Signcryption in a Quantum World

Sanjit Chatterjee, Tapas Pandit, Shravan Kumar Parshuram Puria, and Akash Shah

Department of Computer Science and Automation,
Indian Institute of Science, Bangalore, India.
E-mail: sanjit@iisc.ac.in, {tapasgmmath, sppuria94, shahakash94}@gmail.com

Abstract

This work initiates a formal study of signcryption in the quantum setting. We start with formulating suitable security definitions for confidentiality and authenticity of signcryption both in insider and outsider models against quantum adversaries. We investigate the quantum security of generic constructions of signcryption schemes based on three paradigms, viz., encrypt-then-sign ($\mathcal{E}t\mathcal{S}$), sign-then-encrypt ($\mathcal{S}t\mathcal{E}$) and commit-then-encrypt-and-sign ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$). In the insider model, we show that the quantum variants of the classical results hold in the quantum setting with an exception in the $\mathcal{S}t\mathcal{E}$ paradigm. However, in outsider model we need to consider an intermediate setting in which the adversary is given quantum access to unsigncryption oracle but classical access to signcryption oracle. In two-user outsider model, as in the classical setting, we show that post-quantum CPA security of the base encryption scheme is amplified in the $\mathcal{E}t\mathcal{S}$ paradigm if the base signature scheme satisfies a stronger definition. We prove an analogous result in the $\mathcal{S}t\mathcal{E}$ paradigm. Interestingly, in the multi-user setting, our results strengthen the known classical results. Furthermore, our results for the $\mathcal{E}t\mathcal{S}$ and $\mathcal{S}t\mathcal{E}$ paradigms in the two-user outsider model also extend to the setting of authenticated encryption. In this course, we point out a flaw in the proof of quantum security of authenticated encryption in the $\mathcal{E}t\mathcal{S}$ paradigm given in a recent paper. We briefly discuss the difficulties in analyzing the full quantum security of signcryption in outsider model. Finally, we briefly discuss concrete instantiations in various paradigms utilising some available candidates of quantum secure encryption and signature schemes.

Keywords: Signcryption, Post-quantum cryptography, Quantum security, Authenticated encryption

1 Introduction

The possible advent of quantum computers in the foreseeable future poses a threat to the security of many classical cryptosystems. Recently, the National Institute of Standards and Technology (NIST) announced the Post-Quantum Crypto project [NIS17] to evaluate and standardize the quantum-resistant public-key cryptographic algorithms. This was followed by 82 submissions in the first round, of which 26 were shortlisted for the third round of evaluation. After the third round of evaluation [NIS20], 7 (resp. 8) candidates have been shortlisted as finalists (resp. alternatives). The security of the post-quantum cryptographic schemes relies on computational problems which are believed to be intractable even on quantum computers. To formally establish post-quantum security of cryptographic constructions, one generally models all parties and the communication between them to be classical while the adversary is considered to have access to a quantum computer. This setting allows the adversary to perform quantum computations locally and communicate classical information with the parties involved in the protocol. It is well known that quantum immune assumptions alone do not always imply post-quantum security due to fundamental notions such as the no-cloning, which is unique to quantum setting. There have been many works along this line [BDF⁺11, ARU14, ES15, Unr15, SXY18, HHK17, FTTY18] which analyze the security of various post-quantum cryptographic constructions.

Security of classical cryptographic constructions has also been studied in a stronger setting where, in addition to local quantum computations, the adversary is provided access to cryptographic oracle which can be queried quantumly on superposition of inputs [BZ13, GHS16, SJS16]. For example, in case of signature (resp. encryption), the adversary can issue quantum chosen message queries to the signature (resp. encryption/decryption) oracle. We refer to security notions covering such settings as quantum security throughout this paper.

In this work, we extend the above line of study to the generic constructions of signcryption. Signcryption is a public key cryptographic primitive which provides both privacy and authenticity of data. There exists a vast literature on signcryption in the classical setting. It was originally proposed by Zheng [Zhe97], followed by later works [ADR02, BSZ07, MMS09], which focused on formalizing the security of signcryption and analyzing the security of various constructions. The symmetric variant of signcryption, a.k.a., authenticated encryption has been extensively studied in the classical setting, e.g., [BN08].

As already mentioned, signcryption encompasses confidentiality as well as authenticity of data. We quickly recall some of the relevant classical notions for signature and encryption schemes that we will frequently refer to, in the rest of our discussion. The quantum variants of these notions have been discussed in Section 3. For signatures, we use the standard definition of weak/strong existential unforgeability under chosen message attack ((w/s)UF-CMA) and for encryption we use the standard definitions of indistinguishability under chosen plaintext attack (IND-CPA) and indistinguishability under chosen ciphertext attack (IND-CCA). We also take recourse to the notion of indistinguishability under generalized chosen ciphertext attack (IND-gCCA)[1] security. Commitment scheme has also been used as a building block in the one of the generic constructions of signcryption. For commitment schemes, we refer to the standard notions of Hiding, Binding and rConcealment[2].

In the classical setting, An, Dodis and Rabin [ADR02] proposed generic constructions of signcryption schemes based on three paradigms, viz., encrypt-then-sign ($\mathcal{E}t\mathcal{S}$), sign-then-encrypt ($\mathcal{S}t\mathcal{E}$) and commit-then-encrypt-and-sign ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$). Security in each paradigm was proven in two-user insider and outsider models. In insider model the adversary is allowed to corrupt all parties except the receiver (resp. sender) in case of confidentiality (resp. unforgeability) whereas in outsider model the adversary is allowed to corrupt all parties except the sender and receiver. The $\mathcal{E}t\mathcal{S}$ paradigm preserves sUF-CMA and IND-gCCA security of the primitive signature scheme and encryption scheme respectively in the insider model. The $\mathcal{S}t\mathcal{E}$ paradigm preserves wUF-CMA and IND-CCA security of the primitive signature scheme and encryption scheme respectively in insider model. On the other hand, $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm can preserve only weak security in insider model, viz., the wUF-CMA security and IND-gCCA security of the primitive signature scheme and encryption scheme respectively. In the two-user outsider model, it was shown that the weak security of the encryption (resp. signature) scheme in the $\mathcal{E}t\mathcal{S}$ (resp. $\mathcal{S}t\mathcal{E}$) paradigm gets amplified to strong if the base signature (resp. encryption) satisfies a stronger definition. However, it was argued in [DZ10] that the same result doesn't hold in the multi-user outsider model.

Some Notations. Here, we assume that the reader is familiar with the basic concepts of quantum computation discussed in Section 2. We represent quantum states using the braket notation. In the discussion which follows, we deal with quantum adversaries that can query cryptographic oracles (such

[1] IND-gCCA notion is a generalization of IND-CCA security notion where the adversary is forbidden from making certain decryption queries which are related to the challenge ciphertext. For more details refer to [ADR02].

[2] Informally, rConcealment ensures that given a commitment pair (com, decom) corresponding to a message m, it is difficult to produce com′ ≠ com such that the pair (com′, decom) opens to a valid message [NP16].

as signcryption, unsigncryption, etc.) on quantum superposition of classical input values. A quantum superposition query comprises of different component registers. For example, a signcryption query of the form $\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{u}_\mathsf{p}\rangle$ consists of a message register and a signcryption text register. The action of cryptographic oracles (such as signcryption, unsigncryption, etc.) on quantum states is represented as a unitary transformation. For example, signcryption of $\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{u}_\mathsf{p}\rangle$ is represented as:

$$\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{u}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{u}_\mathsf{p} \oplus \mathsf{u}\rangle .$$

The challenge of simulating quantum queries. Before proceeding to discuss about results, we first discuss a unique feature of the quantum queries that needs to be tackled in our proofs. We elaborate on this problem in the context of the proof of authenticity of $\mathcal{E}t\mathcal{S}$ paradigm in the two user insider security model. Given an adversary $\mathcal{A}$ against the $\mathsf{sUF\text{-}CMA}$ security of signcryption scheme SC one has to construct a simulator $\mathcal{B}$ that breaks the $\mathsf{sUF\text{-}CMA}$ security of the underlying signature scheme PKS. Classically, to simulate a signcryption query m, the simulator first encrypts m using the public key to obtain the ciphertext c. Then, the simulator requests its challenger for a signature oracle query on c. The challenger replies with the signature σ and the simulator returns $\mathsf{u} := (\mathsf{c}, \sigma)$ to the adversary.

However, in the quantum setting, an adversary can prepare an arbitrary superposition of classical messages, which it can then send as a signcryption query. For example, let $\mathsf{m}_{\mathsf{quant}} = \sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{u}_\mathsf{p}\rangle$ be a signcryption query which consists of two components called respectively the message register M and signcryption text register U. In the security game, the adversary initializes the signcryption text register $\mathsf{U} = (\mathsf{C}, \mathsf{S})$ arbitrarily with values $(\mathsf{c}_\mathsf{p}, \sigma_\mathsf{p})$ on its own and the task of the simulator is to return to $\mathcal{A}$ the state $\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{c}_\mathsf{p} \oplus \mathsf{c}, \sigma_\mathsf{p} \oplus \sigma\rangle$. As long as the content of c_p is not known to the simulator, xoring the output of encryption with c_p will result in an unknown string. Hence, the simulator cannot simply send the prepared ciphertext register to its own challenger to obtain the signature as it would yield a signature on $\mathsf{c}_\mathsf{p} \oplus \mathsf{c}$ instead of c. Furthermore, the destructiveness of quantum measurement disallows the simulator from performing any kind of measurement on the signcryption text register. Also, quantum no-cloning prevents the simulator from copying adversary's query. One solution for the above problem is to store the encryption output in an ancilla register (an auxiliary register with constant input), initially set to $|0^{\ell_c}\rangle$, where ℓ_c is the length of ciphertext register. The encryption operator is applied on the message register and ancilla register as described below.

$$\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{c}_\mathsf{p}, \sigma_\mathsf{p}, 0^{\ell_c}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{c}_\mathsf{p} \oplus \mathsf{c}, \sigma_\mathsf{p}, 0^{\ell_c} \oplus \mathsf{c}\rangle \tag{1}$$

Then, the simulator can send a signature query on the last two registers, the result of which will be $\sum_{\mathsf{m},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{c}_\mathsf{p} \oplus \mathsf{c}, \sigma_\mathsf{p} \oplus \sigma, \mathsf{c}\rangle$. The last register can be called as simulator's state and the adversary is given everything except the simulator's state. But in the above process the simulator's state gets entangled with adversary's state. Further, it was recently shown in [Zha18] that the adversary can detect this type of behavior and may refuse to continue, rendering the simulation to fail.

Similar problem arises in the proof of confidentiality of $\mathcal{E}t\mathcal{S}$ paradigm in the two user insider security model. Classically, to simulate an unsigncryption query $\mathsf{u} = (\mathsf{c}, \sigma)$, the simulator first checks if σ is valid signature on c. If this is the case, simulator requests for a decryption oracle query on c to its challenger. The challenger replies with the decryption m if it is a valid query else it replies with $\perp$ and the simulator returns the same to the adversary. In the quantum case, to answer a query $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle$, conditioned on the validity of the signature on the ciphertext the simulator returns the underlying message or $\perp$. If the simulator follows a similar process, it ends up with the state

$$\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} \left|\mathsf{c}, \sigma, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{m}), \mathsf{m}\right\rangle \tag{2}$$

where

$$f(\mathsf{u}, \mathsf{m}) = \begin{cases} \mathsf{m} & \text{if } \mathcal{V}(\mathsf{c}, \sigma) = 1 \\ \perp & \text{otherwise.} \end{cases}$$

The adversary is returned everything except the last register. Again, in this case the simulation may fail as the simulator's state gets entangled with the adversary's state.

Entangle-then-Unentangle. The problem is to construct a quantum circuit for a function f, say signcryption oracle, which takes as input (x, y) and outputs $(x, y \oplus f(x))$. However, as shown above, in the process of constructing such a circuit some garbage bits (a.k.a ancilla bits) gets entangled with the registers x, y. In other words, for an input (x, y), we obtain as output $(x, y \oplus f(x), g(x))$, where $g(x)$ represents the garbage bits. By using ideas derived from the uncomputation technique [NC00], one can construct a quantum circuit for f that uncomputes the garbage bits $g(x)$ and provides the desired output $(x, y \oplus f(x))$. However, for uncomputing the garbage bits, the simulator must have access to the reverse of the circuit used to compute the garbage bits. In our case, the simulator $\mathcal{B}$ performs uncomputation either by running the respective algorithm twice locally on the same input (using the same randomness) or by making the same queries twice provided that the oracle is deterministic. Since, in this whole process of simulation the ancilla register first gets entangled with the input registers and then gets unentangled, we call it as *Entangle-then-Unentangle* (EtU) in the rest of this paper.

