\rangle$. Suppose that we measure this state in Hadamard basis and let d be the measurement outcome. Then an easy calculation shows that we have

$$b = d \cdot (0 \| \sigma(0,r) \oplus 1 \| \sigma(1,r)). \tag{8}$$

Thus, sending (r, d) as a ciphertext is sufficient for the receiver to recover the plaintext b. Moreover, this variant is at least as secure as the original one with quantum ciphertexts since the Hadamard-basis measurement only loses information of the ciphertext.

[6] $\alpha \| r$ is the concatenation of two bit strings α and r.

Given the above observation, it is straightforward to use one quantum public key to encrypt many plaintexts by standard hybrid encryption. When a sender encrypts a message msg for the first time, it generates a key K of a symmetric key encryption scheme, encrypt each bit of K by the above scheme in a bit-by-bit manner, and encrypt msg by the symmetric key encryption scheme under the key K. Since the encryption of K is classical, the sender can reuse it when it encrypts another message later. We formalize this construction as a *recyclable* QPKE.[7]

Adding decryption error detectability. So far, we are only concerned with security under tampered public keys (IND-pkTA security). On the other hand, the schemes presented in the previous paragraphs do not satisfy decryption error detectability. (See Section 1.2 for its informal definition and Definition 3.3 for formal definition.) Fortunately, there is a simple generic conversion that adds decryption error detectability while preserving IND-pkTA security by using digital signatures. The idea is that the encryption algorithm first generates a signature for the message under a signing key generated by itself, encrypts both the original message and signature under the building block scheme, and outputs the ciphertexts along with the verification key for the signature scheme in the clear. Then, the decryption algorithm can verify that the decryption result is correct as long as it is a valid message-signature pair (except for a negligible probability).

1.5 Related Works

The possibility that QPKE can be achieved from weaker assumptions was first pointed out by Gottesman [Got], though he did not give any concrete construction. The first concrete construction of QPKE was proposed by Kawachi, Koshiba, Nishimura, and Yamakami [KKNY05]. They formally defined the notion of QPKE with quantum public keys, and provided a construction satisfying it from a distinguishing problem of two quantum states. Recently, Morimae and Yamakawa [MY22a] pointed out that QPKE defined by [KKNY05] can be achieved from any classical or quantum symmetric key encryption almost trivially. The constructions proposed in these two works have mixed state quantum public keys. Then, subsequent works [Col23, BMW23, GSV23] independently studied the question whether QPKE with pure state quantum public keys can be constructed from OWFs or even weaker assumptions.

The definition of QPKE studied in the above works essentially assume that a sender can obtain intact quantum public keys. As far as we understand, this requires unsatisfactory physical setup assumptions such as secure quantum channels or tamper-proof quantum hardware, regardless of whether the quantum public keys are pure states or mixed states. In our natural setting where an adversary can touch the quantum channel where quantum public keys are sent, the adversary can easily attack the previous constructions by simply replacing the quantum public key on the channel with the one generated by itself that the adversary knows the corresponding secret key. We need to take such adversarial behavior into consideration, unless we assume physical setup assumptions that deliver intact quantum public keys to the sender. Our work is the first one that proposes a QPKE scheme secure in this natural setting assuming only classical authenticated channels that is the same assumption as classical PKE and can be implemented by digital signature schemes. It is unclear if we could solve the problem in the previous constructions by using classical authenticated channels similarly to our work. Below, we review the constructions of QPKE from OWFs proposed in the recent works.

The construction by Morimae and Yamakawa [MY22a] is highly simple. A (mixed state) public key of their construction is of the form $(\mathsf{ct}_0, \mathsf{ct}_1)$, where ct_b is an encryption of b by a symmetric key encryption scheme. The encryption algorithm with input message b simply outputs ct_b.

[7] Such a recyclable property is a default requirement in [GSV23], and our definition is similar to theirs with the important difference that we consider public key tampering. The idea to achieve the recyclability by the hybrid encryption technique was also used in one of their constructions.

Coladangelo [Col23] constructed a QPKE scheme with quantum public keys and quantum ciphertexts from pseudorandom functions (PRFs), which are constructed from OWFs. The public key is

$$|\mathsf{pk}\rangle := \sum_y (-1)^{\mathsf{PRF}_k(y)} |y\rangle , \tag{9}$$

and the secret key is k. The ciphertext for the plaintext m is

$$(Z^x |\mathsf{pk}\rangle = \sum_y (-1)^{x\cdot y+\mathsf{PRF}_k(y)} |y\rangle , r, r\cdot x \oplus m), \tag{10}$$

where r is chosen uniformly at random.

Barooti, Malavolta, and Walter [BMW23] constructed a QPKE scheme with quantum public keys and classical ciphertexts from PRFs. The public key is $|\mathsf{pk}\rangle := (|\mathsf{pk}_0\rangle , |\mathsf{pk}_1\rangle)$, where

$$|\mathsf{pk}_b\rangle := \sum_x |x\rangle |\mathsf{PRF}_{k_b}(x)\rangle , \tag{11}$$

and the secret key is (k_0, k_1). The encryption algorithm measures $|\mathsf{pk}_b\rangle$ in the computational basis and sends the measurement result as the ciphertext when the plaintext is $b \in \{0, 1\}$. Barooti et al. showed that this construction is a QPKE scheme for the plaintext space $\{0, 1\}$ that satisfies chosen ciphertext security (as long as intact quantum public keys are securely transmitted to the sender).

Grilo, Sattath, and Vu [GSV23] constructed three QPKE schemes with quantum public keys from OWFs or pseudorandom function-like states generators. We review their construction based on OWFs. The public key is

$$|\mathsf{pk}\rangle := \sum_x |x\rangle |\mathsf{PRF}_k(x)\rangle , \tag{12}$$

and the secret key is k. The encryption algorithm first measures $|\mathsf{pk}\rangle$ in the computational basis to get $(x, \mathsf{PRF}_k(x))$ and outputs $(x, \mathsf{SKE.Enc}(\mathsf{PRF}_k(x), m))$ as the ciphertext for the plaintext m, where $\mathsf{SKE.Enc}$ is the encryption algorithm of a symmetric key encryption scheme.

We finally compare Quantum Key Distribution (QKD) [BB84] with our notion of QPKE. QKD also enables us to establish secure communication over an untrusted quantum channel assuming that an authenticated classical channel is available similarly to our QPKE. An advantage of QKD is that it is information theoretically secure and does not need any computational assumption. On the other hand, it has disadvantages that it must be interactive and parties must record secret information for each session. Thus, it is incomparable to the notion of QPKE.

1.6 Open Problems

In our construction, public keys are quantum states. It is an open problem whether QPKE with classical public keys are possible from OWFs. Another interesting open problem is whether we can construct QPKE defined in this work from an even weaker assumption than OWFs such as pseudorandom states generators.

In our model of QPKE, a decryption error could occur frequently as a result of tampering attacks on the quantum public key. To address this issue, we introduce the security notion we call decryption error detectability that guarantees that a legitimate receiver of a ciphertext can notice if the decrypted message is different from the message intended by the sender. We could consider even stronger variant of decryption error detectability that requires that a sender can notice if a given quantum public key does not provide decryption correctness. It is an open problem to construct a QPKE scheme satisfying such a stronger decryption error detectability.

2 Preliminaries

2.1 Basic Notations

We use the standard notations of quantum computing and cryptography. We use λ as the security parameter. For any set S, $x \leftarrow S$ means that an element x is sampled uniformly at random from the set S. We write negl to mean a negligible function. PPT stands for (classical) probabilistic polynomial-time and QPT stands for quantum polynomial-time. For an algorithm A, $y \leftarrow A(x)$ means that the algorithm A outputs y on input x. For two bit strings x and y, $x\|y$ means the concatenation of them. For simplicity, we sometimes omit the normalization factor of a quantum state. (For example, we write $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$ just as $|x_0\rangle + |x_1\rangle$.) $I := |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. For the notational simplicity, we sometimes write $I^{\otimes n}$ just as I when the dimension is clear from the context.

2.2 Digital Signatures

Definition 2.1 (Digital signatures). *A digital signature scheme is a set of algorithms* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *such that*

- $\mathsf{Gen}(1^\lambda) \to (k, \mathsf{vk})$: *It is a PPT algorithm that, on input the security parameter λ, outputs a signing key k and a verification key* vk.
- $\mathsf{Sign}(k, \mathsf{msg}) \to \sigma$: *It is a PPT algorithm that, on input the message* msg *and k, outputs a signature σ.*
- $\mathsf{Ver}(\mathsf{vk}, \mathsf{msg}, \sigma) \to \top/\bot$: *It is a deterministic classical polynomial-time algorithm that, on input* vk, msg, *and σ, outputs $\top/\bot$.*

We require the following correctness and strong EUF-CMA security.

Correctness: *For any* msg,

$$\Pr[\top \leftarrow \mathsf{Ver}(\mathsf{vk}, \mathsf{msg}, \sigma) : (k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda), \sigma \leftarrow \mathsf{Sign}(k, \mathsf{msg})] \geq 1 - \mathsf{negl}(\lambda). \tag{13}$$

Strong EUF-CMA security: *For any QPT adversary $\mathcal{A}$ with classical oracle access to the signing oracle* $\mathsf{Sign}(k, \cdot)$,

$$\Pr[(\mathsf{msg}^*, \sigma^*) \notin \mathcal{Q} \wedge \top \leftarrow \mathsf{Ver}(\mathsf{vk}, \mathsf{msg}^*, \sigma^*) : (k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda), (\mathsf{msg}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(k,\cdot)}(\mathsf{vk})] \leq \mathsf{negl}(\lambda), \tag{14}$$

where $\mathcal{Q}$ is the set of message-signature pairs returned by the signing oracle.

Remark 2.2. Without loss of generality, we can assume that Sign is deterministic. (The random seed used for Sign can be generated by applying a PRF on the message signed, and the key of PRF is appended to the signing key.)

Theorem 2.3 ([Gol04, Sec. 6.5.2]). *Strong EUF-CMA secure digital signatures exist if OWFs exist.*

2.3 Symmetric Key Encryption

Definition 2.4 (Symmetric Key Encryption (SKE)). *A (classical) symmetric key encryption (SKE) scheme with message space* $\{0,1\}^\ell$ *is a set of algorithms* $(\mathsf{Enc}, \mathsf{Dec})$ *such that*

- $\mathsf{Enc}(K, \mathsf{msg}) \to \mathsf{ct}$: *It is a PPT algorithm that, on input* $K \in \{0,1\}^\lambda$ *and the message* $\mathsf{msg} \in \{0,1\}^\ell$*, outputs a ciphertext* ct.
- $\mathsf{Dec}(K, \mathsf{ct}) \to \mathsf{msg}'$: *It is a deterministic classical polynomial-time algorithm that, on input* K *and* ct*, outputs* msg'.

We require the following correctness and IND-CPA security.