We use the EtU technique to simulate signcryption and unsigncryption queries. To handle a signcryption query in the $\mathcal{E}t\mathcal{S}$ paradigm, the simulator can choose a classical randomness while applying the encryption operator. To unentangle the ancilla register with the adversary's state, the simulator can apply the encryption operator on the output state of Equation 1 using the same randomness

$$\sum_{\mathsf{m},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{u_p} \oplus \mathsf{u}, \mathsf{c}\right\rangle \longmapsto \sum_{\mathsf{m},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{u_p} \oplus \mathsf{u}, \mathsf{c} \oplus \mathsf{c}\right\rangle.$$

The final state that the simulator obtains is $\sum_{\mathsf{m},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{u_p} \oplus \mathsf{u}\right\rangle \otimes \left|0^{\ell_c}\right\rangle$.

Similarly, to unentangle the ancilla register with the adversary's state in unsigncryption queries in $\mathcal{E}t\mathcal{S}$ paradigm, the simulator can request a decryption oracle query on the state appearing in Equation 2. The challenger, in response, applies the following unitary operation

$$\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} \left|\mathsf{u}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{m}), \mathsf{m}\right\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} \left|\mathsf{u}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{m}), \mathsf{m} \oplus \mathsf{m}\right\rangle.$$

The final state that the simulator receives is $\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} \left|\mathsf{u}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{m})\right\rangle \otimes \left|0^{\ell_m}\right\rangle$, where ℓ_m is the length of message register.

Note that, by this approach the ancilla register gets unentangled with adversary's state and hence, the adversary's view is properly simulated.

Our Contributions. In this paper, we initiate the formal study of security of signcryption in the quantum setting. We first propose appropriate quantum security definitions for signcryption, which are natural adaptation of the existing classical definitions to the quantum setting. We investigate the quantum security of generic constructions of signcryption schemes based on three paradigms, viz., $\mathcal{E}t\mathcal{S}$, $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$. In the multi-user insider model, our results are along the expected lines with one exception in the $\mathcal{S}t\mathcal{E}$ paradigm. In the outsider model, however, the quantum no-cloning stands as a main barrier in proving full quantum security. Nonetheless, we consider an intermediate setting where the signcryption oracle remains classical and the unsigncryption oracle can be quantumly accessed. Intuitively, this models a setting where the sender always runs the protocol on a classical device whereas the receiver may run the protocol on a quantum device. To model confidentiality, we introduce the notion of uqCCA security which means that the adversary is only provided quantum access to the unsigncryption oracle and access to signcryption oracle remains classical. Similarly, for authenticity we introduce the notion of uqCMA security. We analyze outsider security in the above setting. Interestingly, our results in the multi-user outsider model strengthen the existing classical results. To prove our results, we make use of a technique, based on uncomputation, which we call *Entangle-then-Unentangle* (*EtU*), that facilitates simulating quantum queries in security reductions.

In more detail, our contributions (also see Table 1) are as follows:

Encrypt-then-Sign: The $\mathcal{E}t\mathcal{S}$ paradigm preserves sUF-qCMA and IND-qgCCA[3] security of the primitive signature scheme and encryption scheme respectively in the multi-user insider security model. In the two-user outsider model, we show that post-quantum IND-CPA security of the underlying encryption scheme can be amplified to IND-uqCCA (resp. IND-uqgCCA) security, if the signature scheme is post quantum sUF-CMA (resp. wUF-CMA). While this is in line with the classical setting, our result in the multi-user outsider model is somewhat surprising. In particular, we establish that IND-qgCCA security of the underlying encryption scheme can be amplified to IND-uqCCA security if the signature scheme is post quantum sUF-CMA secure. As a consequence, we obtain a similar result in the classical setting which, to the best of our knowledge, was not known prior to this work.

Sign-then-Encrypt: The $\mathcal{S}t\mathcal{E}$ paradigm preserves IND-qCCA security of the primitive encryption scheme and wUF-qCMA of the signature scheme in the multi-user insider security model. In the two-user outsider model, we show that post-quantum UF-NMA security of the underlying signature scheme can be amplified to sUF-uqCMA (resp. wUF-uqCMA) security, if the encryption scheme is IND-qCCA (resp. IND-qgCCA), exactly as in the classical setting. As in the case of confidentiality of $\mathcal{E}t\mathcal{S}$ paradigm in the multi-user outsider model, we show that wUF-qCMA security of the underlying signature scheme can be amplified to sUF-uqCMA security if the encryption scheme is IND-qCCA secure. Again, this result naturally holds in the classical setting but was not known prior to this work.

Commit-Encrypt-and-Sign: The $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm preserves wUF-qCMA and IND-qgCCA security of the primitive signature scheme and encryption scheme respectively in the multi-user insider security model assuming that the commitment scheme satisfies some standard security properties. In the outsider model, we show that the IND-qCCA and post quantum sUF-CMA security of the underlying encryption and signature are preserved under reasonable assumptions on the commitment scheme. This result too holds in the classical setting but was not known prior to this work.

Our results for the $\mathcal{E}t\mathcal{S}$ and $\mathcal{S}t\mathcal{E}$ paradigms in the two-user outsider model also extend to the symmetric setting. In this course, we point out a flaw in the quantum security proof of authenticated encryption in the

[3] sUF-qCMA is the quantum analogue of classical sUF-CMA security notion where the adversary can query the signature oracle quantumly on a superposition of messages. Similarly, IND-qCCA and IND-qgCCA are quantum analogues of IND-CCA and IND-gCCA notions of security. For formal definitions, refer to Section 3.

$\mathcal{E}t\mathcal{S}$ paradigm given in a recent paper [SJS16]. Thus, the full quantum security of signcryption in outsider model and authenticated encryption remains an open problem.

Finally, we briefly recall some candidates for post-quantum and quantum secure signature and encryption schemes which can be used to instantiate the generic constructions of post-quantum and quantum secure signcryption schemes.

Prim	Paradigms					
	$\mathcal{E}t\mathcal{S}$		$\mathcal{S}t\mathcal{E}$		$\mathcal{C}t\mathcal{E}\&\mathcal{S}$	
	Confidentiality	Authenticity	Confidentiality	Authenticity	Confidentiality	Authenticity
E	IND-qgCCA	-	IND-(qg/q)CCA	-	IND-qgCCA	-
S	-	(w/s)UF-qCMA	-	wUF-qCMA	-	wUF-qCMA
C	-	-	-	-	qHiding $\wedge$ qrCon	qBinding
SC^i	dM-IND-iqgCCA	dM-(w/s)UF-iqCMA	dM-IND-i(qg/q)CCA	dM-wUF-iqCMA	dM-IND-iqgCCA	dM-wUF-iqCMA
Thm	Thm 5.1	Thm 5.2	Thm 5.3	Thm 5.4	Thm 5.5	Thm 5.6
E	pqIND-CPA			IND-(qg/q)CCA		
S	pq(w/s)UF-CMA	Same as	Same as	pqUF-NMA	Same as	Same as
C	-	Insider	Insider	-	Multi-User	Multi-User
SC^2	IND-o(uqg/uq)CCA	Model	Model	(w/s)UF-ouqCMA	Outsider	Outsider
Thm	Thm 6.1			Thm 6.2	Setting	Setting
E	IND-qgCCA			IND-qCCA	IND-qCCA	IND-qCCA
S	pqsUF-CMA	Same as	Same as	pqwUF-CMA	pqsUF-CMA	pqsUF-CMA
C	-	Insider	Insider	-	qHiding	qfBinder
SC^o	fM-IND-ouqCCA	Model	Model	fM-sUF-ouqCMA	fM-IND-ouqCCA	fM-sUF-ouqCMA
Thm	Thm 6.3			Thm 6.4	Thm 6.5	Thm 6.6

The abbreviations Thm, E, S and C stand for Theorem, Encryption, Signature and Commitment respectively. The symbols SC^i, SC^o and SC^2 denote Signcryptions in multi-user insider, multi-user outsider and two-user outsider models respectively. The logical flow "$(t_1/t_2)Y$ implies $(p_1/p_2)V$" means t_1Y (resp. t_2Y) implies p_1V (resp. p_2V). Refer to Section 3 for other notations.

Table 1: A summary of our results.

Some Related Works. Recently, there have been works which study the security of joint signature and encryption in the quantum setting. In [GM18], the authors construct a concrete post-quantum signcryption scheme based on the lattice assumption. In [SJS16], the authors extended the study of authenticated encryption of [BN08] from classical to quantum setting. In a different line than ours, [AGM18] gives definitions for confidentiality and authentication of *quantum* data followed by constructions realizing them.

Organization. In Section 3, we propose definitions for commitment and signcryption in the quantum setting. Section 4 contains the construction of signcryption schemes based on different paradigms. In Sections 5 and 6, we prove the quantum security of generic constructions of signcryption scheme in the insider and outsider models respectively. In Section 7, we discuss concrete instantiation for the generic constructions. We have deferred the details of some proofs to Appendix A and B.

2 Preliminaries

2.1 Notations

For $m \in \mathbb{N}$, $[m]$ denotes the set $\{1, \ldots, m\}$. We use $\lambda \in \mathbb{N}$ to denote the security parameter. A function $\epsilon = \epsilon(\lambda)$ is said to be negligible if, for all polynomials $p(n)$, $\epsilon(n) < 1/p(n)$ for large enough n. For two strings x and y, $x\|y$ represents the concatenation of the two strings. For a string $str = str_1\|\ldots\|str_n \in \{0,1\}^{t_1} \times \cdots \times \{0,1\}^{t_n}$, we use $[str]_i$ to represent the i^{th} component str_i.

2.2 Quantum Computation

In this section, we recall a few basic concepts of quantum computation from [NC00]. A quantum system $\mathcal{H}$ is a complex euclidean space (a.k.a., Hilbert space). The state of a quantum system is completely described by its state vector $|\psi\rangle$ which is a unit vector ($\langle\psi|\psi\rangle = 1$) in the system's state space. Given quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the joint quantum system is given by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. Given $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, the joint state (product state) is given by $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. The joint state $|\psi_1\rangle \otimes |\psi_2\rangle$ is also denoted as $|\psi_1\rangle |\psi_2\rangle$ or $|\psi_1, \psi_2\rangle$ in many places. In general, the joint state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ cannot be expressed as a product state. If $|\psi\rangle$ is not a product state, we say that the systems $\mathcal{H}_1$ and $\mathcal{H}_2$ are entangled. If $|\psi\rangle$ is a product state, we say the systems are unentangled.

The evolution of a closed quantum system is completely described by a unitary transformation. In particular, if $|\psi\rangle$ is a quantum state and U be any unitary transformation, then the resulting state after transformations is $|\psi'\rangle = U|\psi\rangle$.

For a n qubit system, the dimension of the Hilbert space $\mathcal{H}$ is 2^n. The set $\{|i\rangle : 0 < i \leq 2^n\}$ forms an orthonormal basis of $\mathcal{H}$, where $|i\rangle$ is a column vector with only the i^{th} bit set to 1 and all other bits set to 0. The set $\{|i\rangle\}$ is also called as computational basis. If an element $|\psi\rangle \in \mathcal{H}$ is a linear combination of several $|i\rangle$, then $|\psi\rangle$ is said to be in superposition of computational basis states. Given a quantum state $|\psi\rangle$, measurement in the computational basis yields a value i with probability $|\langle i|\psi\rangle|^2$. After measurement, conditioned on the measurement outcome being i, $|\psi\rangle$ collapses to the state $|i\rangle$.

A register is a memory element and is associated with a finite non-empty set of classical states.

By appending a state $|\psi_1\rangle \in \mathcal{H}_1$ to a state $|\psi_2\rangle \in \mathcal{H}_2$, we mean the joint state $|\psi_1\rangle |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. In the security proofs, we append the state $|0^m\rangle$ to various states, where $m \in \mathbb{N}$ may denote the length of ciphertext/signcryption text/signature and is understood from the context.

3 Syntax and Security Definitions

We adopt the definitions given in [BZ13] for security of encryption and signature in the quantum setting. The quantum variant of IND-gCCA security notion [ADR02] was not formalized in [BZ13]. However, it follows as a natural extension of the definition of IND-qCCA security. In addition, we formulate new security definitions for commitment and signcryption in the quantum setting. The definitions we propose follow naturally from their classical counterparts [BSZ07, ADR02, MMS09, NP16].

3.1 Public Key Encryption

Public Key Encryption Scheme. A public key encryption (PKE) scheme consists of three PPT algorithms: $\mathcal{G}_\mathcal{E}, \mathcal{E}$ and $\mathcal{D}$.