Correctness: *For any* $\mathsf{msg} \in \{0,1\}^\ell$,

$$\Pr[\mathsf{msg} \leftarrow \mathsf{Dec}(K, \mathsf{ct}) : K \leftarrow \{0,1\}^\lambda, \mathsf{ct} \leftarrow \mathsf{Enc}(K, \mathsf{msg})] = 1. \tag{15}$$

IND-CPA Security: *For any QPT adversary* $\mathcal{A}$ *with classical oracle access to the encryption oracle* $\mathsf{Enc}(K, \cdot)$,

$$\Pr\left[b \leftarrow \mathcal{A}(\mathsf{ct}, \mathsf{st}) : \begin{array}{r} K \leftarrow \{0,1\}^\lambda \\ (\mathsf{msg}_0, \mathsf{msg}_1, \mathsf{st}) \leftarrow \mathcal{A}^{\mathsf{Enc}(K,\cdot)}(1^\lambda) \\ b \leftarrow \{0,1\} \\ \mathsf{ct} \leftarrow \mathsf{Enc}(K, \mathsf{msg}_b) \end{array} \right] \leq \frac{1}{2} + \mathsf{negl}(\lambda). \tag{16}$$

Remark 2.5. IND-CPA secure SKE exists if OWFs exist [GGM86, HILL99].

2.4 Lemma by Boneh and Zhandry

In this paper, we use the following lemma by Boneh and Zhandry [BZ13].

Lemma 2.6 ([BZ13, Lemma 2.1]). *Let* A *be a quantum algorithm, and let* $\Pr[x]$ *be the probability that* A *outputs* x*. Let* A' *be another quantum algorithm obtained from* A *by pausing* A *at an arbitrary stage of execution, performing a partial measurement that obtains one of* k *outcomes, and then resuming* A*. Let* $\Pr'[x]$ *be the probability that* A' *outputs* x*. Then* $\Pr'[x] \geq \Pr[x]/k$.

3 Definition of QPKE

In this section, we define QPKE that can be used in the setting where quantum unauthenticated channels and classical authenticated channels are available. The difference on the syntax from the previous definitions is as follows.

- The secret key generation algorithm outputs a classical verification key together with the secret key.
- The verification key is given to the encryption algorithm together with a quantum public key and a message so that the encryption algorithm can check the validity of the given quantum public key.

We require a QPKE scheme to satisfy the security notion that we call IND-pkTA security. It roughly guarantees that indistinguishability holds even if messages are encrypted by a public key tampered with by an adversary. The formal definition is as follows.

Definition 3.1 (Quantum Public-Key Encryption (QPKE)). *A quantum public-key encryption scheme with message space* $\{0,1\}^\ell$ *is a set of algorithms* $(\mathsf{SKGen}, \mathsf{PKGen}, \mathsf{Enc}, \mathsf{Dec})$ *such that*

- $\mathsf{SKGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{vk})$: *It is a PPT algorithm that, on input the security parameter* λ*, outputs a classical secret key* sk *and a classical verification key* vk.
- $\mathsf{PKGen}(\mathsf{sk}) \to \mathsf{pk}$: *It is a QPT algorithm that, on input* sk*, outputs a quantum public key* pk.
- $\mathsf{Enc}(\mathsf{vk}, \mathsf{pk}, \mathsf{msg}) \to \mathsf{ct}$: *It is a QPT algorithm that, on input* vk*,* pk*, and a plaintext* $\mathsf{msg} \in \{0,1\}^\ell$*, outputs a classical ciphertext* ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{msg}'$: *It is a classical deterministic polynomial-time algorithm that, on input* sk *and* ct*, outputs* $\mathsf{msg}' \in \{0,1\}^\ell \cup \{\bot\}$.

We require the following correctness and IND-pkTA security.

Correctness: *For any* $\mathsf{msg} \in \{0,1\}^\ell$,

$$\Pr[\mathsf{msg} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) : (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda), \mathsf{pk} \leftarrow \mathsf{PKGen}(\mathsf{sk}), \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{vk}, \mathsf{pk}, \mathsf{msg})] \geq 1 - \mathsf{negl}(\lambda). \tag{17}$$

IND-pkTA Security: *For any polynomial* m*, and any QPT adversary* $\mathcal{A}$,

$$\Pr\left[b \leftarrow \mathcal{A}(\mathsf{ct}^*, \mathsf{st}) : \begin{array}{r} (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda) \\ \mathsf{pk}_1, ..., \mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m} \\ (\mathsf{pk}', \mathsf{msg}_0, \mathsf{msg}_1, \mathsf{st}) \leftarrow \mathcal{A}(\mathsf{vk}, \mathsf{pk}_1, ..., \mathsf{pk}_m) \\ b \leftarrow \{0,1\} \\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{vk}, \mathsf{pk}', \mathsf{msg}_b) \end{array} \right] \leq \frac{1}{2} + \mathsf{negl}(\lambda). \tag{18}$$

Here, $\mathsf{pk}_1, ..., \mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m}$ *means that* PKGen *is executed* m *times and* pk_i *is the output of the* i*th execution of* PKGen. st *is a quantum internal state of* $\mathcal{A}$*, which can be entangled with* pk'.

As we discussed in Section 1.3, the above definition does not require the quantum public key pk to be a pure state.

Remark 3.2. IND-pkTA security captures the setting where the classical verification key is sent via a classical authenticated channel and thus everyone can obtain correct verification key, but a quantum public key is sent via an unauthenticated quantum channel and thus can be tampered with by an adversary. Especially, it captures an adversary $\mathcal{A}$ who steals a quantum public key pk sent to a user, replace it with a tampered one pk', and try to break the secrecy of a message encrypted by pk'. To capture wide range of usage scenarios, we give multiple copies of the quantum public keys $\mathsf{pk}_1, ..., \mathsf{pk}_m$ to $\mathcal{A}$.

We also define a security notion related to the correctness notion that we call decryption error detectability. It roughly guarantees that a legitimate receiver of a ciphertext can notice if the decrypted message is different from the message intended by the sender. Such a decryption error could occur frequently in our setting as a result of the tampering attacks on the quantum public key sent via an unauthenticated quantum channel. Note that our definition of QPKE requires a ciphertext of QPKE be a classical string and we assume every classical information is sent though a classical authenticated channel. Thus, similarly to the verification key, we can assume that ciphertexts can be sent without being tampered. The formal definition is as follows.

Definition 3.3 (Decryption error detectability). *We say that a QPKE scheme has decryption error detectability if for any polynomial m, and any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\mathsf{msg}' \neq \bot \ \wedge\ \mathsf{msg}' \neq \mathsf{msg} : \begin{array}{r} (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda) \\ \mathsf{pk}_1, ..., \mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m} \\ (\mathsf{pk}', \mathsf{msg}) \leftarrow \mathcal{A}(\mathsf{vk}, \mathsf{pk}_1, ..., \mathsf{pk}_m) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{vk}, \mathsf{pk}', \mathsf{msg}) \\ \mathsf{msg}' \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \end{array}\right] \leq \mathsf{negl}(\lambda). \tag{19}$$

It is easy to see that we can generically add decryption error detectability by letting the sender generate a signature for the message under a signing key generated by itself, encrypt the concatenation of the message and signature, and send the ciphertext along with the verification key of the signature to the receiver. The receiver can check that there is no decryption error (except for a negligible probability) if the decryption result is a valid message-signature pair. That is, we have the following theorem.

Theorem 3.4. *If there exist OWFs and a QPKE scheme that satisfies correctness and IND-pkTA security, there exists a QPKE scheme that satisfies correctness, IND-pkTA security, and decryption error detectability.*

We omit the proof since it is straightforward by the construction explained above. Since we have this theorem, we focus on constructing QPKE that satisfies correctness and IND-pkTA security in the rest of this paper.

4 Construction of QPKE

In this section, we construct a QPKE scheme that satisfies correctness and IND-pkTA security (but not decryption error detectability) from strong EUF-CMA secure digital signatures. The message space of our construction is $\{0,1\}$, but it can be extended to be arbitrarily many bits by parallel repetition. Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ be a strong EUF-CMA secure digital signature scheme with a deterministic Sign algorithm and message space $\{0,1\}^u$ for $u = \omega(\log \lambda)$.

Our construction of QPKE is as follows.

- $\mathsf{SKGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{vk})$: Run $(k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$. Output $\mathsf{sk} := k$. Output vk.
- $\mathsf{PKGen}(\mathsf{sk}) \to \mathsf{pk}$: Parse $\mathsf{sk} = k$. Choose $r \leftarrow \{0,1\}^u$. By running Sign coherently, generate the state
$$|\psi_r\rangle := |0\rangle_{\mathbf{A}} \otimes |\mathsf{Sign}(k, 0\|r)\rangle_{\mathbf{B}} + |1\rangle_{\mathbf{A}} \otimes |\mathsf{Sign}(k, 1\|r)\rangle_{\mathbf{B}} \tag{20}$$
over registers $(\mathbf{A}, \mathbf{B})$. Output
$$\mathsf{pk} := (r, |\psi_r\rangle). \tag{21}$$
- $\mathsf{Enc}(\mathsf{vk}, \mathsf{pk}, b) \to \mathsf{ct}$: Parse $\mathsf{pk} = (r, \rho)$, where ρ is a quantum state over registers $(\mathbf{A}, \mathbf{B})$. The Enc algorithm consists of the following three steps.
  1. It coherently checks the signature in ρ. In other words, it applies the unitary
  $$U_{r,\mathsf{vk}} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |0...0\rangle_{\mathbf{D}} = |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\mathsf{Ver}(\mathsf{vk}, \alpha\|r, \beta)\rangle_{\mathbf{D}} \tag{22}$$
  on $\rho_{\mathbf{A},\mathbf{B}} \otimes |0...0\rangle\langle 0...0|_{\mathbf{D}}$,[8] and measures the register $\mathbf{D}$ in the computational basis. If the result is $\bot$, it outputs $\mathsf{ct} := \bot$ and halts. If the result is $\top$, it goes to the next step.

[8] $\mathbf{C}$ is skipped, because $\mathbf{C}$ will be used later.

2. It applies Z^b on the register $\mathbf{A}$.
3. It measures all qubits in the registers $(\mathbf{A}, \mathbf{B})$ in the Hadamard basis to get the result d. It outputs

$$\mathsf{ct} := (r, d). \tag{23}$$

- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to b'$: Parse $\mathsf{sk} = k$ and $\mathsf{ct} = (r, d)$. Output

$$b' := d \cdot (0\|\mathsf{Sign}(k, 0\|r) \oplus 1\|\mathsf{Sign}(k, 1\|r)). \tag{24}$$

Theorem 4.1. *If* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is a strong EUF-CMA secure digital signature scheme, then the QPKE scheme* $(\mathsf{SKGen}, \mathsf{PKGen}, \mathsf{Enc}, \mathsf{Dec})$ *above is correct and IND-pkTA secure.*

The correctness is straightforward. First, the state over the registers $(\mathbf{A}, \mathbf{B})$ is $|\psi_r\rangle$ if pk was not tampered with and the first step of Enc algorithm got $\top$. Second, in that case, the state becomes

$$|0\rangle |\mathsf{Sign}(k, 0\|r)\rangle + (-1)^b |1\rangle |\mathsf{Sign}(k, 1\|r)\rangle \tag{25}$$

after the second step of Enc algorithm. Finally, because in that case d obtained in the third step of Enc algorithm satisfies

$$b = d \cdot (0\|\mathsf{Sign}(k, 0\|r) \oplus 1\|\mathsf{Sign}(k, 1\|r)), \tag{26}$$

we have $b' = b$.

We prove IND-pkTA security in the next section.

5 Proof of IND-pkTA Security

In this section, we show IND-pkTA security of our construction to complete the proof of Theorem 4.1. The outline of the proof is as follows. The security game for the IND-pkTA security of our QPKE (Hybrid 0) is given in Figure 1. We introduce two more hybrids, Hybrid 1 (Figure 2) and Hybrid 2 (Figure 3). Hybrid 1 is the same as Hybrid 0 except that the challenger does not do the Hadamard-basis measurement in the third step of Enc algorithm, and the challenger sends the adversary r and the state over the registers $(\mathbf{A}, \mathbf{B})$. Hybrid 2 is the same as Hybrid 1 except that the adversary outputs two bit strings μ_0, μ_1 and the adversary wins if $\mu_0 = \mathsf{Sign}(k, 0\|r)$ and $\mu_1 = \mathsf{Sign}(k, 1\|r)$. The formal proof is as follows.

Assume that the IND-pkTA security of our construction is broken by a QPT adversary $\mathcal{A}$. It means the QPT adversary $\mathcal{A}$ wins Hybrid 0 with a non-negligible advantage. Then, it is clear that there is another QPT adversary $\mathcal{A}'$ that wins Hybrid 1 with a non-negligible advantage. ($\mathcal{A}'$ has only to do the Hadamard-basis measurement by itself.) From the $\mathcal{A}'$, we can construct a QPT adversary $\mathcal{A}''$ that wins Hybrid 2 with a non-negligible probability by using the idea of [HMY22]. (For details, see Section 5.1). Finally, we show in Section 5.2 that no QPT adversary can win Hybrid 2 except for a negligible probability. We thus have the contradiction, and therefore our QPKE is IND-pkTA secure.

5.1 From Distinguishing to Outputting Two Signatures

We present the construction of $\mathcal{A}''$. Assume that there exists a QPT adversary $\mathcal{A}'$ and a polynomial p such that

$$|\Pr[1 \leftarrow \mathcal{A}' \mid b = 0] - \Pr[1 \leftarrow \mathcal{A}' \mid b = 1]| \geq \frac{1}{p(\lambda)} \tag{28}$$

Hybrid 0

1. $\mathcal{C}$ runs $(k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$. $\mathcal{C}$ sends vk to $\mathcal{A}$.
2. $\mathcal{C}$ chooses $r_1, ..., r_m \leftarrow \{0,1\}^u$.
3. $\mathcal{C}$ sends $\{(r_i, |\psi_{r_i}\rangle)\}_{i=1}^m$ to the adversary $\mathcal{A}$, where

$$|\psi_{r_i}\rangle := |0\rangle \otimes |\mathsf{Sign}(k, 0\|r_i)\rangle + |1\rangle \otimes |\mathsf{Sign}(k, 1\|r_i)\rangle . \tag{27}$$

4. $\mathcal{A}$ generates a quantum state over registers $(\mathbf{A}, \mathbf{B}, \mathbf{C})$. ($(\mathbf{A}, \mathbf{B})$ corresponds to the quantum part of pk', and $\mathbf{C}$ corresponds to st.) $\mathcal{A}$ sends a bit string r and the registers $(\mathbf{A}, \mathbf{B})$ to $\mathcal{C}$. $\mathcal{A}$ keeps the register $\mathbf{C}$.
5. $\mathcal{C}$ coherently checks the signature in the state sent from $\mathcal{A}$. If the result is $\perp$, it sends $\perp$ to $\mathcal{A}$ and halts. If the result is $\top$, it goes to the next step.
6. $\mathcal{C}$ chooses $b \leftarrow \{0,1\}$. $\mathcal{C}$ applies Z^b on the register $\mathbf{A}$.
7. $\mathcal{C}$ measures all qubits in $(\mathbf{A}, \mathbf{B})$ in the Hadamard basis to get the result d. $\mathcal{C}$ sends (r, d) to $\mathcal{A}$.
8. $\mathcal{A}$ outputs b'. If $b' = b$, $\mathcal{A}$ wins.

Figure 1: Hybrid 0

Hybrid 1

1.-6. All the same as Figure 1.

7. $\mathcal{C}$ does not do the Hadamard-basis measurement, and $\mathcal{C}$ sends r and registers $(\mathbf{A}, \mathbf{B})$ to $\mathcal{A}$.
8. The same as Figure 1.

Figure 2: Hybrid 1

in Hybrid 1 (Figure 2) for all $\lambda \in I$ with an infinite set I. From the $\mathcal{A}'$, we construct a QPT adversary $\mathcal{A}''$ such that

$$\Pr[(\mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathcal{A}''] \geq \frac{1}{q(\lambda)} \tag{29}$$

in Hybrid 2 (Figure 3) with a polynomial q for infinitely many λ.

Let $t := (k, \mathsf{vk}, r_1, ..., r_m, r)$, and $\Pr[t]$ be the probability that t is generated in Item 1, Item 2, and Item 4 in the game of Figure 2. Let Good be the event that $\mathcal{C}$ gets $\top$ in Item 5 in the game of Figure 2. Let Bad be the event that Good does not occur. Then, from Equation (28), we have

$$\begin{aligned}
\frac{1}{p(\lambda)} \leq \Big| &\sum_t \Pr[t] \Pr[\mathsf{Good} \mid t] \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=0] + \sum_t \Pr[t] \Pr[\mathsf{Bad} \mid t] \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Bad}, b=0] \\
&- \sum_t \Pr[t] \Pr[\mathsf{Good} \mid t] \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=1] - \sum_t \Pr[t] \Pr[\mathsf{Bad} \mid t] \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Bad}, b=1] \Big| \qquad (30) \\
\leq &\sum_t \Pr[t] \Pr[\mathsf{Good} \mid t] \Big| \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=1] \Big| \\
&+ \sum_t \Pr[t] \Pr[\mathsf{Bad} \mid t] \Big| \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Bad}, b=0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Bad}, b=1] \Big| \qquad (31) \\
= &\sum_t \Pr[t] \Pr[\mathsf{Good} \mid t] \Big| \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b=1] \Big| \qquad (32)
\end{aligned}$$

Hybrid 2

1.-7. All the same as Figure 2.

8. $\mathcal{A}$ outputs (μ_0, μ_1). If $\mu_0 = \mathsf{Sign}(k, 0\|r)$ and $\mu_1 = \mathsf{Sign}(k, 1\|r)$, $\mathcal{A}$ wins.

Figure 3: Hybrid 2

for all $\lambda \in I$, because if Bad occurs, $\mathcal{A}'$ gets only $\perp$ which contains no information about b. (Here, we often abuse notation to just write t to mean the event that t is generated in Item 1, Item 2, and Item 4.) Therefore, if we define

$$T_\lambda := \Big\{t : \Pr[\mathsf{Good} \mid t] \cdot \Big|\Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 1]\Big| \geq \frac{1}{2p(\lambda)}\Big\}, \quad (33)$$

we have, for all $\lambda \in I$,

$$\Pr[\mathsf{Good} \mid t] \geq \frac{1}{4p(\lambda)} \quad (34)$$

and

$$\Big|\Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 1]\Big| \geq \frac{1}{2p(\lambda)} \quad (35)$$

for any $t \in T_\lambda$ and

$$\sum_{t \in T_\lambda} \Pr[t] \geq \frac{1}{2p(\lambda)}. \quad (36)$$

Let $|\phi_b^{t,good}\rangle$ be the state over the registers $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ immediately before Item 8 of Figure 2 given that t is generated, Good occurred, and b is chosen in Item 6 of Figure 2. We can show the following lemma. (Its proof is given later.)

Lemma 5.1. *If* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is strong EUF-CMA secure, there exists a subset* $T'_\lambda \subseteq T_\lambda$ *such that the following is satisfied for all* $\lambda \in I'$*, where* $I' := \{\lambda \in I : \lambda \geq \lambda_0\}$ *with a certain* λ_0.

- $\sum_{t \in T'_\lambda} \Pr[t] \geq \frac{1}{4p(\lambda)}$.
- *For any* $t \in T'_\lambda$, $|\phi_b^{t,good}\rangle$ *is close to a state*

$$|\tilde{\phi}_b^{t,good}\rangle := c_0 |0\rangle_{\mathbf{A}} |\mathsf{Sign}(k, 0\|r)\rangle_{\mathbf{B}} |\Psi_0\rangle_{\mathbf{C}} + (-1)^b c_1 |1\rangle_{\mathbf{A}} |\mathsf{Sign}(k, 1\|r)\rangle_{\mathbf{B}} |\Psi_1\rangle_{\mathbf{C}} \quad (37)$$

within the trace distance $\frac{1}{p^{10}(\lambda)}$*, where* c_0 *and* c_1 *are some complex coefficients such that* $|c_0|^2 + |c_1|^2 = 1$*, and* $|\Psi_0\rangle$ *and* $|\Psi_1\rangle$ *are some normalized states.*

Now let us fix $t \in T'_\lambda$. Also, assume that Good occurred. Because $T'_\lambda \subseteq T_\lambda$, it means that $t \in T_\lambda$. Then, from Equation (35),

$$\Big|\Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 0] - \Pr[1 \leftarrow \mathcal{A}' \mid t, \mathsf{Good}, b = 1]\Big| = \Delta \quad (38)$$

for a non-negligible $\Delta \geq \frac{1}{2p(\lambda)}$ for all $\lambda \in I$. Without loss of generality, we can assume that in Item 8 of Figure 2, $\mathcal{A}'$ applies a unitary V on the state $|\phi_b^{t,good}\rangle$, and measures the register $\mathbf{A}$ in the computational basis to get $b' \in \{0,1\}$. By Equation (38) we have

$$V|\phi_0^{t,good}\rangle = \sqrt{p}\,|1\rangle_{\mathbf{A}}|\nu_1\rangle_{\mathbf{B},\mathbf{C}} + \sqrt{1-p}\,|0\rangle_{\mathbf{A}}|\nu_0\rangle_{\mathbf{B},\mathbf{C}} \tag{39}$$

$$V|\phi_1^{t,good}\rangle = \sqrt{1-p+\Delta}\,|0\rangle_{\mathbf{A}}|\xi_0\rangle_{\mathbf{B},\mathbf{C}} + \sqrt{p-\Delta}\,|1\rangle_{\mathbf{A}}|\xi_1\rangle_{\mathbf{B},\mathbf{C}} \tag{40}$$

for some real number p and some normalized states $|\nu_0\rangle, |\nu_1\rangle, |\xi_0\rangle, |\xi_1\rangle$. (This is because any state can be written as $p|1\rangle|\nu_1\rangle + \sqrt{1-p}\,|0\rangle|\nu_0\rangle$ with some p and normalized states $|\nu_0\rangle, |\nu_1\rangle$, and due to Equation (38), the coefficients of $|1\rangle|\xi_1\rangle$ has to be $\sqrt{p-\Delta}$.) If we define W as