- $\mathcal{G}_\mathcal{E}$: It takes as input a security parameter λ and outputs a public key and private key pair $(\mathsf{pk}, \mathsf{sk})$.
- $\mathcal{E}$: It takes as input a message $\mathsf{m} \in \mathcal{M}$, where $\mathcal{M}$ is the message space, and the public key pk and outputs a ciphertext c.
- $\mathcal{D}$: It takes as input a ciphertext c and the secret key sk and outputs a message $\mathsf{m} \in \mathcal{M}$ or $\perp$.

Correctness: For all $(\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G}_\mathcal{E}(1^\lambda)$ and for all messages $\mathsf{m} \in \mathcal{M}$, it is required that $\mathcal{D}(\mathcal{E}(\mathsf{m}, \mathsf{pk}), \mathsf{sk}) = \mathsf{m}$.

Security of PKE in the Quantum Setting.

Definition 1. *A public key encryption scheme* $\mathsf{PKE} = (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be post-quantum indistinguishable under chosen ciphertext attack* ($\mathsf{pqIND\text{-}CCA}$) *if for all quantum PPT adversaries* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$*, the advantage*

$$\mathsf{Adv}^{\mathsf{pqIND\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda) := \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|$$

in $\mathsf{Exp}^{\mathsf{pqIND\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda)$ *defined in Figure 1 is a negligible function in security parameter* λ*, where* $\mathcal{A}$ *is provided classical access to decryption oracle* $\mathcal{O}_D$ *(described below) with a natural restriction* NRn *that* c^* *can never queried to* $\mathcal{O}_D$*.*

- Decryption oracle *($\mathcal{O}_D$): Given a classical ciphertext* c*, oracle returns* $\mathcal{D}(\mathsf{c}, \mathsf{sk})$*.*

```
$\mathsf{Exp}^{\mathsf{pqIND\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda)$:
  • $(\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$
  • $(\mathsf{m}_0, \mathsf{m}_1, st) \longleftarrow \mathcal{A}_1^{\mathcal{O}_D}(1^\lambda, \mathsf{pk})$ with $|\mathsf{m}_0| = |\mathsf{m}_1|$
  • $b \xleftarrow{\mathrm{U}} \{0,1\}$
  • $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk})$
  • $b' \longleftarrow \mathcal{A}_2^{\mathcal{O}_D}(1^\lambda, \mathsf{pk}, \mathsf{c}^*, st)$
```

Figure 1: Experiment for confidentiality ($\mathsf{pqIND\text{-}CCA}$ security)

Definition 2. *A public key encryption scheme* $\mathsf{PKE} = (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be post-quantum indistinguishable under chosen plaintext attack* ($\mathsf{pqIND\text{-}CPA}$) *if it satisfies the same definition as* $\mathsf{pqIND\text{-}CCA}$ *with the exception that the adversary is forbidden to ask decryption oracle queries.*

Remark: By post-quantum security, we mean the adversary can perform local quantum computation. Hence, if any hash function is modeled as random oracle it is required that the adversary must be given quantum access to the random oracle as illustrated in [BDF+11]. This model is also called as the Quantum Random Oracle Model (QROM). This is also applicable in other contexts, viz., signature, commitment and signcryption.

Definition 3 ([BZ13])**.** *A public key encryption scheme* $\mathsf{PKE} = (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be indistinguishable under a quantum chosen ciphertext attack* ($\mathsf{IND\text{-}qCCA}$) *if it satisfies the same definition as* $\mathsf{pqIND\text{-}CCA}$ *with the exception that the adversary is provided superposition access to decryption oracle* $\mathcal{O}^{\mathsf{q}}_D$ *(described below).*

- Quantum Decryption oracle *($\mathcal{O}^{\mathsf{q}}_D$): For each superposition query, the oracle decrypts all ciphertexts in the superposition, except those that were returned in response to a challenge query:*

$$\sum_{\mathsf{c},\mathsf{m_p}} \psi_{\mathsf{c},\mathsf{m_p}} \left|\mathsf{c}, \mathsf{m_p}\right\rangle \longmapsto \sum_{\mathsf{c},\mathsf{m_p}} \psi_{\mathsf{c},\mathsf{m_p}} \left|\mathsf{c}, \mathsf{m_p} \oplus f(\mathsf{c})\right\rangle \tag{3}$$

  where

$$f(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathsf{c} = \mathsf{c}^* \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}) & \text{otherwise.} \end{cases}$$

Now, we consider the $\mathsf{IND\text{-}qgCCA}$ notion of security which is the quantum analogue of $\mathsf{IND\text{-}gCCA}$ security [ADR02]. It is defined in a way similar to $\mathsf{IND\text{-}qCCA}$ except that the adversary is forbidden from making certain type of decryption queries. Let $\mathcal{R}$ be an equivalence relation over the ciphertexts which can depend on the public key pk. $\mathcal{R}$ is said to be decryption respecting if $\mathcal{R}(\mathsf{c}_1, \mathsf{c}_2) = \mathsf{True}$ implies that $\mathcal{D}(\mathsf{c}_1, \mathsf{sk}) = \mathcal{D}(\mathsf{c}_2, \mathsf{sk})$. $\mathcal{A}$ is not allowed to query on c if $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$. A superposition query can be handled by modifying the description of f in Equation 3 in the following way:

$$f(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}) & \text{otherwise.} \end{cases}$$

Definition 4. *A public key encryption scheme* $\mathsf{PKE} = (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be* $\mathsf{IND\text{-}qgCCA}$ *secure, if there exists some efficient decryption-respecting relation* $\mathcal{R}$ *w.r.t. which it is* qCCA *secure.*

3.2 Public Key Signature

Public Key Signature Scheme. A public key signature (PKS) scheme consists of three PPT algorithms: $\mathcal{G}_{\mathcal{S}}, \mathcal{S}$ and $\mathcal{V}$.

- $\mathcal{G}_{\mathcal{S}}$: It takes as input a security parameter λ and outputs a public key and private key pair $(\mathsf{pk}, \mathsf{sk})$.
- $\mathcal{S}$: It takes as input a message $\mathsf{m} \in \mathcal{M}$, where $\mathcal{M}$ is the message space, and the secret key sk and outputs a signature σ.
- $\mathcal{V}$: It takes as input a message-signature pair (m, σ) and the public key pk. It outputs a value 1 if (m, σ) is a valid message-signature pair else it outputs 0.

Correctness: For all $(\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and for all messages $\mathsf{m} \in \mathcal{M}$, it is required that

$$\mathcal{V}(\mathsf{m}, \mathcal{S}(\mathsf{m}, \mathsf{sk}), \mathsf{pk}) = 1.$$

Security of PKS in the Quantum Setting.

Definition 5. *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is post-quantum strongly existentially unforgeable under a chosen message attack* $(\mathsf{pqsUF\text{-}CMA})$ *if, for any quantum PPT algorithm* $\mathcal{A}$*, the advantage*

$$\mathsf{Adv}^{\mathsf{pqsUF\text{-}CMA}}_{\mathcal{A},\mathsf{PKS}}(\lambda) := \Pr\left[\mathcal{V}(\mathsf{m}^*, \sigma^*, \mathsf{pk}) = 1 \;\middle|\; \begin{array}{c} (\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda); \\ (\mathsf{m}^*, \sigma^*) \longleftarrow \mathcal{A}^{\mathcal{O}_{Sg}}(1^\lambda, \mathsf{pk}) \end{array}\right]$$

is a negligible function in λ*, where* $\mathcal{A}$ *is provided access to sign oracle* $\mathcal{O}_{Sg}$ *(described below) with a natural restriction that if* σ *is a signature obtained from signature oracle on the message* m*, then* $(\mathsf{m}, \sigma) \neq (\mathsf{m}^*, \sigma^*)$.

- Signature oracle *($\mathcal{O}_{Sg}$): Given a message* m*, oracle returns* $\sigma \longleftarrow \mathcal{S}(\mathsf{m}, \mathsf{sk})$.

Definition 6. *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is post-quantum weakly existentially unforgeable under a chosen message attack* $(\mathsf{pqwUF\text{-}CMA})$ *if it satisfies the same definition as* $\mathsf{pqsUF\text{-}CMA}$*, except the requirement that the forged message* m^* *was not queried to the signature oracle.*

Definition 7. *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is post-quantum existentially unforgeable under no message message attack* $(\mathsf{pqUF\text{-}NMA})$ *if the probability that any quantum PPT algorithm* $\mathcal{A}$*, provided no access to the signature oracle, produces a valid message-signature pair is negligible in* λ.

Definition 8 ([BZ13])**.** *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is strongly existentially unforgeable under quantum chosen message attack* (sUF-qCMA) *if, for any quantum PPT algorithm* $\mathcal{A}$ *and any polynomial* q*, the advantage*

$$\mathsf{Adv}^{\mathsf{sUF\text{-}qCMA}}_{\mathcal{A},\mathsf{PKS}}(\lambda) := \Pr\left[\mathcal{V}(\mathsf{m}_i, \sigma_i, \mathsf{pk}) = 1 \forall i \in [q+1] \;\middle|\; \begin{array}{c} (\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda); \\ \{(\mathsf{m}_i, \sigma_i) : i \in [q+1]\} \longleftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{q}}_{Sg}}(1^\lambda, \mathsf{pk}) \end{array}\right]$$

is a negligible function in λ*, where* $\mathcal{A}$ *is provided superposition access to signature oracle* $\mathcal{O}^{\mathsf{q}}_{Sg}$ *(described below),* q *is the number of signature oracle queries and the* $q+1$ *forgeries, viz.,* $\{(\mathsf{m}_i, \sigma_i) : i \in [q+1]\}$ *are pairwise distinct.*

- Quantum Signature oracle *(*$\mathcal{O}^{\mathsf{q}}_{Sg}$*): For each query, the oracle chooses randomness* r*, and responds by signing each message in the query using* r *as randomness:*

$$\sum_{\mathsf{m},\sigma_{\mathsf{p}}} \psi_{\mathsf{m},\sigma_{\mathsf{p}}} |\mathsf{m}, \sigma_{\mathsf{p}}\rangle \longmapsto \sum_{\mathsf{m},\sigma_{\mathsf{p}}} \psi_{\mathsf{m},\sigma_{\mathsf{p}}} |\mathsf{m}, \sigma_{\mathsf{p}} \oplus \mathcal{S}(\mathsf{m}, \mathsf{sk}; r)\rangle .$$

Definition 9 ([BZ13])**.** *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is weakly existentially unforgeable under a quantum chosen message attack* (wUF-qCMA) *if it satisfies the same definition as* sUF-qCMA*, except the requirement that the* $q+1$ *message-signature pairs should have distinct messages.*

3.3 Commitment

Commitment Scheme. A non-interactive commitment (C) scheme consists of three PPT algorithms: CSetup, Commit and Open.

- CSetup: It takes as input a security parameter λ and outputs a public commitment key $\mathcal{CK}$.
- Commit: It takes as input a message $\mathsf{m} \in \mathcal{M}$, where $\mathcal{M}$ is the message space, and the public commitment key $\mathcal{CK}$ and returns a pair (com, decom), where com and decom are the commitment and decommitment of m respectively.
- Open: It takes as input a pair (com, decom) and the commitment key $\mathcal{CK}$ and outputs $\mathsf{m} \in \mathcal{M}$ or $\perp$.

Correctness: For all $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$ and for all messages $\mathsf{m} \in \mathcal{M}$, it is required that

$$\mathsf{Open}(\mathsf{Commit}(\mathsf{m}, \mathcal{CK}), \mathcal{CK})^4 = \mathsf{m}.$$

Security of Commitment in the Quantum Setting. A stronger property for commitment in the quantum setting was defined in [Unr16]. But for our purpose, the following definitions suffice.