$$W := V^\dagger(Z\otimes I)V, \tag{41}$$

we have

$$|\langle\tilde{\phi}_b^{t,good}|W|\tilde{\phi}_b^{t,good}\rangle - \langle\phi_b^{t,good}|W|\phi_b^{t,good}\rangle| \leq \frac{2}{p^{10}(\lambda)} \tag{42}$$

for all $\lambda \in I'$ from Lemma 5.1. Therefore,

$$|c_0^* c_1 \langle 0|\langle \mathsf{Sign}(k,0\|r)|\langle\Psi_0|W|1\rangle|\mathsf{Sign}(k,1\|r)\rangle|\Psi_1\rangle \tag{43}$$

$$+ c_0 c_1^* \langle 1|\langle \mathsf{Sign}(k,1\|r)|\langle\Psi_1|W|0\rangle|\mathsf{Sign}(k,0\|r)\rangle|\Psi_0\rangle| \tag{44}$$

$$= \frac{1}{4}|(\langle\tilde{\phi}_0^{t,good}| + \langle\tilde{\phi}_1^{t,good}|)W(|\tilde{\phi}_0^{t,good}\rangle - |\tilde{\phi}_1^{t,good}\rangle) \tag{45}$$

$$+ (\langle\tilde{\phi}_0^{t,good}| - \langle\tilde{\phi}_1^{t,good}|)W(|\tilde{\phi}_0^{t,good}\rangle + |\tilde{\phi}_1^{t,good}\rangle)| \tag{46}$$

$$= \frac{1}{2}|\langle\tilde{\phi}_0^{t,good}|W|\tilde{\phi}_0^{t,good}\rangle - \langle\tilde{\phi}_1^{t,good}|W|\tilde{\phi}_1^{t,good}\rangle| \tag{47}$$

$$\geq \frac{1}{2}|\langle\phi_0^{t,good}|W|\phi_0^{t,good}\rangle - \langle\phi_1^{t,good}|W|\phi_1^{t,good}\rangle| - \frac{2}{p^{10}(\lambda)} \tag{48}$$

$$\begin{aligned}= \frac{1}{2}\Big|&\Big(\sqrt{p}\langle 1|\langle\nu_1| + \sqrt{1-p}\langle 0|\langle\nu_0|\Big)\Big(-\sqrt{p}|1\rangle|\nu_1\rangle + \sqrt{1-p}|0\rangle|\nu_0\rangle\Big) \\ &- \Big(\sqrt{1-p+\Delta}\langle 0|\langle\xi_0| + \sqrt{p-\Delta}\langle 1|\langle\xi_1|\Big)\Big(\sqrt{1-p+\Delta}|0\rangle|\xi_0\rangle - \sqrt{p-\Delta}|1\rangle|\xi_1\rangle\Big)\Big| - \frac{2}{p^{10}(\lambda)}\end{aligned} \tag{49}$$

$$= \frac{1}{2}|-p + (1-p) - (1-p+\Delta) + (p-\Delta)| - \frac{2}{p^{10}(\lambda)} \tag{50}$$

$$= \Delta - \frac{2}{p^{10}(\lambda)} \tag{51}$$

$$\geq \frac{1}{2p(\lambda)} - \frac{2}{p^{10}(\lambda)} \tag{52}$$

$$\geq \frac{1}{p(\lambda)} \tag{53}$$

for all $\lambda \in I'$. Here, Equation (48) follows from Equation (42), and Equation (49) follows from Equations (39) and (40) and the definition of W. From the triangle inequality and the facts that $|c_0| \leq 1$ and $|c_1| \leq 1$,

$$\frac{1}{p(\lambda)} \leq |c_1| \cdot |\langle 0|\langle \mathsf{Sign}(k,0\|r)|\langle\Psi_0|W|1\rangle|\mathsf{Sign}(k,1\|r)\rangle|\Psi_1\rangle| \tag{54}$$

$$+ |c_0| \cdot |\langle 1|\langle \mathsf{Sign}(k,1\|r)|\langle\Psi_1|W|0\rangle|\mathsf{Sign}(k,0\|r)\rangle|\Psi_0\rangle| \tag{55}$$

for all $\lambda \in I'$. Then,

$$\frac{1}{2p(\lambda)} \leq |c_1| \cdot |\langle 0| \langle \mathsf{Sign}(k, 0\|r)| \langle \Psi_0| W |1\rangle |\mathsf{Sign}(k, 1\|r)\rangle |\Psi_1\rangle | \tag{56}$$

or

$$\frac{1}{2p(\lambda)} \leq |c_0| \cdot |\langle 1| \langle \mathsf{Sign}(k, 1\|r)| \langle \Psi_1| W |0\rangle |\mathsf{Sign}(k, 0\|r)\rangle |\Psi_0\rangle | \tag{57}$$

holds for all $\lambda \in I'$. Assume that the latter holds. (The following proof can be easily modified even if the former holds.) Then

$$\frac{1}{4p^2(\lambda)} \leq |c_0|^2 \cdot |\langle 1| \langle \mathsf{Sign}(k, 1\|r)| \langle \Psi_1| W |0\rangle |\mathsf{Sign}(k, 0\|r)\rangle |\Psi_0\rangle |^2 \tag{58}$$

$$\leq |c_0|^2 \cdot \|(I \otimes \langle \mathsf{Sign}(k, 1\|r)| \otimes I) W |0\rangle |\mathsf{Sign}(k, 0\|r)\rangle |\Psi_0\rangle \|^2 \tag{59}$$

for all $\lambda \in I'$. With this W, we construct the QPT adversary $\mathcal{A}''$ as is shown in Figure 4.

$\mathcal{A}''$

1. Simulate $\mathcal{A}'$ in steps 1.-7. of Figure 3. If $\perp$ is sent from $\mathcal{C}$, output $\perp$ and halt.
2. Measure the register $\mathbf{A}$ in the computational basis. If the result is 1, output $\perp$ and halt. If the result is 0, measure the register $\mathbf{B}$ of the post-measurement state in the computational basis to get the measurement result μ_0.
3. Apply W on the post-measurement state and measure the register $\mathbf{B}$ in the computational basis to get the result μ_1.
4. Output (μ_0, μ_1).

Figure 4: $\mathcal{A}''$

We show that $\mathcal{A}''$ wins the game of Figure 3 with a non-negligible probability for infinitely many λ. The probability that $t \in T'_\lambda$ and Good occur in Item 1 of Figure 4 is at least $\frac{1}{16p^2(\lambda)}$ for all $\lambda \in I'$, because of the following reasons. First, $\sum_{t \in T'_\lambda} \Pr[t] \geq \frac{1}{4p(\lambda)}$ for all $\lambda \in I'$ from Lemma 5.1. Second, because $t \in T'_\lambda$ means $t \in T_\lambda$, $\Pr[\mathsf{Good} \mid t] \geq \frac{1}{4p(\lambda)}$ for all $\lambda \in I$ from Equation (34).

Assume that $t \in T'_\lambda$ and Good occur. If $\mathcal{A}''$ does the operations in Item 2 and Item 3 on $|\tilde{\phi}_b^{t,good}\rangle$, the probability that $(\mu_0, \mu_1) = (\mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r))$ is at least $\frac{1}{4p^2(\lambda)}$ for all $\lambda \in I'$ from Equation (59). From Lemma 5.1, the trace distance between $|\phi_b^{t,good}\rangle$ and $|\tilde{\phi}_b^{t,good}\rangle$ is at most $\frac{1}{p^{10}(\lambda)}$ for all $\lambda \in I'$. Therefore, if $\mathcal{A}''$ does the operations in Item 2 and Item 3 on $|\phi_b^{t,good}\rangle$, the probability that $(\mu_0, \mu_1) = (\mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r))$ is at least $\frac{1}{4p^2(\lambda)} - \frac{1}{p^{10}(\lambda)}$ for all $\lambda \in I'$. Hence, the overall probability that $\mathcal{A}''$ outputs $(\mu_0, \mu_1) = (\mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r))$ is non-negligible for infinitely many λ.

We prove Lemma 5.1 to complete this subsection.

Proof of Lemma 5.1. Fix $t \in T_\lambda$. Immediately before the coherent signature test in Item 5 of Figure 2, the entire state over the registers $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ is generally written as

$$\sum_{\alpha,\beta} d_{\alpha,\beta} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\Lambda_{\alpha,\beta}\rangle_{\mathbf{C}}, \tag{60}$$

where $d_{\alpha,\beta}$ are some complex coefficients such that $\sum_{\alpha,\beta} |d_{\alpha,\beta}|^2 = 1$, and $|\Lambda_{\alpha,\beta}\rangle$ are some normalized states. Define the set

$$S := \{(\alpha, \beta) : \mathsf{Ver}(\mathsf{vk}, \alpha \| r, \beta) = \top \wedge \beta \neq \mathsf{Sign}(k, \alpha \| r)\}. \tag{61}$$

The (unnormalized) state after obtaining $\top$ in the coherent signature test in Item 5 of Figure 2 is

$$\begin{aligned} &d_{0,\mathsf{Sign}(k,0\|r)} |0\rangle_{\mathbf{A}} |\mathsf{Sign}(k, 0\|r)\rangle_{\mathbf{B}} |\Lambda_{0,\mathsf{Sign}(k,0\|r)}\rangle_{\mathbf{C}} \\ &+ d_{1,\mathsf{Sign}(k,1\|r)} |1\rangle_{\mathbf{A}} |\mathsf{Sign}(k, 1\|r)\rangle_{\mathbf{B}} |\Lambda_{1,\mathsf{Sign}(k,1\|r)}\rangle_{\mathbf{C}} \\ &+ \sum_{(\alpha,\beta)\in S} d_{\alpha,\beta} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\Lambda_{\alpha,\beta}\rangle_{\mathbf{C}}. \end{aligned} \tag{62}$$

Define

$$T'_\lambda := \Big\{t \in T_\lambda : \sum_{(\alpha,\beta)\in S} |d_{\alpha,\beta}|^2 \leq \frac{1}{4p^{21}(\lambda)}\Big\}. \tag{63}$$

If

$$\sum_{t\in T_\lambda \setminus T'_\lambda} \Pr[t] \geq \frac{1}{4p(\lambda)} \tag{64}$$

for infinitely many $\lambda \in I$, it contradicts the strong EUF-CMA security of the digital signature scheme. Therefore,

$$\sum_{t\in T_\lambda \setminus T'_\lambda} \Pr[t] \leq \frac{1}{4p(\lambda)} \tag{65}$$

for all $\lambda \in I'$, where $I' := \{\lambda \in I : \lambda \geq \lambda_0\}$ with a certain λ_0. This means that

$$\sum_{t\in T'_\lambda} \Pr[t] \geq \sum_{t\in T_\lambda} \Pr[t] - \frac{1}{4p(\lambda)} \tag{66}$$

$$\geq \frac{1}{2p(\lambda)} - \frac{1}{4p(\lambda)} \tag{67}$$

$$= \frac{1}{4p(\lambda)} \tag{68}$$

for all $\lambda \in I'$.

Moreover, because $t \in T'_\lambda$ means $t \in T_\lambda$, $\Pr[\mathsf{Good} \mid t] \geq \frac{1}{4p(\lambda)}$ for all $\lambda \in I$ from Equation (34). Therefore, for any $t \in T'_\lambda$,

$$|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2 + \sum_{(\alpha,\beta)\in S} |d_{\alpha,\beta}|^2 \geq \frac{1}{4p(\lambda)} \tag{69}$$

for all $\lambda \in I$. If we renormalize the state of Equation (62) and apply Z^b, we have

$$|\phi_b^{t,good}\rangle = \frac{d_{0,\mathsf{Sign}(k,0\|r)}}{\sqrt{|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2 + \sum_{(\alpha,\beta)\in S}|d_{\alpha,\beta}|^2}} |0\rangle_{\mathbf{A}} |\mathsf{Sign}(k,0\|r)\rangle_{\mathbf{B}} |\Lambda_{0,\mathsf{Sign}(k,0\|r)}\rangle_{\mathbf{C}} \tag{70}$$

$$+ (-1)^b \frac{d_{1,\mathsf{Sign}(k,1\|r)}}{\sqrt{|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2 + \sum_{(\alpha,\beta)\in S}|d_{\alpha,\beta}|^2}} |1\rangle_{\mathbf{A}} |\mathsf{Sign}(k,1\|r)\rangle_{\mathbf{B}} |\Lambda_{1,\mathsf{Sign}(k,1\|r)}\rangle_{\mathbf{C}} \tag{71}$$

$$+ Z^b \frac{\sum_{(\alpha,\beta)\in S} d_{\alpha,\beta}}{\sqrt{|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2 + \sum_{(\alpha,\beta)\in S}|d_{\alpha,\beta}|^2}} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\Lambda_{\alpha,\beta}\rangle_{\mathbf{C}}. \tag{72}$$

For any $t \in T'_\lambda$, its trace distance to the state

$$\frac{d_{0,\mathsf{Sign}(k,0\|r)}}{\sqrt{|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2}} |0\rangle_{\mathbf{A}} |\mathsf{Sign}(k,0\|r)\rangle_{\mathbf{B}} |\Lambda_{0,\mathsf{Sign}(k,0\|r)}\rangle_{\mathbf{C}} \tag{73}$$

$$+ (-1)^b \frac{d_{1,\mathsf{Sign}(k,1\|r)}}{\sqrt{|d_{0,\mathsf{Sign}(k,0\|r)}|^2 + |d_{1,\mathsf{Sign}(k,1\|r)}|^2}} |1\rangle_{\mathbf{A}} |\mathsf{Sign}(k,1\|r)\rangle_{\mathbf{B}} |\Lambda_{1,\mathsf{Sign}(k,1\|r)}\rangle_{\mathbf{C}} \tag{74}$$

is less than $\frac{1}{p^{10}(\lambda)}$ for all $\lambda \in I$. □

5.2 No QPT Adversary Can Output Two Signatures

Here we show that no QPT adversary can win Hybrid 2 (Figure 3) with a non-negligible probability. We first give an intuitive argument for the proof, and them give a precise proof.

Intuitive argument for the proof is as follows. First, note that the probability that all $\{r_i\}_{i=1}^m$ are distinct in Item 2 in Figure 3 is at least $1 - \mathsf{negl}(\lambda)$. Therefore, we can assume that all $\{r_i\}_{i=1}^m$ are distinct with a negligible loss in the adversary's winning probability. If $r \notin \{r_i\}_{i=1}^m$, it is clear that $\mathcal{A}$ cannot win the game of Figure 3 except for a negligible probability. The reason is that $\mathcal{A}$ cannot find $\mathsf{Sign}(k,0\|r)$ or $\mathsf{Sign}(k,1\|r)$ except for a negligible probability due to the security of the digital signature scheme. Therefore, we assume that r is equal to one of the $\{r_i\}_{i=1}^m$.

Assume that, in the game of Figure 3, $\mathcal{C}$ is replaced with $\mathcal{C}'$ who is the same as $\mathcal{C}$ except that it measures the first qubit of $|\psi_r\rangle$ in the computational basis before sending the states in Item 3. Let $s \in \{0,1\}$ be the measurement result. Then, for any QPT adversary $\mathcal{A}$, the probability that $\mathcal{A}$ wins the game of Figure 3 is negligible. The reason is that $\mathcal{A}$ cannot find $\mathsf{Sign}(k, s \oplus 1\|r)$ except for a negligible probability due to the strong EUF-CMA security of the digital signature scheme. From Lemma 2.6, we therefore have

$$\Pr[(\mathsf{Sign}(k,0\|r), \mathsf{Sign}(k,1\|r)) \leftarrow \mathcal{A} \mid \mathcal{C}] \le 2\Pr[(\mathsf{Sign}(k,0\|r), \mathsf{Sign}(k,1\|r)) \leftarrow \mathcal{A} \mid \mathcal{C}'] \tag{75}$$

$$\le \mathsf{negl}(\lambda), \tag{76}$$

where the left-hand-side of Equation (75) is the probability that $\mathcal{A}$ outputs $(\mathsf{Sign}(k,0\|r), \mathsf{Sign}(k,1\|r))$ with the challenger $\mathcal{C}$, and the right-hand-side is that with the challenger $\mathcal{C}'$.

We give a precise proof below. Let Alg be an algorithm that, on input $(r_1, ..., r_m)$, simulates $\mathcal{C}$ and $\mathcal{A}$ in Figure 3 and outputs (r, μ_0, μ_1). The probability that $\mathcal{A}$ wins in the game of Figure 3 is

$$\frac{1}{2^{um}} \sum_{r_1,...,r_m} \sum_r \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{77}$$

$$= \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_r \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{78}$$

$$+ \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\notin R} \sum_r \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{79}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_r \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] + \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\notin R} \tag{80}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_r \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] + \frac{(m-1)m}{2^u} \tag{81}$$

$$= \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\in\{r_i\}_{i=1}^m} \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{82}$$

$$+ \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\notin\{r_i\}_{i=1}^m} \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] + \frac{(m-1)m}{2^u} \tag{83}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\in\{r_i\}_{i=1}^m} \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{84}$$

$$+ \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \mathsf{negl}(\lambda) + \frac{(m-1)m}{2^u} \tag{85}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\in\{r_i\}_{i=1}^m} \Pr[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{86}$$

$$+ \mathsf{negl}(\lambda) + \frac{(m-1)m}{2^u} \tag{87}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\in\{r_i\}_{i=1}^m} 2\Pr'[(r, \mathsf{Sign}(k, 0\|r), \mathsf{Sign}(k, 1\|r)) \leftarrow \mathsf{Alg}(r_1, ..., r_m)] \tag{88}$$

$$+ \mathsf{negl}(\lambda) + \frac{(m-1)m}{2^u} \tag{89}$$

$$\leq \frac{1}{2^{um}} \sum_{(r_1,...,r_m)\in R} \sum_{r\in\{r_i\}_{i=1}^m} \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \frac{(m-1)m}{2^u} \tag{90}$$

$$\leq \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \frac{(m-1)m}{2^u} \tag{91}$$

$$= \mathsf{negl}(\lambda). \tag{92}$$

Here, $R \coloneqq \{(r_1, ..., r_m) : \text{All of them are distinct}\}$. In Equation (85), we have used the strong EUF-CMA security of the digital signature scheme. $\Pr'$ is the probability that, in Alg, $\mathcal{C}$ is replaced with $\mathcal{C}'$ who is the same as $\mathcal{C}$ except that it measures the first qubit of $|\psi_r\rangle$ in the computational basis before sending the states in Item 3. Equation (88) comes from Lemma 2.6. Equation (90) is from the strong EUF-CMA security of the digital signature scheme.

6 Recyclable Variant

In the construction given in Section 4, a quantum public key can be used to encrypt only one message and a sender needs to obtain a new quantum public key whenever it encrypts a message. This is not desirable from practical perspective. In this section, we define recyclable QPKE where a sender only needs to receive one quantum public key to send arbitrarily many messages. The definition is similar to QPKE as defined in Definition 3.1 except that the encryption algorithm outputs a classical *recycled* key that can be reused to encrypt messages many times.

Definition 6.1 (Recyclable QPKE). *A recyclable QPKE scheme with message space* $\{0,1\}^\ell$ *is a set of algorithms* $(\mathsf{SKGen}, \mathsf{PKGen}, \mathsf{Enc}, \mathsf{rEnc}, \mathsf{Dec})$ *such that*

- $\mathsf{SKGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{vk})$: *It is a PPT algorithm that, on input the security parameter* λ*, outputs a classical secret key* sk *and a classical verification key* vk.
- $\mathsf{PKGen}(\mathsf{sk}) \to \mathsf{pk}$: *It is a QPT algorithm that, on input* sk*, outputs a quantum public key* pk.
- $\mathsf{Enc}(\mathsf{vk}, \mathsf{pk}, \mathsf{msg}) \to (\mathsf{ct}, \mathsf{rk})$: *It is a QPT algorithm that, on input* vk, pk*, and a plaintext* $\mathsf{msg} \in \{0,1\}^\ell$*, outputs a classical ciphertext* ct *and classical recycled key* rk.
- $\mathsf{rEnc}(\mathsf{rk}, \mathsf{msg}) \to \mathsf{ct}$: *It is a PPT algorithm that, on input* rk *and a plaintext* $\mathsf{msg} \in \{0,1\}^\ell$*, outputs a classical ciphertext* ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{msg}'$: *It is a classical deterministic polynomial-time algorithm that, on input* sk *and* ct*, outputs* $\mathsf{msg}' \in \{0,1\}^\ell \cup \{\bot\}$.

We require the following correctness and IND-pkTA security.

Correctness: *For any* $\mathsf{msg}, \mathsf{msg}' \in \{0,1\}^\ell$,

$$\Pr\left[\mathsf{msg} \leftarrow \mathsf{Dec}(\mathsf{sk},\mathsf{ct}) \wedge \mathsf{msg}' \leftarrow \mathsf{Dec}(\mathsf{sk},\mathsf{ct}') : \begin{array}{r} (\mathsf{sk},\mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda) \\ \mathsf{pk} \leftarrow \mathsf{PKGen}(\mathsf{sk}) \\ (\mathsf{ct},\mathsf{rk}) \leftarrow \mathsf{Enc}(\mathsf{vk},\mathsf{pk},\mathsf{msg}) \\ \mathsf{ct}' \leftarrow \mathsf{rEnc}(\mathsf{rk},\mathsf{msg}') \end{array}\right] \geq 1 - \mathsf{negl}(\lambda). \quad (93)$$

IND-pkTA security under quantum public keys: *For any polynomial* m*, and any QPT adversary* $\mathcal{A}$,

$$\Pr\left[b \leftarrow \mathcal{A}^{\mathsf{rEnc}(\mathsf{rk},\cdot)}(\mathsf{ct}^*,\mathsf{st}) : \begin{array}{r} (\mathsf{sk},\mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda) \\ \mathsf{pk}_1,...,\mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m} \\ (\mathsf{pk}',\mathsf{msg}_0,\mathsf{msg}_1,\mathsf{st}) \leftarrow \mathcal{A}(\mathsf{vk},\mathsf{pk}_1,...,\mathsf{pk}_m) \\ b \leftarrow \{0,1\} \\ (\mathsf{ct}^*,\mathsf{rk}) \leftarrow \mathsf{Enc}(\mathsf{vk},\mathsf{pk}',\mathsf{msg}_b) \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda). \quad (94)$$

Here, $\mathsf{pk}_1,...,\mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m}$ *means that* PKGen *is executed* m *times and* pk_i *is the output of the* i*th execution of* PKGen, $\mathsf{rEnc}(\mathsf{rk},\cdot)$ *means a classically-accessible encryption oracle, and* st *is a quantum internal state of* $\mathcal{A}$*, which can be entangled with* pk'.