Definition 10. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* qHiding *property, if for any quantum PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

$$\mathsf{Adv}^{\mathsf{qHiding}}_{\mathcal{A},\mathsf{C}}(\lambda) := \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|$$

in $\mathsf{Exp}^{\mathsf{qHiding}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 2 is a negligible function in security parameter* λ*.*

[4] Hereafter, for simplicity, we will skip writing $\mathcal{CK}$ in the input argument of Open and Commit.

```
$\underline{\mathsf{Exp}^{\mathsf{qHiding}}_{\mathcal{A},\mathsf{C}}(\lambda)}$:
    • $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$
    • $(\mathsf{m}_0, \mathsf{m}_1, st) \longleftarrow \mathcal{A}_1(1^\lambda, \mathcal{CK})$
    • $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$
    • $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$
    • $b' \longleftarrow \mathcal{A}_2(1^\lambda, \mathcal{CK}, \mathsf{com}^*, st)$
```

Figure 2: Experiment for qHiding

Definition 11. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* qBinding *property, if for any quantum PPT algorithm* $\mathcal{A}$ *the advantage*

$$\mathsf{Adv}^{\mathsf{qBinding}}_{\mathcal{A},\mathsf{C}}(\lambda) := \Pr\left[(\mathsf{m} \neq \mathsf{m}') \wedge (\mathsf{m}, \mathsf{m}' \neq \bot)\right]$$

in $\mathsf{Exp}^{\mathsf{qBinding}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 3 is a negligible function in security parameter* λ*.*

Definition 12. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* qfBinder *property, if for any quantum PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

$$\mathsf{Adv}^{\mathsf{qfBinder}}_{\mathcal{A},\mathsf{C}}(\lambda) := \Pr\left[\mathsf{Open}(\mathsf{com}, \mathsf{decom}') \neq \bot\right]$$

in $\mathsf{Exp}^{\mathsf{qfBinder}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 3 is a negligible function in security parameter* λ*.*

```
$\underline{\mathsf{Exp}^{\mathsf{qBinding}}_{\mathcal{A},\mathsf{C}}(\lambda)}$:
    • $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$
    • $(\mathsf{com}, \mathsf{decom}, \mathsf{decom}') \longleftarrow \mathcal{A}(1^\lambda, \mathcal{CK})$
    • $\mathsf{m} \longleftarrow \mathsf{Open}(\mathsf{com}, \mathsf{decom})$
    • $\mathsf{m}' \longleftarrow \mathsf{Open}(\mathsf{com}, \mathsf{decom}')$
```

```
$\underline{\mathsf{Exp}^{\mathsf{qfBinder}}_{\mathcal{A},\mathsf{C}}(\lambda)}$:
    • $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$
    • $(\mathsf{m}, st) \longleftarrow \mathcal{A}_1(1^\lambda, \mathcal{CK})$
    • $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$
    • $\mathsf{decom}' \longleftarrow \mathcal{A}_2(1^\lambda, \mathcal{CK}, \mathsf{com}, st)$
```

Figure 3: Experiment for qBinding and qfBinder

Definition 13. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* qrConcealment *property, if for any quantum PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

$$\mathsf{Adv}^{\mathsf{qrConcealment}}_{\mathcal{A},\mathsf{C}}(\lambda) := \Pr\left[\mathsf{Open}(\mathsf{com}', \mathsf{decom}) \neq \bot \wedge \mathsf{com} \neq \mathsf{com}'\right]$$

in $\mathsf{Exp}^{\mathsf{qrConcealment}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 4 is a negligible function in security parameter* λ*.*

$\underline{\mathsf{Exp}^{\mathsf{qrConcealment}}_{\mathcal{A},\mathsf{C}}(\lambda)}$:

- $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$
- $(\mathsf{m}, st) \longleftarrow \mathcal{A}_1(1^\lambda, \mathcal{CK})$
- $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$
- $\mathsf{com}' \longleftarrow \mathcal{A}_2(1^\lambda, \mathcal{CK}, \mathsf{com}, \mathsf{decom}, st)$

Figure 4: Experiment for qrConcealment

3.4 Signcryption

Signcryption Scheme. A signcryption (SC) scheme consists of five PPT algorithms: Setup, $\mathsf{KeyGen}_\mathsf{S}$, $\mathsf{KeyGen}_\mathsf{R}$, $\mathcal{SC}$ and $\mathcal{US}$.

- Setup: It takes as input a security parameter λ and outputs public parameters $\mathcal{PP}$.
- $\mathsf{KeyGen}_\mathsf{S}$: It takes as input $\mathcal{PP}$ and outputs a public key and private key pair $(\mathsf{pk}_\mathsf{S}, \mathsf{sk}_\mathsf{S})$ for the sender.
- $\mathsf{KeyGen}_\mathsf{R}$: It takes as input $\mathcal{PP}$ and outputs a public key and private key pair $(\mathsf{pk}_\mathsf{R}, \mathsf{sk}_\mathsf{R})$ for the receiver.
- $\mathcal{SC}$: It takes as input a message $\mathsf{m} \in \mathcal{M}$, where $\mathcal{M}$ is the message space, sender's private key sk_S and receiver's public key pk_R and outputs a signcryption text u.
- $\mathcal{US}$: It takes as input a signcryption text u, receiver's private key sk_R and sender's public key pk_S and outputs a message $\mathsf{m} \in \mathcal{M}$ or $\perp$.

Correctness: For all $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^\lambda)$, all $(\mathsf{pk}_\mathsf{S}, \mathsf{sk}_\mathsf{S}) \longleftarrow \mathsf{KeyGen}_\mathsf{S}(\mathcal{PP})$, all $(\mathsf{pk}_\mathsf{R}, \mathsf{sk}_\mathsf{R}) \longleftarrow \mathsf{KeyGen}_\mathsf{R}(\mathcal{PP})$ and for all $\mathsf{m} \in \mathcal{M}$, it is required that $\mathcal{US}(\mathcal{SC}(\mathsf{m}, \mathsf{sk}_\mathsf{S}, \mathsf{pk}_\mathsf{R}), \mathsf{sk}_\mathsf{R}, \mathsf{pk}_\mathsf{S}) = \mathsf{m}$.

Security of SC in the Quantum Setting.

Insider Model. In the insider model the adversary is allowed to corrupt all parties except the receiver (resp. sender) in case of confidentiality (resp. unforgeability).

Definition 14. *A signcryption scheme* SC *is said to be* pqIND-CCA *secure in dynamic multi-user insider model* (dM-pqIND-iCCA) *if for all quantum PPT algorithms* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$*, the advantage*

$$\mathsf{Adv}^{\mathsf{dM\text{-}pqIND\text{-}iCCA}}_{\mathcal{A},\mathsf{SC}}(\lambda) := \left|\mathsf{Pr}\left[b = b'\right] - \frac{1}{2}\right|$$

in $\mathsf{Exp}^{\mathsf{dM\text{-}IND\text{-}iCCA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 5 is a negligible function in security parameter* λ*, where* $\mathcal{A}$ *is provided classical access to unsigncryption oracle* $\mathcal{O}_U$ *(described below) with natural restrictions that* $(\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*})$ *was never queried to* $\mathcal{O}_U$ *and* $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ *is a valid pair.*

- Unsigncryption oracle *(*$\mathcal{O}_U$*): Given* $(\mathsf{u}^*, \mathsf{pk}_\mathsf{S})$*, oracle returns* $\mathcal{US}(\mathsf{u}^*, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_\mathsf{S})$.

$\underline{\mathsf{Exp}^{\mathsf{dM\text{-}pqIND\text{-}iCCA}}_{\mathcal{A},\mathsf{SC}}(\lambda)}$:

- $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^{\lambda})$
- $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathsf{KeyGen}_{\mathsf{R}}(\mathcal{PP})$
- $(\mathsf{m}_0, \mathsf{m}_1, \mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}, st) \longleftarrow \mathcal{A}_1^{\mathcal{O}_U}(\mathcal{PP}, \mathsf{pk}_{\mathsf{R}^*})$ with $|\mathsf{m}_0| = |\mathsf{m}_1|$
- $b \xleftarrow{\text{U}} \{0,1\}$
- $\mathsf{u}^* \longleftarrow \mathcal{SC}(\mathsf{m}_b, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$
- $b' \longleftarrow \mathcal{A}_2^{\mathcal{O}_U}(\mathcal{PP}, \mathsf{pk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{u}^*, st)$

Figure 5: Experiment for confidentiality (dynamic multi-user insider model)

Definition 15. *A signcryption scheme* SC *is said to be* IND-qCCA *secure in dynamic multi-user insider model* (dM-IND-iqCCA) *if it satisfies the same definition as* dM-pqIND-iCCA *with the exception that the adversary is provided superposition access to unsigncryption oracle $\mathcal{O}_U^{\mathsf{q}}$ (described below).*

- Quantum Unsigncryption oracle *($\mathcal{O}_U^{\mathsf{q}}$): For each such query, the challenger unsigncrypts all signcryption texts in the superposition, except those that were returned in response to a challenge query:*

$$\sum_{\mathsf{u},\mathsf{pk}_{\mathsf{S}},\mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u},\mathsf{pk}_{\mathsf{S}},\mathsf{m}_{\mathsf{p}}} |\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_{\mathsf{S}},\mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u},\mathsf{pk}_{\mathsf{S}},\mathsf{m}_{\mathsf{p}}} |\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\mathsf{u}, \mathsf{pk}_{\mathsf{S}})\rangle \tag{4}$$

where

$$f(\mathsf{u}, \mathsf{pk}_{\mathsf{S}}) = \begin{cases} \bot & \textit{if } (\mathsf{u}, \mathsf{pk}_{\mathsf{S}}) = (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*}) \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}}) & \textit{otherwise.} \end{cases}$$

The notion of dM-IND-iqgCCA can be defined in a similar way as in IND-qgCCA (Definition 4). We define an equivalence relation $\mathcal{R}$ over the pairs $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}})$. $\mathcal{R}$ is said to be unsigncryption-respecting if $\mathcal{R}((\mathsf{u}_1, \mathsf{pk}_{\mathsf{S}_1}), (\mathsf{u}_2, \mathsf{pk}_{\mathsf{S}_2})) = \mathsf{True} \implies (\mathcal{US}(\mathsf{u}_1, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}_1}) = \mathcal{US}(\mathsf{u}_2, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}_2})) \wedge (\mathsf{pk}_{\mathsf{S}_1} = \mathsf{pk}_{\mathsf{S}_2})$. The unsigncryption oracle query is restricted using relation $\mathcal{R}$ instead of equality relation. A superposition query can be handled by modifying the description of f in Equation 4 in the following way:

$$f(\mathsf{u}, \mathsf{pk}_{\mathsf{S}}) = \begin{cases} \bot & \text{if } \mathcal{R}((\mathsf{u}, \mathsf{pk}_{\mathsf{S}}), (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*})) = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}}) & \text{otherwise.} \end{cases}$$

Definition 16. *A signcryption scheme* SC *is said to be* IND-qgCCA *secure in dynamic multi-user insider model* (dM-IND-iqgCCA)*, if there exists some efficient unsigncryption-respecting relation $\mathcal{R}$ w.r.t. which it is* qCCA *secure.*

Definition 17. *A signcryption scheme* SC *is* pqsUF-CMA *secure in dynamic multi-user insider model* (dM-pqsUF-iCMA) *if, for any quantum PPT algorithm $\mathcal{A}$, the advantage*

$$\mathsf{Adv}^{\mathsf{dM\text{-}pqsUF\text{-}iCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda) := \Pr[\mathsf{m}^* \neq \bot]$$

in $\mathsf{Exp}^{\mathsf{dM\text{-}pqsUF\text{-}iCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ defined in Figure 6 is a negligible function in λ, where $\mathcal{A}$ is provided classical access to signcryption oracle $\mathcal{O}_S$ (described below) with natural restrictions that if u *is a signcryption obtained from signcryption oracle on* $(\mathsf{m}, \mathsf{pk}_{\mathsf{R}})$*, then* $(\mathsf{u}, \mathsf{m}, \mathsf{pk}_{\mathsf{R}}) \neq (\mathsf{u}^*, \mathsf{m}^*, \mathsf{pk}_{\mathsf{R}^*})$ *and* $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*})$ *is a valid pair.*

$\underline{\mathsf{Exp}^{\mathsf{dM\text{-}pqsUF\text{-}iCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)\text{:}}$

- $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^\lambda)$
- $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathsf{KeyGen}_{\mathsf{S}}(\mathcal{PP})$
- $(\mathsf{u}^*, \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{A}^{\mathcal{O}_S}(\mathcal{PP}, \mathsf{pk}_{\mathsf{S}^*})$
- $\mathsf{m}^* \longleftarrow \mathcal{US}(\mathsf{u}^*, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*})$

Figure 6: Experiment for unforgeability (dynamic multi-user insider model)

- Signcryption oracle *($\mathcal{O}_S$): Given* $(\mathsf{m}, \mathsf{pk}_{\mathsf{R}})$*, oracle returns* $\mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}})$.