IND-pkTA security under recycled keys: *For any polynomial m, and any QPT adversary $\mathcal{A}$,*

$$\Pr\left[b \leftarrow \mathcal{A}^{\mathsf{rEnc}(\mathsf{rk},\cdot)}(\mathsf{ct}^*, \mathsf{st}') : \begin{array}{r} (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{SKGen}(1^\lambda) \\ \mathsf{pk}_1, ..., \mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m} \\ (\mathsf{pk}', \mathsf{msg}, \mathsf{st}) \leftarrow \mathcal{A}(\mathsf{vk}, \mathsf{pk}_1, ..., \mathsf{pk}_m) \\ (\mathsf{ct}, \mathsf{rk}) \leftarrow \mathsf{Enc}(\mathsf{vk}, \mathsf{pk}', \mathsf{msg}) \\ (\mathsf{msg}_0, \mathsf{msg}_1, \mathsf{st}') \leftarrow \mathcal{A}^{\mathsf{rEnc}(\mathsf{rk},\cdot)}(\mathsf{ct}, \mathsf{st}) \\ b \leftarrow \{0,1\} \\ \mathsf{ct}^* \leftarrow \mathsf{rEnc}(\mathsf{rk}, \mathsf{msg}_b) \end{array}\right] \le \frac{1}{2} + \mathsf{negl}(\lambda). \tag{95}$$

Here, $\mathsf{pk}_1, ..., \mathsf{pk}_m \leftarrow \mathsf{PKGen}(\mathsf{sk})^{\otimes m}$ *means that* PKGen *is executed* m *times and* pk_i *is the output of the* i*th execution of* PKGen*,* $\mathsf{rEnc}(\mathsf{rk}, \cdot)$ *means a classically-accessible encryption oracle, and* st *and* st' *are quantum internal states of* $\mathcal{A}$*, which can be entangled with* pk'*.*

Construction. We show a generic construction of recyclable QPKE from (non-recyclable) QPKE with classical ciphertexts and IND-CPA secure SKE via standard hybrid encryption.

Let $\mathsf{QPKE} = (\mathsf{QPKE.SKGen}, \mathsf{QPKE.PKGen}, \mathsf{QPKE.Enc}, \mathsf{QPKE.Dec})$ be a (non-recyclable) QPKE scheme with message space $\{0,1\}^\lambda$ and $\mathsf{SKE} = (\mathsf{SKE.Enc}, \mathsf{SKE.Dec})$ be an SKE scheme with message space $\{0,1\}^\ell$. Then we construct a recyclable QPKE scheme $\mathsf{QPKE}' = (\mathsf{QPKE}'.\mathsf{SKGen}, \mathsf{QPKE}'.\mathsf{PKGen}, \mathsf{QPKE}'.\mathsf{Enc}, \mathsf{QPKE}'.\mathsf{rEnc}, \mathsf{QPKE}'.\mathsf{Dec})$ with message space $\{0,1\}^\ell$ as follows:

- $\mathsf{QPKE}'.\mathsf{SKGen}(1^\lambda) \to (\mathsf{sk}', \mathsf{vk}')$: Run $(\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{QPKE.SKGen}(1^\lambda)$ and output a secret key $\mathsf{sk}' := \mathsf{sk}$ and verification key $\mathsf{vk}' := \mathsf{vk}$.
- $\mathsf{QPKE}'.\mathsf{PKGen}(\mathsf{sk}') \to \mathsf{pk}'$: Run $\mathsf{pk} \leftarrow \mathsf{QPKE.PKGen}(\mathsf{sk})$ and outputs $\mathsf{pk}' := \mathsf{pk}$.
- $\mathsf{QPKE}'.\mathsf{Enc}(\mathsf{vk}', \mathsf{pk}', \mathsf{msg}) \to (\mathsf{ct}', \mathsf{rk}')$: Parse $\mathsf{pk}' = \mathsf{pk}$ and $\mathsf{vk}' = \mathsf{vk}$, sample $K \leftarrow \{0,1\}^\lambda$, run $\mathsf{ct} \leftarrow \mathsf{QPKE.Enc}(\mathsf{vk}, \mathsf{pk}, K)$ and $\mathsf{ct}_{\mathsf{ske}} \leftarrow \mathsf{SKE.Enc}(K, \mathsf{msg})$, and output a ciphertext $\mathsf{ct}' := (\mathsf{ct}, \mathsf{ct}_{\mathsf{ske}})$ and recycled key $\mathsf{rk}' := (K, \mathsf{ct})$.
- $\mathsf{QPKE}'.\mathsf{rEnc}(\mathsf{rk}', \mathsf{msg}) \to \mathsf{ct}'$: Parse $\mathsf{rk}' = (K, \mathsf{ct})$, run $\mathsf{ct}_{\mathsf{ske}} \leftarrow \mathsf{SKE.Enc}(K, \mathsf{msg})$, and output a ciphertext $\mathsf{ct}' := (\mathsf{ct}, \mathsf{ct}_{\mathsf{ske}})$.
- $\mathsf{QPKE}'.\mathsf{Dec}(\mathsf{sk}', \mathsf{ct}') \to \mathsf{msg}'$: Parse $\mathsf{ct}' = (\mathsf{ct}, \mathsf{ct}_{\mathsf{ske}})$ and $\mathsf{sk}' = \mathsf{sk}$, run $K' \leftarrow \mathsf{QPKE.Dec}(\mathsf{sk}, \mathsf{ct})$ and $\mathsf{msg}' \leftarrow \mathsf{SKE.Dec}(K', \mathsf{ct}_{\mathsf{ske}})$, and output msg'.

Correctness. Correctness of QPKE' immediately follows from correctness of QPKE and SKE.

IND-pkTA security. IND-pkTA security of QPKE implies that the SKE key K chosen by $\mathsf{QPKE}'.\mathsf{Enc}$ is computationally indistinguishable from uniformly random for an adversary. Then IND-CPA security of SKE directly implies IND-pkTA security under quantum public keys and recycled keys of QPKE' since msg is encrypted by SKE under the key K in both of $\mathsf{QPKE}'.\mathsf{Enc}$ and $\mathsf{QPKE}'.\mathsf{rEnc}$.

Remark 6.2. We can generically add decryption error detectability by using digital signatures similarly to (non-recyclable) QPKE.

Acknowledgments. TM is supported by JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in-Aid for Scientific Research (B) No.JP19H04066, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

References

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions. *Electron. Colloquium Comput. Complex.*, page 146, 2020. (Cited on page 3, 4, 5.)

[AGM21] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Can you sign a quantum state? *Quantum*, 2021. (Cited on page 2.)

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. TCC, 2022. (Cited on page 2.)

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Heidelberg, August 2022. (Cited on page 2.)

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179. IEEE, 1984. (Cited on page 2, 8.)

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *43rd FOCS*, pages 449–458. IEEE Computer Society Press, November 2002. (Cited on page 2.)

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 467–496, Virtual Event, August 2021. Springer, Heidelberg. (Cited on page 2.)

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. ITCS 2023: 14th Innovations in Theoretical Computer Science, 2023. (Cited on page 2.)

[BMW23] Khashayar Barooti, Giulio Malavolta, and Michael Walter. A simple construction of quantum public-key encryption from quantum-secure one-way functions. Cryptology ePrint Archive, Paper 2023/306, 2023. https://eprint.iacr.org/2023/306. (Cited on page 2, 3, 4, 7, 8.)

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Heidelberg, August 2013. (Cited on page 6, 10.)

[Col23] Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. Cryptology ePrint Archive, Paper 2023/282, 2023. https://eprint.iacr.org/2023/282. (Cited on page 2, 3, 7, 8.)

[CX22] Shujiao Cao and Rui Xue. On constructing one-way quantum state generators, and more. Cryptology ePrint Archive, Report 2022/1323, 2022. https://eprint.iacr.org/2022/1323. (Cited on page 2.)

[DS15] Nico Döttling and Dominique Schröder. Efficient pseudorandom functions via on-the-fly adaptation. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 329–350. Springer, Heidelberg, August 2015. (Cited on page 28.)

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986. (Cited on page 10.)

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in MiniQCrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 531–561. Springer, Heidelberg, October 2021. (Cited on page 2.)

[Gol04] Oded Goldreich. Foundations of cryptography: Volume 2, basic applications. 2004. (Cited on page 9, 25.)

[Got] Daniel Gottesman. Quantum public-key cryptography with information-theoretic security. *https://www2.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt*. (Cited on page 7.)

[GSV23] Alex B. Grilo, Or Sattath, and Quoc-Huy Vu. Encryption with quantum public keys. Cryptology ePrint Archive, Paper 2023/345, 2023. `https://eprint.iacr.org/2023/345`. (Cited on page 2, 3, 4, 7, 8.)

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. (Cited on page 10.)

[HMY22] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. *arXiv:2210.05978*, 2022. (Cited on page 3, 4, 13.)

[IR90] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. Springer, Heidelberg, August 1990. (Cited on page 2.)

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Heidelberg, August 2018. (Cited on page 2.)

[KKNY05] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 268–284. Springer, Heidelberg, May 2005. (Cited on page 7.)

[KQST22] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. *arXiv:2212.00879*, 2022. (Cited on page 2.)

[Kre21] W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021. (Cited on page 2.)

[MY22a] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Report 2022/1336, 2022. https://eprint.iacr.org/2022/1336. (Cited on page 2, 3, 7.)

[MY22b] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2022. (Cited on page 2.)

[YZ21] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 568–597. Springer, Heidelberg, October 2021. (Cited on page 26, 29, 30.)

[Zha12] Mark Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, October 2012. (Cited on page 26.)

A Pure State Public Key Variant

As discussed in Section 1.3, we believe that the distinction between pure state and mixed state public keys is not important from a practical point of view. Nonetheless, it is a mathematically valid question if we can construct an IND-pkTA secure QPKE scheme with pure state public keys. We give such a scheme based on the existence of quantum-secure OWFs by extending the construction given in Section 4. For the ease of exposition, we first show a construction based on *slightly superpolynomially secure* OWFs in Appendix A.1. Then, we explain how to modify the scheme to base its security on standard polynomially secure OWFs in Appendix A.2.

Preparation. We define a fine-grained version of strong EUF-CMA security for digital signature schemes.

Definition A.1 (**T-strong EUF-CMA security**)**.** *A digital signature scheme* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is T-strong EUF-CMA secure if the following holds: For any quantum adversary $\mathcal{A}$ that runs in time T and makes at most T classical queries to the signing oracle* $\mathsf{Sign}(k, \cdot)$*,*

$$\Pr[(\mathsf{msg}^*, \sigma^*) \notin \mathcal{Q} \wedge \top \leftarrow \mathsf{Ver}(\mathsf{vk}, \mathsf{msg}^*, \sigma^*) : (k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda), (\mathsf{msg}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(k,\cdot)}(\mathsf{vk})] \leq T^{-1}, \tag{96}$$

where $\mathcal{Q}$ is the set of message-signature pairs returned by the signing oracle.

Remark A.2. Strong EUF-CMA security defined in Definition 2.1 holds if and only if T-strong EUF-CMA security holds for all polynomials T.

Remark A.3. We can show that there exists a T-strong EUF-CMA secure digital signature scheme for some $T = \lambda^{\omega(1)}$ if slightly superpolynomially secure OWFs exist similarly to the proof of Theorem 2.3 in [Gol04, Sec. 6.5.2]. Here, a superpolynomially secure OWF is a function f for which there exists $T = \lambda^{\omega(1)}$ such that any adversary with running time T can invert f with probability at most T^{-1}.

We define quantum-query pseudorandom functions.

Definition A.4 (Pseudorandom functions (PRFs)). *A keyed function* $\{\mathsf{PRF}_K : \mathcal{X} \to \mathcal{Y}\}_{K \in \{0,1\}^\lambda}$ *that is computable in classical deterministic polynomial-time is a quantum-query secure pseudorandom function if for any QPT adversary $\mathcal{A}$ with quantum access to the evaluation oracle* $\mathsf{PRF}_K(\cdot)$*,*

$$|\Pr[1 \leftarrow \mathcal{A}^{\mathsf{PRF}_K(\cdot)}(1^\lambda)] - \Pr[1 \leftarrow \mathcal{A}^{H(\cdot)}(1^\lambda)]| \leq \mathsf{negl}(\lambda), \tag{97}$$

where $K \leftarrow \{0,1\}^\lambda$ and $H : \mathcal{X} \rightarrow \mathcal{Y}$ is a function chosen uniformly at random.

Remark A.5 ([Zha12]). Quantum-query secure PRFs exist if quantum-secure OWFs exist.

We also need the following lemma in the security proof.

Lemma A.6. *For a function $H : \{0,1\}^{u+1} \rightarrow \{0,1\}^v$, let $|\psi_H\rangle := \sum_{R\in\{0,1\}^{u+1}} |R\rangle |H(R)\rangle$. For any integer m and (unbounded-time) quantum algorithm $\mathcal{A}$,*

$$\Pr_H[y_0 = H(0\|r) \wedge y_1 = H(1\|r) : (r, y_0, y_1) \leftarrow \mathcal{A}(|\psi_H\rangle^{\otimes m})] \leq (2m+1)^4(2^{-u} + 2^{-v}) \tag{98}$$

where H is a uniformly random function from $\{0,1\}^{u+1}$ to $\{0,1\}^v$.

We priove it using the result of [YZ21]. We defer the proof to Appendix A.3.

A.1 Construction from Slightly Superpolynomially Secure OWFs

In this section, we construct a QPKE scheme that satisfies correctness and IND-pkTA security (but not decryption error detectability) and has pure state public keys from T-strong EUF-CMA secure digital signatures for a superpolynomial T and quantum-query secure PRFs. Note that they exist assuming the existence of slightly superpolynomially secure OWFs as noted in Remarks A.3 and A.5. The message space of our construction is $\{0,1\}$, but it can be extended to be arbitrarily many bits by parallel repetition. Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ be a T-strong EUF-CMA secure digital signature scheme with a deterministic Sign algorithm and message space $\{0,1\}^{u+v+1}$ and $\{\mathsf{PRF}_K : \{0,1\}^{u+1} \rightarrow \{0,1\}^v\}_{K\in\{0,1\}^\lambda}$ be a quantum-query secure PRF where $T = \lambda^{\omega(1)}$, $u := \lfloor(\log T)/2\rfloor$, and $v = \omega(\log \lambda)$.

Then we construct a QPKE scheme $(\mathsf{SKGen}, \mathsf{PKGen}, \mathsf{Enc}, \mathsf{Dec})$ as follows.

- $\mathsf{SKGen}(1^\lambda) \rightarrow (\mathsf{sk}, \mathsf{vk})$: Run $(k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and sample $K \leftarrow \{0,1\}^\lambda$. Output $\mathsf{sk} := (k, K)$ and vk.
- $\mathsf{PKGen}(\mathsf{sk}) \rightarrow \mathsf{pk}$: Parse $\mathsf{sk} = (k, K)$. Choose $r \leftarrow \{0,1\}^u$. By running Sign and PRF coherently, generate the state
$$|\psi_{\mathsf{sk}}\rangle := \sum_{r\in\{0,1\}^u} |r\rangle_{\mathbf{R}} \otimes \begin{pmatrix} |0\rangle_{\mathbf{A}} \otimes |y(0,r)\rangle_{\mathbf{B}} \otimes |\sigma(0,r)\rangle_{\mathbf{C}} \\ +|1\rangle_{\mathbf{A}} \otimes |y(1,r)\rangle_{\mathbf{B}} \otimes |\sigma(1,r)\rangle_{\mathbf{C}} \end{pmatrix} \tag{99}$$
over registers $(\mathbf{R}, \mathbf{A}, \mathbf{B}, \mathbf{C})$ where $y(b,r) := \mathsf{PRF}_K(b\|r)$ and $\sigma(b,r) := \mathsf{Sign}(k, b\|r\|y(b,r))$ for $b \in \{0,1\}$ and $r \in \{0,1\}^u$. (We omit K and k from the notations for simplicity.) Output
$$\mathsf{pk} := |\psi_{\mathsf{sk}}\rangle . \tag{100}$$
- $\mathsf{Enc}(\mathsf{vk}, \mathsf{pk}, b) \rightarrow \mathsf{ct}$: Parse $\mathsf{pk} = \rho$, where ρ is a quantum state over registers $(\mathbf{R}, \mathbf{A}, \mathbf{B}, \mathbf{C})$. The Enc algorithm consists of the following three steps.
  1. It coherently checks the signature in ρ. In other words, it applies the unitary
  $$U_{\mathsf{vk}} |r\rangle_{\mathbf{R}} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\gamma\rangle_{\mathbf{C}} |0...0\rangle_{\mathbf{E}} = |r\rangle_{\mathbf{R}} |\alpha\rangle_{\mathbf{A}} |\beta\rangle_{\mathbf{B}} |\gamma\rangle_{\mathbf{C}} |\mathsf{Ver}(\mathsf{vk}, \alpha\|r\|\beta, \gamma)\rangle_{\mathbf{E}} \tag{101}$$
  on $\rho_{\mathbf{R},\mathbf{A},\mathbf{B},\mathbf{C}} \otimes |0...0\rangle\langle 0...0|_{\mathbf{E}}$, and measures the register $\mathbf{E}$ in the computational basis. If the result is $\bot$, it outputs $\mathsf{ct} := \bot$ and halts. If the result is $\top$, it goes to the next step.

2. It applies Z^b on the register $\mathbf{A}$.
3. It measures $\mathbf{R}$ in the computational basis to get r and all qubits in the registers $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ in the Hadamard basis to get the result d. It outputs

$$\mathsf{ct} := (r, d). \tag{102}$$

- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to b'$: Parse $\mathsf{sk} = (k, K)$ and $\mathsf{ct} = (r, d)$. Output

$$b' := d \cdot (0\|y(0, r)\|\sigma(0, r) \oplus 1\|y(1, r)\|\sigma(1, r)). \tag{103}$$

Theorem A.7. *If* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is a T-strong EUF-CMA secure digital signature scheme and* $\{\mathsf{PRF}_K : \{0, 1\}^{u+1} \to \{0, 1\}^v\}_{K \in \{0,1\}^\lambda}$ *is a quantum-query secure PRF, then the QPKE scheme* $(\mathsf{SKGen}, \mathsf{PKGen}, \mathsf{Enc}, \mathsf{Dec})$ *above is correct and satisfies IND-pkTA security.*

Proof (sketch). The correctness is easily seen similarly to the proof of Theorem 4.1.

For IND-pkTA security, we only explain the differences from the proof of Theorem 4.1 since it is very similar. We define Hybrid $0, 1$, and 2 similarly to those in the proof of Theorem 4.1. For clarity, we describe them in Figures 5 to 7.

Assume that the IND-pkTA security of our construction is broken by a QPT adversary $\mathcal{A}$. It means the QPT adversary $\mathcal{A}$ wins Hybrid 0 with a non-negligible advantage. Then, it is clear that there is another QPT adversary $\mathcal{A}'$ that wins Hybrid 1 with a non-negligible advantage. ($\mathcal{A}'$ has only to do the Hadamard-basis measurement by itself.)

From the $\mathcal{A}'$, we construct a QPT adversary $\mathcal{A}''$ that wins Hybrid 2 with a non-negligible probability based on a similar proof to that in Section 5.1. Indeed, the proof is almost identical once we show that any QPT adversary given polynomially many copies of the public key can output a valid signature for a message that is not of the form $b\|r\|y(b, r)$ only with a negligible probability. To prove this, we consider a reduction algorithm that queries signatures on *all* messages of the form $b\|r\|y(b, r)$. Thus, the reduction algorithm makes 2^{u+1} queries and runs in time $2^u \cdot \mathrm{poly}(\lambda)$. Since we have $2^{u+1} < T$ and $2^u \cdot \mathrm{poly}(\lambda) < T$ for sufficiently large λ by $u = \lfloor (\log T)/2 \rfloor$, which in particular implies $2^u \leq T^{1/2}$, and $T = \lambda^{\omega(1)}$, the reduction enables us to prove the above property assuming the T-strong EUF-CMA security of the digital signature scheme.[9]

Thus, we are left to prove that no QPT adversary can win Hybrid 2 with a non-negligible probability. Let Hybrid 2' be a hybrid that works similarly to Hybrid 2 except that $y(b, r)$ is defined as $y(b, r) := H(b\|r)$ for a uniformly random function H instead of PRF. By the quantum-query security of PRF, the winning probabilities in Hybrid 2' and Hybrid 2 are negligibly close. Thus, it suffices to prove the winning probability in Hybrid 2' is negligible. This is proven by a straightforward reduction to Lemma A.6 noting that $|\psi_{\mathsf{sk}}\rangle$ with the modification of $y(b, r)$ as above can be generated from $|\psi_H\rangle = \sum_{R \in \{0,1\}^{u+1}} |R\rangle |H(R)\rangle$ by coherently running Sign. This completes the proof of IND-pkTA security.