Definition 18. *A signcryption scheme* SC *is* pqwUF-CMA *secure in dynamic multi-user insider model* (dM-pqwUF-iCMA) *if it satisfies the same definition as* dM-pqsUF-iCMA*, except the requirement that the the message* $(\mathsf{m}^*, \mathsf{pk}_{\mathsf{R}^*})$ *corresponding to the forgery was not queried to the signcryption oracle.*

Definition 19. *A signcryption scheme* SC *is* sUF-qCMA *secure in dynamic multi-user insider model* (dM-sUF-iqCMA) *if for any quantum PPT algorithm $\mathcal{A}$, the advantage*

$$\mathsf{Adv}^{\mathsf{dM\text{-}sUF\text{-}iqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda) := \Pr\left[\mathsf{m}_i \neq \bot \forall i \in [q+1]\right]$$

in $\mathsf{Exp}^{\mathsf{dM\text{-}sUF\text{-}iqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 7 is a negligible function in λ, where $\mathcal{A}$ is provided superposition access to signcryption oracle $\mathcal{O}^{\mathsf{q}}_S$ (described below), q is the number of signcryption oracle queries with the requirement that $q+1$ forgeries are pairwise distinct and* $(\mathsf{pk}_{\mathsf{R}i}, \mathsf{sk}_{\mathsf{R}i})$ *are valid key pairs for each $i \in [q+1]$.*

- Quantum Signcryption oracle *($\mathcal{O}^{\mathsf{q}}_S$): For each query, the oracle chooses randomness r, and responds by signcrypting each message in the query using r as randomness:*

$$\sum_{\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}}} \psi_{\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}}} \left|\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}}\right\rangle \longmapsto \sum_{\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}}} \psi_{\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}}} \left|\mathsf{m}, \mathsf{pk}_{\mathsf{R}}, \mathsf{u}_{\mathsf{p}} \oplus \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}}; r)\right\rangle.$$

$\underline{\mathsf{Exp}^{\mathsf{dM\text{-}sUF\text{-}iqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)\text{:}}$

- $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^\lambda)$
- $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathsf{KeyGen}_{\mathsf{S}}(\mathcal{PP})$
- $\{(\mathsf{u}_i, \mathsf{pk}_{\mathsf{R}i}, \mathsf{sk}_{\mathsf{R}i}) : i \in [q+1]\} \longleftarrow \mathcal{A}^{\mathcal{O}_S}(\mathcal{PP}, \mathsf{pk}_{\mathsf{S}^*})$
- $\mathsf{m}_i \longleftarrow \mathcal{US}(\mathsf{u}_i, \mathsf{sk}_{\mathsf{R}i}, \mathsf{pk}_{\mathsf{S}^*}), \forall i \in [q+1]$

Figure 7: Experiment for unforgeability (dynamic multi-user insider model)

Definition 20. *A signcryption scheme* SC *is* wUF-qCMA *secure in dynamic multi-user insider model* (dM-wUF-iqCMA) *if it satisfies the same definition as* dM-sUF-iqCMA*, except the requirement that the tuples* $\{(\mathcal{US}(\mathsf{u}_i, \mathsf{sk}_{\mathsf{R}i}, \mathsf{pk}_{\mathsf{S}^*}), \mathsf{pk}_{\mathsf{R}i}) : i \in [q+1]\}$ *are valid and pairwise distinct.*

Outsider Model. In the outsider model the adversary is allowed to corrupt all other parties except the sender and receiver for both confidentiality and unforgeability. In other words, adversary can only learn the public keys of sender and receiver and can learn secret keys of all other parties.

Definition 21. *A signcryption scheme* SC *is said to be* $\mathsf{IND\text{-}qCCA}$ *secure in multi-user outsider model* $(\mathsf{fM\text{-}IND\text{-}oqCCA})$ *if for all quantum PPT algorithms* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$*, the advantage*

$$\mathsf{Adv}_{\mathcal{A},\mathsf{SC}}^{\mathsf{fM\text{-}IND\text{-}oqCCA}}(\lambda) := \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|$$

in $\mathsf{Exp}_{\mathcal{A},\mathsf{SC}}^{\mathsf{fM\text{-}IND\text{-}oqCCA}}(\lambda)$ *defined in Figure 8 is a negligible function in security parameter* λ*, where* $\mathcal{A}$ *is provided superposition access to signcryption oracle* $\mathcal{O}_S^{\mathsf{q}}$ *and unsigncryption oracle* $\mathcal{O}_U^{\mathsf{q}}$ *(described below) with natural restrictions that* $(\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*})$ *was never queried to* $\mathcal{O}_U^{\mathsf{q}}$*.*

- Quantum Unsigncryption oracle *(*$\mathcal{O}_U^{\mathsf{q}}$*): For each such query, the challenger unsigncrypts all signcryption texts in the superposition, except those that were returned in response to a challenge query:*

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u}, \mathsf{pk}_\mathsf{S})\rangle \tag{5}$$

  where

$$f(\mathsf{u}, \mathsf{pk}_\mathsf{S}) = \begin{cases} \perp & \textit{if } (\mathsf{u}, \mathsf{pk}_\mathsf{S}) = (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*}) \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_\mathsf{S}) & \textit{otherwise.} \end{cases}$$

- Quantum Signcryption oracle *(*$\mathcal{O}_S^{\mathsf{q}}$*): For each query, the oracle chooses randomness* r*, and responds by signcrypting each message in the query using* r *as randomness:*

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p} \oplus \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R}; r)\rangle\,.$$

$\underline{\mathsf{Exp}_{\mathcal{A},\mathsf{SC}}^{\mathsf{fM\text{-}IND\text{-}oqCCA}}(\lambda):}$

- $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^\lambda)$
- $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathsf{KeyGen}_\mathsf{R}(\mathcal{PP})$
- $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathsf{KeyGen}_\mathsf{S}(\mathcal{PP})$
- $(\mathsf{m}_0, \mathsf{m}_1, st) \longleftarrow \mathcal{A}_1^{\mathcal{O}_U^{\mathsf{q}}, \mathcal{O}_S^{\mathsf{q}}}(\mathcal{PP}, \mathsf{pk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*})$ with $|\mathsf{m}_0| = |\mathsf{m}_1|$
- $b \xleftarrow{\mathrm{U}} \{0,1\}$
- $\mathsf{u}^* \longleftarrow \mathcal{SC}(\mathsf{m}_b, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$
- $b' \longleftarrow \mathcal{A}_2^{\mathcal{O}_U^{\mathsf{q}}, \mathcal{O}_S^{\mathsf{q}}}(\mathcal{PP}, \mathsf{pk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*}, \mathsf{u}^*, st)$

Figure 8: Experiment for confidentiality (multi-user outsider model)

The notion of $\mathsf{fM\text{-}IND\text{-}oqgCCA}$ can be defined in a similar way as in $\mathsf{IND\text{-}qgCCA}$ (Definition 4). We define an equivalence relation $\mathcal{R}$ over the pairs $(\mathsf{u}, \mathsf{pk}_\mathsf{S})$. $\mathcal{R}$ is said to be unsigncryption-respecting if $\mathcal{R}((\mathsf{u}_1, \mathsf{pk}_{\mathsf{S}_1}), (\mathsf{u}_2, \mathsf{pk}_{\mathsf{S}_2})) = \mathsf{True}$ implies that $(\mathcal{US}(\mathsf{u}_1, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}_1}) = \mathcal{US}(\mathsf{u}_2, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}_2})) \wedge (\mathsf{pk}_{\mathsf{S}_1} = \mathsf{pk}_{\mathsf{S}_2})$. The unsigncrypt oracle query is restricted using relation $\mathcal{R}$ instead of equality relation. A superposition query can be handled by modifying the description of f in Equation 5 in the following way:

$$f(\mathsf{u},\mathsf{pk_S}) = \begin{cases} \perp & \text{if } \mathcal{R}((\mathsf{u},\mathsf{pk_S}),(\mathsf{u}^*,\mathsf{pk_{S^*}})) = \mathsf{True} \\ \mathcal{US}(\mathsf{u},\mathsf{sk_{R^*}},\mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

Definition 22. *A signcryption scheme* SC *is* IND-qgCCA *secure in multi-user outsider model* (fM-IND-oqgCCA)*, if there exists an efficient unsigncryption-respecting relation* $\mathcal{R}$ *w.r.t. which it is* qCCA *secure.*

Definition 23. *A signcryption scheme* SC *is* sUF-qCMA *secure in multi-user outsider model* (fM-sUF-oqCMA) *if for any quantum PPT algorithm* $\mathcal{A}$*, the advantage*

$$\mathsf{Adv}^{\mathsf{fM\text{-}sUF\text{-}oqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda) := \Pr[\mathsf{m}_i \neq \perp \forall i \in [q+1]]$$

in $\mathsf{Exp}^{\mathsf{fM\text{-}sUF\text{-}oqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 9 is a negligible function in* λ*, where* $\mathcal{A}$ *is provided superposition access to signcryption oracle* $\mathcal{O}^{\mathsf{q}}_{S}$ *and unsigncryption oracle* $\mathcal{O}^{\mathsf{q}}_{U}$ *(described below),* q *is the number of signcryption oracle queries with the requirement that* $q+1$ *forgeries are pairwise distinct.*

- Quantum Signcryption oracle *($\mathcal{O}^{\mathsf{q}}_{S}$): For each query, the oracle chooses randomness* r*, and responds by signcrypting each message in the query using* r *as randomness:*

$$\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} |\mathsf{m},\mathsf{pk_R},\mathsf{u_p}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} |\mathsf{m},\mathsf{pk_R},\mathsf{u_p} \oplus \mathcal{SC}(\mathsf{m},\mathsf{sk_{S^*}},\mathsf{pk_R};r)\rangle .$$

- Quantum Unsigncryption oracle *($\mathcal{O}^{\mathsf{q}}_{U}$): For each query, the oracle responds by applying the following transformation:*

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p} \oplus \mathcal{US}(\mathsf{u},\mathsf{sk_{R^*}},\mathsf{pk_S})\rangle .$$

$\underline{\mathsf{Exp}^{\mathsf{fM\text{-}sUF\text{-}oqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)}$:

- $\mathcal{PP} \longleftarrow \mathsf{Setup}(1^\lambda)$
- $(\mathsf{pk_{S^*}},\mathsf{sk_{S^*}}) \longleftarrow \mathsf{KeyGen_S}(\mathcal{PP})$
- $(\mathsf{pk_{R^*}},\mathsf{sk_{R^*}}) \longleftarrow \mathsf{KeyGen_R}(\mathcal{PP})$
- $\{\mathsf{u}_i : i \in [q+1]\} \longleftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{q}}_{U},\mathcal{O}^{\mathsf{q}}_{S}}(\mathcal{PP},\mathsf{pk_{S^*}},\mathsf{pk_{R^*}})$
- $\mathsf{m}_i \longleftarrow \mathcal{US}(\mathsf{u}_i,\mathsf{sk_{R^*}},\mathsf{pk_{S^*}}), \forall i \in [q+1]$

Figure 9: Experiment for unforgeability (multi-user outsider model)

Definition 24. *A signcryption scheme* SC *is* wUF-qCMA *secure in multi-user outsider model* (fM-wUF-oqCMA) *if it satisfies the same definition as* fM-sUF-oqCMA*, except the requirement that the* $q+1$ *signcryption texts should unsigncrypt to distinct messages.*

We also consider a weaker variant of the definitions for quantum security in the outsider model where quantum access is provided only to the unsigncryption oracle and the challenge queries and signcryption oracle queries are classical. Intuitively, such definitions capture the situation where the sender party runs the protocol on a classical device and the receiver party may run the protocol on a quantum device. We call these definitions as $\mathsf{fM\text{-}IND\text{-}ouqCCA}$, $\mathsf{fM\text{-}IND\text{-}ouqgCCA}$ in the confidentiality case and $\mathsf{fM\text{-}sUF\text{-}ouqCMA}$, $\mathsf{fM\text{-}wUF\text{-}ouqCMA}$ in the authenticity case. Similarly, for the two-user model we call these definitions as $\mathsf{IND\text{-}ouqCCA}$, $\mathsf{IND\text{-}ouqgCCA}$ in the confidentiality case and $\mathsf{sUF\text{-}ouqCMA}$, $\mathsf{wUF\text{-}ouqCMA}$ in the authenticity case. Note that in the authenticity case, the adversary is only required to produce a single forgery instead of $q+1$ forgeries.

4 Constructions

Here, we describe various paradigms of constructing signcryption schemes that are based on generic composition of encryption, signature and commitment schemes. In particular, we discuss the encrypt-then-sign ($\mathcal{E}t\mathcal{S}$) and sign-then-encrypt ($\mathcal{S}t\mathcal{E}$) paradigms [ADR02] which are based on sequential generic composition of encryption and signature. We also discuss the commit-then-encrypt-and-sign ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$) [ADR02] which is a parallel composition of encryption and signature.