□

Remark A.8. We can add decryption error detectability by Theorem 3.4 and extend it to recyclable QPKE by the construction of Section 6. These extensions preserve the property that public keys are pure states.

[9] In the proof for the mixed state public key version in Section 5.1, the reduction algorithm only needs to query signatures on $b\|r$ for r's used in one of the public keys given to the adversary. On the other hand, in the pure state public key case, each public key involves all r's and thus the reduction algorithm needs to query signatures on superpolynomially many messages. This is why we need superpolynomial security for the digital signature scheme.

Hybrid 0

1. $\mathcal{C}$ runs $(k, \mathsf{vk}) \leftarrow \mathsf{Gen}(1^\lambda)$. $\mathcal{C}$ sends vk to $\mathcal{A}$.
2. $\mathcal{C}$ sends $|\psi_{\mathsf{sk}}\rangle^{\otimes m}$ to the adversary $\mathcal{A}$, where

$$|\psi_{\mathsf{sk}}\rangle := \sum_{r\in\{0,1\}^u} |r\rangle \otimes \begin{pmatrix} |0\rangle \otimes |y(0,r)\rangle \otimes |\sigma(0,r)\rangle \\ +|1\rangle \otimes |y(1,r)\rangle \otimes |\sigma(1,r)\rangle \end{pmatrix} \tag{104}$$

3. $\mathcal{A}$ generates a quantum state over registers $(\mathbf{R}, \mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D})$. ($(\mathbf{R}, \mathbf{A}, \mathbf{B}, \mathbf{C})$ corresponds to the quantum part of pk', and $\mathbf{D}$ corresponds to st.) $\mathcal{A}$ sends the registers $(\mathbf{R}, \mathbf{A}, \mathbf{B}, \mathbf{C})$ to $\mathcal{C}$. $\mathcal{A}$ keeps the register $\mathbf{D}$.
4. $\mathcal{C}$ coherently checks the signature in the state sent from $\mathcal{A}$. If the result is $\bot$, it sends $\bot$ to $\mathcal{A}$ and halts. If the result is $\top$, it goes to the next step.
5. $\mathcal{C}$ chooses $b \leftarrow \{0,1\}$. $\mathcal{C}$ applies Z^b on the register $\mathbf{A}$.
6. $\mathcal{C}$ measures $\mathbf{R}$ in the computational basis to get r.
7. $\mathcal{C}$ measures all qubits in $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ in the Hadamard basis to get the result d. $\mathcal{C}$ sends (r, d) to $\mathcal{A}$.
8. $\mathcal{A}$ outputs b'. If $b' = b$, $\mathcal{A}$ wins.

Figure 5: Hybrid 0

Hybrid 1

1.-6. All the same as Figure 5.

7. $\mathcal{C}$ does not do the Hadamard-basis measurement, and $\mathcal{C}$ sends r and registers $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ to $\mathcal{A}$.
8. The same as Figure 5.

Figure 6: Hybrid 1

A.2 Construction from Polynomially Secure OWFs

We explain how to extend the construction in Appendix A.1 to base security on standard polynomial hardness of OWFs. We rely on a similar idea to the "on-the-fly-adaptation" technique introduced in [DS15]. The reason why we need superpolynomial security in Appendix A.1 is that the reduction algorithm for the transition from Hybrid 1 to 2 has to make $2^{u+1} \approx 2T^{1/2}$ signing queries for a superpolynomial T. Suppose that we set T to be a polynomial. i.e., $T = \lambda^c$ for some constant c. Then, the reduction algorithm for the transition from Hybrid 1 to 2 works under polynomial security of the digital signature scheme. The problem, however, is that we cannot show that the winning probability in Hybrid 2 is negligible: It can be only bounded by $(2m+1)^4(2^{-u}+2^{-v})$, which is not negligible since $2^u \approx T^{1/2} = \lambda^{c/2}$. On the other hand, we can make it arbitrarily small inverse-polynomial by making c larger. Based on this observation, we can show the following: Let $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ be the QPKE scheme given in Appendix A.1 where $T := \lambda^c$. Then, for any polynomials p and m, there exists a constant c such that any QPT adversary given m copies of the quantum public key has an advantage to break IND-pkTA security of $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ at most $1/p(\lambda)$ for all sufficiently large λ.

Then, our idea is to parallelly run $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ for $c = 1, 2, ..., \lambda$ where the encryption algorithm generates a λ-out-of-λ secret sharing of the message and encrypts c-th share under Enc_c.[10] Suppose that this scheme is not IND-pkTA secure. Then, there is a polynomial q and QPT adversary $\mathcal{A}$ given

[10] In fact, it suffices to parallelly run $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ for $c = 1, 2, ..., \eta(\lambda)$ for any super-constant function η.

Hybrid 2

1.-7. All the same as Figure 6.

8. $\mathcal{A}$ outputs (μ_0, μ_1). If $\mu_0 = y(0,r)\|\sigma(0,r)$ and $\mu_1 = y(1,r)\|\sigma(1,r)$, $\mathcal{A}$ wins.

Figure 7: Hybrid 2

$m = \mathrm{poly}(\lambda)$ copies of the quantum public key that has an advantage to break the IND-pkTA security at least $1/q(\lambda)$ for infinitely many λ. For each c, it is easy to construct a QPT adversary $\mathcal{A}_c$ that breaks IND-pkTA security of $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ with the same advantage as $\mathcal{A}$'s advantage. On the other hand, by the observation explained above, we can take a constant c (depending on q and m) such that any QPT adversary given m copies of the public key has an advantage to break IND-pkTA security of $(\mathsf{SKGen}_c, \mathsf{PKGen}_c, \mathsf{Enc}_c, \mathsf{Dec}_c)$ at most $1/2q(\lambda)$ for all sufficiently large λ. This is a contradiction. Thus, the above scheme is IND-pkTA secure.

A.3 Proof of Lemma A.6

For proving Lemma A.6, we rely on the following lemma shown by [YZ21].

Lemma A.9 ([YZ21, Theorem 4.2]). *Let $H : \mathcal{X} \to \mathcal{Y}$ be a uniformly random function. Let $\mathcal{A}$ be an (unbounded-time) randomized algorithm that makes q quantum queries to H and outputs a classical string z. Let $\mathcal{C}$ be an (unbounded-time) randomized algorithm that takes z as input, makes k classical queries to H, and outputs $\top$ or $\bot$. Let $\mathcal{B}$ be the following algorithm that makes at most k classical queries to H:*

$\mathcal{B}^H()$**:** *It does the following:*

1. *Choose a function $H' : \mathcal{X} \to \mathcal{Y}$ from a family of $2q$-wise independent hash functions.*
2. *For each $j \in [k]$, uniformly pick $(i_j, b_j) \in ([q] \times \{0,1\}) \cup \{(\bot,\bot)\}$ under the constraint that there does not exist $j \neq j'$ such that $i_j = i_{j'} \neq \bot$.*
3. *Initialize a stateful oracle $\mathcal{O}$ to be a quantumly-accessible classical oracle that computes H'.*
4. *Run $\mathcal{A}^{\mathcal{O}}()$ where $\mathcal{O}$ is simulated as follows. When $\mathcal{A}$ makes its i-th query, the oracle is simulated as follows:*
   - *(a) If $i = i_j$ for some $j \in [k]$, measure $\mathcal{A}$'s query register to obtain x'_j, query x'_j to the random oracle H to obtain $H(x'_j)$, and do either of the following.*
     - *i. If $b_j = 0$, reprogram $\mathcal{O}$ to output $H(x'_j)$ on x'_j and answer $\mathcal{A}$'s i_j-th query by using the reprogrammed oracle.*
     - *ii. If $b_j = 1$, answer $\mathcal{A}$'s i_j-th query by using the oracle before the reprogramming and then reprogram $\mathcal{O}$ to output $H(x'_j)$ on x'_j.*
   - *(b) Otherwise, answer $\mathcal{A}$'s i-th query by just using the oracle $\mathcal{O}$ without any measurement or reprogramming.*
5. *Output whatever $\mathcal{A}$ outputs.*

Then we have

$$\Pr_H[\mathcal{C}^H(z) = \top : z \leftarrow \mathcal{B}^H()] \geq \frac{1}{(2q+1)^{2k}} \Pr_H[\mathcal{C}^H(z) = \top : z \leftarrow \mathcal{A}^H()]. \quad (105)$$

Remark A.10. There are the following differences from [YZ21, Theorem 4.2] in the statement of the lemma:

1. They consider inputs to $\mathcal{A}$ and $\mathcal{B}$. We omit them because this suffices for our purpose.

2. They consider a more general setting where $\mathcal{A}$ and $\mathcal{B}$ interact with $\mathcal{C}$. We focus on the non-interactive setting.

3. They do not explicitly write how $\mathcal{B}$ works in the statement of [YZ21, Theorem 4.2]. But this is stated at the beginning of its proof.

Using the above lemma, it is easy to prove Lemma A.6.

Proof of Lemma A.6. For an algorithm $\mathcal{A}$ in Lemma A.6, let $\tilde{\mathcal{A}}$ be an oracle-aided algorithm that generates m copies of $|\psi_H\rangle$ by making m quantum queries to H on uniform superpositions of inputs and then runs $\mathcal{A}(|\psi_H\rangle^{\otimes m})$. Let $\mathcal{C}$ be an oracle-aided algorithm that takes $z = (r, y_0, y_1)$ as input, makes two classical queries $0\|r$ and $1\|r$ to H, and outputs $\top$ if and only if $y_0 = H(0\|r)$ and $y_1 = H(1\|r)$. By Lemma A.9, we have

$$\Pr_H[y_0 = H(0\|r) \ \wedge \ y_1 = H(1\|r) : (r, y_0, y_1) \leftarrow \tilde{\mathcal{B}}^H()] \tag{106}$$

$$\geq \frac{1}{(2m+1)^4} \Pr_H[y_0 = H(0\|r) \ \wedge \ y_1 = H(1\|r) : (r, y_0, y_1) \leftarrow \tilde{\mathcal{A}}^H()] \tag{107}$$

where $\tilde{\mathcal{B}}$ is to $\tilde{\mathcal{A}}$ as $\mathcal{B}$ (defined in Lemma A.9) is to $\mathcal{A}$. By the definition of $\tilde{\mathcal{B}}$, it just makes at most two classical queries to H on independently and uniformly random inputs R_0, R_1. The probability that we happen to have $\{R_0, R_1\} = \{0\|r, 1\|r\}$ for some $r \in \{0,1\}^u$ is 2^{-u}. Unless the above occurs, either $H(0\|r)$ or $H(1\|r)$ is uniformly random to $\tilde{\mathcal{B}}$ for all r, and thus the probability that its output satisfies $y_0 = H(0\|r)$ and $y_1 = H(1\|r)$ is at most 2^{-v}. Thus, we have

$$\Pr_H[y_0 = H(0\|r) \ \wedge \ y_1 = H(1\|r) : (r, y_0, y_1) \leftarrow \tilde{\mathcal{B}}^H()] \leq 2^{-u} + 2^{-v}. \tag{108}$$

Combining Equations (107) and (108), we obtain Lemma A.6. □