Encrypt-then-sign. The encrypt-then-sign ($\mathcal{E}t\mathcal{S}$) paradigm is based on the sequential generic composition of encryption and signature. Let $\mathsf{PKE} := (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ and $\mathsf{PKS} := (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ be the primitive encryption scheme and signature scheme respectively. The receiver and sender's public key and private key are obtained by running $(\mathsf{pk_R}, \mathsf{sk_R}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$, $(\mathsf{pk_S}, \mathsf{sk_S}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ respectively. To signcrypt a message m, sender runs $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{m}||\mathsf{pk_S}, \mathsf{pk_R})$, then it executes $\sigma \longleftarrow \mathcal{S}(\mathsf{c}||\mathsf{pk_R}, \mathsf{sk_S})$ and returns $\mathsf{u} := (\mathsf{c}, \sigma)$. To unsigncrypt a signcryption text u, receiver runs $\mathsf{flag} \longleftarrow \mathcal{V}(\mathsf{c}||\mathsf{pk_R}, \sigma, \mathsf{pk_S})$. If $\mathsf{flag} = \mathsf{True}$, it runs $\mathsf{m}||\mathsf{pk_{S'}} \longleftarrow \mathcal{D}(\mathsf{c}, \mathsf{sk_R})$ and returns m if $\mathsf{pk_{S'}} = \mathsf{pk_S}$. In all other cases, it returns $\perp$.

Sign-then-encrypt. The sign-then-encrypt ($\mathcal{S}t\mathcal{E}$) paradigm is based on the sequential generic composition of signature and encryption. Let $\mathsf{PKE} := (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ and $\mathsf{PKS} := (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ be the primitive encryption scheme and signature scheme respectively. The receiver and sender's public key and private key are obtained by running $(\mathsf{pk_R}, \mathsf{sk_R}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$, $(\mathsf{pk_S}, \mathsf{sk_S}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ respectively. To signcrypt a message m, sender runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}||\mathsf{pk_R}, \mathsf{sk_S})$, then it executes $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{m}||\sigma||\mathsf{pk_S}, \mathsf{pk_R})$ and returns $\mathsf{u} := \mathsf{c}$. To unsigncrypt a signcryption text u, receiver runs $\mathsf{m}||\sigma||\mathsf{pk_{S'}} \longleftarrow \mathcal{D}(\mathsf{u}, \mathsf{sk_R})$. If $\mathsf{pk_{S'}} = \mathsf{pk_S}$, it runs $\mathsf{flag} \longleftarrow \mathcal{V}(\mathsf{m}||\mathsf{pk_R}, \sigma, \mathsf{pk_S})$. If $\mathsf{flag} = \mathsf{True}$, it returns m. In all other cases it returns $\perp$.

Commit-then-encrypt-and-sign. The commit-then-encrypt-and-sign ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$) paradigm is based on the parallel composition of encryption and signature. Let $\mathsf{PKE} := (\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$, $\mathsf{PKS} := (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ and $\mathsf{C} := (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ be the primitive encryption scheme, signature scheme and commitment schemes respectively. The public parameters of signcryption scheme are set as $\mathcal{PP} := \mathcal{CK}$, where $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$. The receiver and sender's public key and private key are obtained by running $(\mathsf{pk_R}, \mathsf{sk_R}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$, $(\mathsf{pk_S}, \mathsf{sk_S}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ respectively. To signcrypt a message m, sender runs $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$, then it executes in parallel $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk_R}, \mathsf{sk_S})$ and $\mathsf{c} := \mathcal{E}(\mathsf{decom}||\mathsf{pk_S}, \mathsf{pk_R})$. It returns the signcryption $\mathsf{u} := (\mathsf{com}, \sigma, \mathsf{c})$. To unsigncrypt a signcryption text u, receiver runs $\mathsf{flag} \longleftarrow \mathcal{V}(\mathsf{com}||\mathsf{pk_R}, \sigma, \mathsf{pk_S})$ and $\mathsf{decom}||\mathsf{pk_{S'}} \longleftarrow \mathcal{D}(\mathsf{c}, \mathsf{sk_R})$ in parallel. If $\mathsf{flag} = \mathsf{True}$ and $\mathsf{pk_{S'}} = \mathsf{pk_S}$, it returns $\mathsf{Open}(\mathsf{com}, \mathsf{decom})$ else it returns $\perp$.

5 Insider Model

In this section, we analyze the quantum security of signcryption constructions based on $\mathcal{E}t\mathcal{S}$, $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms in the multi-user insider model where the adversary is allowed to corrupt one of the two participants. The two-user model, being a special case of multi-user model, need not be treated separately as the same results hold. The security proofs, though closely follow their classical counterparts, involve several subtle issues while simulating quantum queries. In particular, the power of adversary to arbitrarily initialize the output register coupled with the property of no-cloning, unique to quantum computing, makes the proofs non-trivial.

We use the following technical tool in the subsequent proofs. Let A_Q be a quantum algorithm performing quantum queries to an oracle O, and let $q_r(|\phi_t\rangle)$ be the magnitude squared of r in the superposition of t^{th} query $|\phi_t\rangle$. We call this the query probability of r in t^{th} query. If we sum over all t, we get the total query probability of r.

Lemma 5.1 ([BBBV97] Theorem 3.3)**.** *Let A_Q be a quantum algorithm running in time T with oracle access to O. Let $\epsilon > 0$ and let $S \subseteq [1,T] \times \{0,1\}^n$ be a set of time-string pairs such that $\sum_{(t,r)\in S} q_r(|\phi_t\rangle) \leq \epsilon$. If we modify O into an oracle O' which answers each query r at time t by providing the same string R (which has been independently sampled at random), then the Euclidean distance between the final states of A_Q when invoking O and O' is at most $\sqrt{T\epsilon}$.*

5.1 Encrypt-then-Sign

Classically, it has been shown that IND-CCA security for signcryption in the $\mathcal{E}t\mathcal{S}$ paradigm cannot be achieved against insider adversaries [ADR02]. However, $\mathcal{E}t\mathcal{S}$ paradigm preserves the IND-gCCA security and sUF-CMA security of the base encryption and signature schemes in the insider model. Here, we analyze the quantum analogues of these results. We start with the quantum security of confidentiality in the $\mathcal{E}t\mathcal{S}$ paradigm based construction in the multi-user insider model. The proof strategy is an amalgamation of its classical counterpart [ADR02] and our techniques.

Theorem 5.1. *If the primitive encryption scheme* PKE *is* IND-qgCCA *secure, then the signcryption scheme* SC *in the $\mathcal{E}t\mathcal{S}$ paradigm is* IND-qgCCA *secure in dynamic multi user insider-security model* (dM-IND-iqgCCA (*c.f., Definition 16*))*.*

Proof. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is IND-qgCCA secure. Let $\mathsf{pk}_{\mathsf{R}^*}$ represent the identity of receiver in the challenge. We define the equivalence relation $\mathcal{R}'$ for the induced encryption for SC to be

$$\mathcal{R}'((\mathsf{u}_1, \mathsf{pk}_{\mathsf{S}1}), (\mathsf{u}_2, \mathsf{pk}_{\mathsf{S}2})) = \mathsf{True}$$

$$\Updownarrow$$

$$\mathcal{R}(\mathsf{c}_1, \mathsf{c}_2) = \mathsf{True} \wedge (\mathcal{V}(\mathsf{c}_1 \| \mathsf{pk}_{\mathsf{R}^*}, \sigma_1, \mathsf{pk}_{\mathsf{S}1}) = 1 \wedge \mathcal{V}(\mathsf{c}_2 \| \mathsf{pk}_{\mathsf{R}^*}, \sigma_2, \mathsf{pk}_{\mathsf{S}2}) = 1) \wedge (\mathsf{pk}_{\mathsf{S}1} = \mathsf{pk}_{\mathsf{S}2}).$$

It can be checked that $\mathcal{R}'$ is an unsigncryption-respecting relation over the signcryption texts.

Let $\mathcal{A}$ be a quantum PPT adversary which has advantage ϵ in breaking dM-IND-iqgCCA security of SC. We construct a quantum PPT algorithm $\mathcal{B}$ which breaks the IND-qgCCA security of PKE with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{B}$. $\mathcal{B}$ forwards $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and submits two equal length messages m_0 and m_1 along with $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ to $\mathcal{B}$. $\mathcal{B}$ submits the message pair $(\mathsf{m}_0 \| \mathsf{pk}_{\mathsf{S}^*}, \mathsf{m}_1 \| \mathsf{pk}_{\mathsf{S}^*})$ to the challenger $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b \| \mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and sends c^* to $\mathcal{B}$. $\mathcal{B}$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^* \| \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, sets $\mathsf{u}^* := (\mathsf{c}^*, \sigma^*)$ and returns it to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}\rangle$ be any unsigncryption query made by $\mathcal{A}$. Note that, the query $\mathsf{u}_{\mathsf{quant}}$ consists of three registers $\mathsf{U} = (\mathsf{C}, \mathsf{S}), \mathsf{PK}_{\mathsf{S}}$ and M. These resisters represent respectively the actual unsigncryption query, the sender public key and the message. The latter is where the message is recorded by the simulator $\mathcal{B}$ after unsigncryption. $\mathcal{B}$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of the 1^{st} register C and the ancilla register to $\mathcal{CH}$. $\mathcal{CH}$ applies the decryption operator on the received quantum state which results in the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}, 0^{\ell_m} \oplus g(\mathsf{c})\rangle$$

where

$$g(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}, g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\Delta), g(\mathsf{c})\rangle$$

where

$$f(\Delta) = \begin{cases} [g(\mathsf{c})]_1 & \text{if } (\mathcal{V}(\mathsf{c} \| \mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_{\mathsf{S}}) = 1 \wedge \mathsf{pk}_{\mathsf{S}} = [g(\mathsf{c})]_2) \\ \perp & \text{otherwise,} \end{cases}$$

for $\Delta = (\mathsf{u}, g(\mathsf{c}), \mathsf{pk}_{\mathsf{S}})$.

Note that in this process the ancilla register may get entangled with the other registers. To perfectly simulate $\mathcal{A}$'s view, $\mathcal{B}$ uses the *EtU* technique to unentangle the ancilla register: $\mathcal{B}$ again sends a decryption query consisting of 1^{st} register C and the ancilla register to $\mathcal{CH}$. $\mathcal{CH}$ applies the decryption operator on the received quantum state which results in the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\Delta), g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\Delta), g(\mathsf{c}) \oplus g(\mathsf{c})\rangle$$

Finally, $\mathcal{B}$ obtains the state $\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends the state $\sum_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} \psi_{\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}} |\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. $\mathcal{B}$ returns the same bit b' to $\mathcal{CH}$.

Analysis: We show that $\mathcal{B}$ simulates $\mathcal{A}$'s unsigncryption queries properly. It suffices to show that each of the basis element $|\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}\rangle$ is handled properly. The definition of $\mathcal{R}'$ states that a query $|\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}\rangle$ is legitimate if one of the following conditions is false:

1. $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$
2. $\mathcal{V}(\mathsf{c}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk_S}) = \mathsf{True}$
3. $\mathsf{pk_S} = \mathsf{pk}_{\mathsf{S}^*}$

If condition 1 is false then $\mathcal{B}$ answers by making decryption query to $\mathcal{CH}$. If condition 1 is true and condition 2 or 3 is false then by the nature of construction $(\mathsf{u}, \mathsf{pk_S})$ is an invalid query. Hence, $\mathcal{B}$ should return $\perp$ for any query u which satisfies $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$. This is exactly how unsigncryption queries are handled in the simulation of $\mathcal{A}$. Hence, $\mathcal{B}$ simulates $\mathcal{A}$'s queries perfectly and breaks the IND-qgCCA security of PKE with advantage at least ϵ. □

In Theorem 5.2, we state the quantum security of unforgeability of signcryption in $\mathcal{E}t\mathcal{S}$ paradigm. To prove Theorem 5.2, we adopt the techniques similar to that used in the proof of Theorem 5.1.

Theorem 5.2. *If the primitive signature scheme* PKS *is* sUF-qCMA (*resp.* wUF-qCMA) *secure, then the signcryption scheme* SC *in the $\mathcal{E}t\mathcal{S}$ paradigm is* sUF-qCMA (*resp.* wUF-qCMA) *secure in dynamic multi user insider-security model* (dM-sUF-iqCMA (*resp.* dM-wUF-iqCMA) (*c.f., Definitions 19, 20*)).

Proof. Let $\mathcal{A}$ be a quantum PPT adversary that can break dM-sUF-iqCMA (resp. dM-wUF-iqCMA) security of the signcryption scheme SC with probability ϵ. Let q be the number of signcryption oracle queries allowed to $\mathcal{A}$. We construct a quantum PPT algorithm $\mathcal{B}$ which makes q signature oracle queries and breaks the sUF-qCMA (resp. wUF-qCMA) security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{B}$. $\mathcal{B}$ forwards $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: Let $\mathsf{m_{quant}} = \sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}\rangle$ be any signcryption query made by $\mathcal{A}$. Note that, the query $\mathsf{m_{quant}}$ consists of three registers $\mathsf{M}, \mathsf{PK_R}$ and $\mathsf{U} = (\mathsf{C}, \mathsf{S})$. These resisters represent respectively the message query, receiver public key and the actual signcryption text. The latter is where the signcryption text is recorded after signcryption. $\mathcal{B}$ appends an ℓ_c qubit ancilla register, containing the state $|0^{\ell_c}\rangle$, to the query and obtains the state $\sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_\mathsf{p}, 0^{\ell_c}\rangle$. $\mathcal{B}$ chooses a randomness r_enc and applies the encryption operator which results in the following unitary transformation

$$\sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_\mathsf{p}, 0^{\ell_c}\rangle \longmapsto \sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_\mathsf{p}, 0^{\ell_c} \oplus \mathcal{E}(\mathsf{m}||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk_R}; r_\mathsf{enc})\rangle .$$

$\mathcal{B}$ sends a signature query on $2^{nd}, 4^{th}$ and 5^{th} registers ($\mathsf{PK_R}, \mathsf{S}$ and the ancilla register) to $\mathcal{CH}$. Here the ancilla register and $\mathsf{PK_R}$ constitute the message register for the signature algorithm and S stores the signature. $\mathcal{CH}$ applies the signature operator on the received quantum state which results in the following unitary transformation (here $\mathsf{c} = \mathcal{E}(\mathsf{m}||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk_R}; r_\mathsf{enc})$)

$$\sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_\mathsf{p}, \mathsf{c}\rangle \longmapsto \sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_\mathsf{p} \oplus \mathcal{S}(\mathsf{c}||\mathsf{pk_R}, \mathsf{sk}_{\mathsf{S}^*}), \mathsf{c}\rangle .$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state (here $\sigma = \mathcal{S}(\mathsf{c}||\mathsf{pk_R}, \mathsf{sk_{S^*}})$)

$$\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p}, \sigma_{\mathsf{p}} \oplus \sigma, \mathsf{c}\right\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{pk_R}, \mathsf{c_p} \oplus \mathsf{c}, \sigma_{\mathsf{p}} \oplus \sigma, \mathsf{c}\right\rangle .$$

The resulting state can be equivalently written as

$$\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p} \oplus \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R}), \mathsf{c}\right\rangle .$$

Note that $\mathcal{B}$ can unentangle the last register by applying encryption operator on 1^{st} and 4^{th} register using the same randomness r_{enc} to obtain the state $\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p} \oplus \mathsf{u}\right\rangle \otimes \left|0^{\ell_c}\right\rangle$, where $\mathsf{u} = \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R})$. It discards the last register and sends $\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \left|\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p} \oplus \mathsf{u}\right\rangle$ to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs $q+1$ forgeries $\{(\mathsf{u}_i, \mathsf{pk_R}_i, \mathsf{sk_R}_i) : i \in [q+1]\}$. $\mathcal{B}$ forwards $(\mathsf{c}_1||\mathsf{pk_R}_1, \sigma_1), \ldots, (\mathsf{c}_{q+1}||\mathsf{pk_R}_{q+1}, \sigma_{q+1})$ as forgeries to $\mathcal{CH}$.

Analysis: It is clear that $\mathcal{B}$ breaks sUF-qCMA (resp. wUF-qCMA) security of PKS with probability at least ϵ. □

5.2 Sign-then-Encrypt

Classically, it has been shown that sUF-CMA security for signcryption in the $\mathcal{StE}$ paradigm cannot be achieved against insider adversaries [ADR02]. However, $\mathcal{StE}$ paradigm preserves the IND-CCA security and wUF-CMA security of the base encryption and signature schemes in the insider model. Here, we analyze the quantum analogues of these results. We first analyze quantum security of confidentiality of signcryption in $\mathcal{StE}$ paradigm. To prove Theorem 5.3, we adopt the techniques similar to that used in the proof of Theorem 5.1.

Theorem 5.3. *If the primitive encryption scheme* PKE *is* IND-qCCA (*resp.* IND-qgCCA) *secure, then the signcryption scheme* SC *in the $\mathcal{StE}$ paradigm is* IND-qCCA (*resp.* IND-qgCCA) *secure in the dynamic multi user insider-security model* (dM-IND-iqCCA (*resp.* dM-IND-iqgCCA) (*c.f., Definitions 15, 16*)).

Proof. Here, we only detail the security reduction in the dM-IND-iqgCCA security model of SC because the proof in the dM-IND-iqCCA security model follows as a special case of dM-IND-iqgCCA security. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is IND-qgCCA secure. We define the equivalence relation $\mathcal{R}'$ for the induced encryption for SC to be

$$\mathcal{R}'((\mathsf{u}_1, \mathsf{pk_S}_1), (\mathsf{u}_2, \mathsf{pk_S}_2)) = \mathsf{True} \Leftrightarrow \mathcal{R}(\mathsf{c}_1, \mathsf{c}_2) = \mathsf{True} \wedge (\mathsf{pk_S}_1 = \mathsf{pk_S}_2).$$

It can be checked that $\mathcal{R}'$ is an unsigncryption-respecting relation over the signcryption texts.

Let $\mathcal{A}$ be a quantum PPT adversary which has advantage ϵ in breaking dM-IND-iqgCCA security of SC. We construct a quantum PPT algorithm $\mathcal{B}$ which breaks the IND-qgCCA security of PKE with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}$. $\mathcal{B}$ forwards $\mathsf{pk_{R^*}}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and submits two equal length messages m_0 and m_1 along with $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ to $\mathcal{B}$. $\mathcal{B}$ runs $\sigma_0 \longleftarrow \mathcal{S}(\mathsf{m}_0 \| \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, $\sigma_1 \longleftarrow \mathcal{S}(\mathsf{m}_1 \| \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and submits $(\mathsf{m}_0 \| \sigma_0 \| \mathsf{pk}_{\mathsf{S}^*}, \mathsf{m}_1 \| \sigma_1 \| \mathsf{pk}_{\mathsf{S}^*})$ to $\mathcal{CH}$. $\mathcal{CH}$ picks $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b \| \sigma_b \| \mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and sends c^* to $\mathcal{B}$. $\mathcal{B}$ sets $\mathsf{u}^* := \mathsf{c}^*$ and returns it to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. Note that, the query $\mathsf{u}_{\mathsf{quant}}$ consists of three registers $\mathsf{U} = (\mathsf{C}), \mathsf{PK}_\mathsf{S}$ and M. These resisters represent respectively the actual unsigncryption query, the sender public key and the message. The latter is where the message is recorded after unsigncryption. $\mathcal{B}$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of 1^{st} and 4^{th} register (U and ancilla register) to $\mathcal{CH}$. $\mathcal{CH}$ applies the decryption operator on the received quantum state which results in the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m} \oplus g(\mathsf{u})\rangle$$

where

$$g(\mathsf{u}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{u}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, g(\mathsf{u})\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta), g(\mathsf{u})\rangle$$

where

$$f(\Delta) = \begin{cases} [g(\mathsf{u})]_1 & \text{if } \mathcal{V}([g(\mathsf{u})]_1 \| \mathsf{pk}_{\mathsf{R}^*}, [g(\mathsf{u})]_2, \mathsf{pk}_\mathsf{S}) = 1 \wedge \mathsf{pk}_\mathsf{S} = [g(\mathsf{u})]_3 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (g(\mathsf{u}), \mathsf{pk}_\mathsf{S})$.

Note that the ancilla register is entangled with the first three registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}$ again sends a decryption query consisting of 1^{st} and 4^{th} register to $\mathcal{CH}$ to unentangle the ancilla register. Finally, $\mathcal{B}$ obtains the state $\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends $\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. $\mathcal{B}$ returns the same bit b' to $\mathcal{CH}$.

Analysis: It is easy to see that $\mathcal{B}$ simulates $\mathcal{A}$'s queries perfectly and it breaks the IND-qgCCA security of PKE with advantage at least ϵ. □

Next, we argue quantum security of unforgeability of signcryption in $\mathcal{S}t\mathcal{E}$ paradigm (Theorem 5.4). Recall that in the dM-wUF-iqCMA security model, the adversary is provided superposition access to the signcryption oracle. A quantum signcryption query consists of three registers, viz., message register (M), receiver public key register ($\mathsf{PK_R}$) and signcryption text register (U) where the latter will record the signcryption of the message contained in register M. We first discuss an issue that arises in the security analysis. If the adversary is allowed to initialize U with arbitrary state during simulation, then the simulator cannot unentangle the ancilla register once it is entangled because of the following reasons. As discussed in Section 1, the *EtU* technique is applicable in cases where all the secret information, viz., secret keys and randomness are known to the simulator or the output of oracle on a given input is deterministic. The first case is not applicable as the simulator does not possess the secret information. Since the signature algorithm may not be deterministic, the second case is not applicable as well. Even if the signature algorithm is deterministic, to answer one signcryption oracle query the simulator will have to make 2 signature oracle queries. For simulating q signcryption oracle queries the simulator shall make $2q$ signature oracle queries, thus rendering the simulation useless.

To bypass above problems, we restrict the adversary to initialize U in the state $\left|0^{\ell_u}\right\rangle$. Assuming that the adversary may not be honest, the above condition can be enforced by requiring the adversary to send a classical description of the quantum query [GHS16]. Further, we use a $\mathsf{Type\text{-}2}$ unitary operator [5] for encryption to avoid querying twice to the signature oracle in answering one signcryption query. The requirement we imposed is achieved in the following way. The adversary outputs a state $\left|0^{\ell_m+\ell_u}\right\rangle$ and a unitary operator $U = U_m \otimes I_u$ such that the joint action of U_m and I_u on the state $\left|0^{\ell_m+\ell_u}\right\rangle$ gives $\mathsf{m_{quant}} \otimes \left|0^{\ell_u}\right\rangle$, where $\mathsf{m_{quant}} = \sum\limits_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R}\right\rangle$. Security analysis in case of arbitrary manipulation of the signcryption text register seems to be difficult and is an interesting problem to pursue.

Theorem 5.4. *If the primitive signature scheme* PKS *is* $\mathsf{wUF\text{-}qCMA}$ *secure, then the signcryption scheme* SC *in the* $\mathcal{S}t\mathcal{E}$ *paradigm is* $\mathsf{wUF\text{-}qCMA}$ *secure in dynamic multi user insider-security model* ($\mathsf{dM\text{-}wUF\text{-}iqCMA}$ (*c.f., Definition 20*)).

Proof. Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{dM\text{-}wUF\text{-}iqCMA}$ security of the signcryption scheme SC with probability ϵ. Let q be the number of signcryption oracle queries allowed to $\mathcal{A}$. We construct a quantum PPT algorithm $\mathcal{B}$ which makes q signature oracle queries and breaks the $\mathsf{wUF\text{-}qCMA}$ security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and sends $\mathsf{pk_{S^*}}$ to $\mathcal{B}$. $\mathcal{B}$ forwards $\mathsf{pk_{S^*}}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: $\mathcal{A}$ outputs a classical description of a quantum message $\mathsf{m_{quant}} \otimes \left|0^{\ell_u}\right\rangle$ by sending a (classical) bitstring describing a quantum circuit U which takes no input but starts from a fixed initial state $\left|0^{\ell_m+\ell_u}\right\rangle$ and outputs $\mathsf{m_{quant}} \otimes \left|0^{\ell_u}\right\rangle$. The second register will store the signcryption text.

Let $\mathsf{m_{quant}} \otimes \left|0^{\ell_u}\right\rangle = \sum\limits_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R},0^{\ell_m},0^{\ell_s},0^{\ell_{ps}},0^{\ell_{pr}},0^{\ell_{r_{\mathsf{enc}}}}\right\rangle$, where $\ell_u = \ell_m + \ell_s + \ell_{ps} + \ell_{pr} + \ell_{r_{\mathsf{enc}}}$, and ℓ_m, ℓ_s, ℓ_{ps}, ℓ_{pr} and $\ell_{r_{\mathsf{enc}}}$ denote the lengths of plaintext, signature, $\mathsf{pk_{S^*}}$, $\mathsf{pk_R}$ and randomness of encryption algorithm respectively. $\mathcal{B}$ sends a signature query consisting of $1^{st}, 2^{nd}$ and 4^{th} register ($\mathsf{M}, \mathsf{PK_R}$ and the first sub-component of ancilla register representing the value 0^{ℓ_s}) to $\mathcal{CH}$. Here M and $\mathsf{PK_R}$ together constitute the message register for the signature challenger $\mathcal{CH}$ and the ancilla register stores the signature corresponding to PKS. $\mathcal{CH}$ applies the signature operator on the received quantum state resulting in the following unitary

[5] For bijective functions like encryption, one can consider transformations of the form:

$$|x, y\rangle \longmapsto |\phi_{x,y}\rangle,$$

where the length of the ancilla register (stores the additional qubits apart from the input) is $|y| = |\mathcal{E}(x)| - |x|$ and $\phi_{x,0} = \mathcal{E}(x)$ for every x, i.e., initializing the ancilla register in the $|0\rangle$ state produces correct evaluation of $\mathcal{E}$.

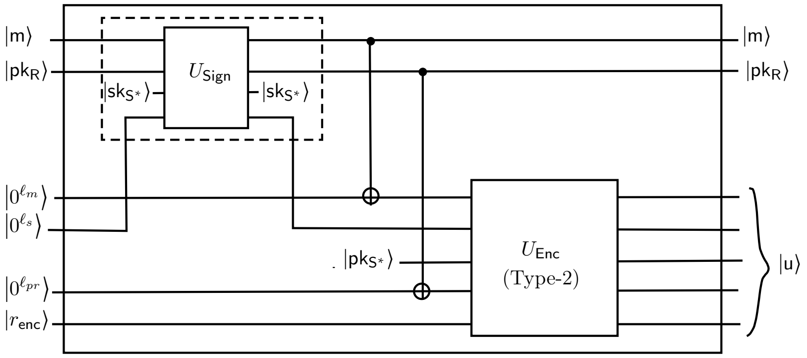

Figure 10: Quantum circuit implementing unitary U_{SC}, where the simulator makes signature queries to its external oracle (shown by dashed line) which is handled by the challenger of the underlying signature scheme and then it encrypts the message-signature.

transformation

$$\sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R},0^{\ell_m},0^{\ell_s},0^{\ell_{ps}},0^{\ell_{pr}},0^{\ell_{r_{\mathsf{enc}}}}\right\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R},0^{\ell_m},0^{\ell_s}\oplus\mathcal{S}(\mathsf{m}\|\mathsf{pk_R},\mathsf{sk_{S^*}}),0^{\ell_{ps}},0^{\ell_{pr}},0^{\ell_{r_{\mathsf{enc}}}}\right\rangle.$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}$. $\mathcal{B}$ applies the following transformation (here $\sigma = \mathcal{S}(\mathsf{m}\|\mathsf{pk_R},\mathsf{sk_{S^*}})$)

$$\sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R},0^{\ell_m},\sigma,0^{\ell_{ps}},0^{\ell_{pr}},0^{\ell_{r_{\mathsf{enc}}}}\right\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} \left|\mathsf{m},\mathsf{pk_R},0^{\ell_m}\oplus\mathsf{m},\sigma,0^{\ell_{ps}},0^{\ell_{pr}}\oplus\mathsf{pk_R},0^{\ell_{r_{\mathsf{enc}}}}\right\rangle.$$

$\mathcal{B}$ adds the states $|\mathsf{pk_{S^*}}\rangle$ and $|r_{\mathsf{enc}}\rangle$ to the resultant state and applies the Type-2 unitary operator for encryption [GHS16] on the $3^{rd}, 4^{th}, 5^{th}$, 6^{th} and 7^{th} registers of the obtained state.

$$\sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} |\mathsf{m},\mathsf{pk_R},\mathsf{m},\sigma,\mathsf{pk_{S^*}},\mathsf{pk_R},r_{\mathsf{enc}}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} |\mathsf{m},\mathsf{pk_R},\mathcal{E}(\mathsf{m}\|\sigma\|\mathsf{pk_{S^*}},\mathsf{pk_R};r_{\mathsf{enc}})\rangle.$$

The resulting state can be equivalently written as $\sum_{\mathsf{m},\mathsf{pk_R}} \psi_{\mathsf{m},\mathsf{pk_R}} |\mathsf{m},\mathsf{pk_R},\mathsf{u}\rangle$, where $\mathsf{u} = \mathcal{SC}(\mathsf{m},\mathsf{sk_{S^*}},\mathsf{pk_R})$. $\mathcal{B}$ forwards the obtained state to $\mathcal{A}$. For better understanding, a quantum circuit for $U_{\mathcal{SC}}$ is shown in Figure 10.

Forgeries: $\mathcal{A}$ outputs $q+1$ forgeries $\{(\mathsf{u}_i,\mathsf{pk_R}_i,\mathsf{sk_R}_i) : i \in [q+1]\}$.

$\mathcal{B}$ forwards the set $\{([(\mathcal{D}(\mathsf{u}_i,\mathsf{sk_R}_i)]_1\|\mathsf{pk_R}_i,[\mathcal{D}(\mathsf{u}_i,\mathsf{sk_R}_i)]_2) : i \in [q+1]\}$ as forgeries to $\mathcal{CH}$.

Analysis: It is clear that $\mathcal{B}$ breaks wUF-qCMA security of PKS with probability at least ϵ. □

5.3 Commit-then-Encrypt-and-Sign

Classically, it has been shown that IND-CCA and sUF-CMA security for signcryption in the $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm cannot be achieved against insider adversaries [ADR02]. However, $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm preserves the IND-gCCA security and wUF-CMA security of the base encryption and signature schemes in the insider model provided that the commitment scheme satisfies the notions of hiding, binding and rconcealment. Here, we analyze the quantum analogues of these results.

In Theorem 5.5, we argue the quantum security of confidentiality of $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm through a hybrid argument as given in [NP16]. The proofs mainly follow techniques that are already elaborated in the context of previous proofs. We only give a proof sketch here and the lemmas involved in the same are deferred to Appendices A.1, A.2 and A.3.

Theorem 5.5. *If the primitive encryption scheme* PKE *is* $\mathsf{IND\text{-}qgCCA}$ *secure and the commitment scheme* C *satisfies* $\mathsf{qHiding}$ *and* $\mathsf{qrConcealment}$ *properties, then the signcryption scheme* SC *in the* $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ *paradigm is* $\mathsf{IND\text{-}qgCCA}$ *secure in the dynamic multi user insider-security model* ($\mathsf{dM\text{-}IND\text{-}iqgCCA}$ (*c.f., Definition 16*)).

Proof Sketch. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is $\mathsf{IND\text{-}qgCCA}$ secure. Let $\mathsf{pk}_{\mathsf{R}^*}$ represent the identity of receiver in the challenge. We define the equivalence relation $\mathcal{R}'$ for the induced encryption for SC to be $\mathcal{R}'((\mathsf{u}_1,\mathsf{pk}_{\mathsf{S}_1}),(\mathsf{u}_2,\mathsf{pk}_{\mathsf{S}_2})) = \mathsf{True}$ if and only if $\mathcal{R}(\mathsf{c}_1,\mathsf{c}_2) = \mathsf{True}$, $(\mathsf{com}_1 = \mathsf{com}_2)$, $(\mathcal{V}(\mathsf{com}_1\|\mathsf{pk}_{\mathsf{R}^*},\sigma_1,\mathsf{pk}_{\mathsf{S}_1}) = 1 \wedge \mathcal{V}(\mathsf{com}_2\|\mathsf{pk}_{\mathsf{R}^*},\sigma_2,\mathsf{pk}_{\mathsf{S}_2}) = 1)$ and $(\mathsf{pk}_{\mathsf{S}_1} = \mathsf{pk}_{\mathsf{S}_2})$. It can be checked that $\mathcal{R}'$ is an unsigncryption-respecting relation over the signcryption texts. Let $(\mathsf{u}^* = (\mathsf{com}^*,\sigma^*,\mathsf{c}^*),\mathsf{pk}_{\mathsf{S}^*})$ denote a challenge signcryption text. Let $(\mathsf{u} = (\mathsf{com},\sigma,\mathsf{c}),\mathsf{pk}_{\mathsf{S}})$ be any signcryption text. We define an event

$$\mathsf{E} \coloneqq [(\mathsf{com}^* \neq \mathsf{com}) \wedge \mathcal{R}(\mathsf{c}^*,\mathsf{c}) = \mathsf{True} \wedge \mathcal{US}(\mathsf{u},\mathsf{sk}_{\mathsf{R}^*},\mathsf{pk}_{\mathsf{S}}) \neq \perp].$$

For any signcryption text $(\mathsf{u},\mathsf{pk}_{\mathsf{S}})$, we say that $\mathsf{E}[\mathsf{u},\mathsf{pk}_{\mathsf{S}}] = \mathsf{True}$ if $(\mathsf{u},\mathsf{pk}_{\mathsf{S}})$ satisfies the event E. We prove security through a sequence of three games.

$\mathbf{Game_{Real}}$: The original $\mathsf{dM\text{-}IND\text{-}iqgCCA}$ game of signcryption.

$\mathbf{Game_0}$: Same as $\mathbf{Game_{Real}}$ except for the answers of unsigncryption queries after the challenge query. In particular, if a query $(\mathsf{u},\mathsf{pk}_{\mathsf{S}})$ satisfies the event E, then the challenger returns $\perp$ to the adversary.

$\mathbf{Game_1}$: Same as $\mathbf{Game_0}$ except for the construction of the challenge signcryption text, viz., $\mathsf{c}^* = \mathcal{E}(\mathsf{decom}_r\|\mathsf{pk}_{\mathsf{S}^*},\mathsf{pk}_{\mathsf{R}^*})$, where decom_r is randomly sampled from the decommitment space.

The proof follows from the following lemmas.

Lemma 5.2. $\mathbf{Game_{Real}}$ *and* $\mathbf{Game_0}$ *are indistinguishable under the* $\mathsf{qrConcealment}$ *property of the commitment scheme* C.

Lemma 5.3. $\mathbf{Game_0}$ *and* $\mathbf{Game_1}$ *are indistinguishable under the* $\mathsf{IND\text{-}qgCCA}$ *property of the primitive encryption scheme* PKE.

Lemma 5.4. *For any quantum PPT adversary* $\mathcal{A}$*, there is a quantum PPT algorithm* $\mathcal{B}$ *such that*

$$\mathsf{Adv}_{\mathcal{A},\mathsf{SC}}^{\mathbf{Game_1}}(1^\lambda) \leq \mathsf{Adv}_{\mathcal{B},\mathsf{C}}^{\mathsf{qHiding}}(1^\lambda).$$

In Theorem 5.6, we state the quantum security of unforgeability of $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm. The $\mathsf{qBinding}$ property of C says that given a signcryption text the adversary cannot change the ciphertext component to produce a signcryption corresponding to a different message. Hence, $\mathsf{wUF\text{-}qCMA}$ security is preserved. The proofs mainly follow techniques that are already elaborated in the context of previous lemmas. We only give a proof sketch here and for completeness the proofs of the lemmas involved in the same are provided in A.4 and A.5.

Theorem 5.6. *If the primitive signature scheme* PKS *is* $\mathsf{wUF\text{-}qCMA}$ *secure and the commitment scheme* C *satisfies* $\mathsf{qBinding}$ *property, then the signcryption scheme* SC *in the* $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ *paradigm is* $\mathsf{wUF\text{-}qCMA}$ *secure in the dynamic multi user insider-security model* ($\mathsf{dM\text{-}wUF\text{-}iqCMA}$ (*c.f., Definition 20*)).

Proof Sketch. Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{dM\text{-}wUF\text{-}iqCMA}$ security of the signcryption scheme SC with probability at least ϵ. Let q be the number of signcryption oracle queries allowed to $\mathcal{A}$ and $\{(\mathsf{u}_i = (\mathsf{com}_i, \sigma_i, \mathsf{c}_i), \mathsf{pk}_{\mathsf{R}_i}) : i \in [q+1]\}$ be the $q+1$ forgeries produced by $\mathcal{A}$. Let Forge denote the event that the tuples $(\mathsf{com}_1, \mathsf{pk}_{\mathsf{R}_1}), \dots, (\mathsf{com}_{q+1}, \mathsf{pk}_{\mathsf{R}_{q+1}})$ are pairwise distinct. Note that,

$$\epsilon \le \Pr[\mathcal{A} \text{ succeeds}] = \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}]$$

$$\implies \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] \ge \frac{\epsilon}{2} \text{ or } \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] \ge \frac{\epsilon}{2}.$$

The proof follows from the following lemmas which contradicts the above statement.

Lemma 5.5. *If* PKS *is* $\mathsf{wUF\text{-}qCMA}$ *secure, then* $\Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] < \frac{\epsilon}{2}$.

Lemma 5.6. *If* C *has* $\mathsf{qBinding}$ *property, then* $\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] < \frac{\epsilon}{2}$.

6 Outsider Model

In this section, we analyze the quantum security of constructions based on $\mathcal{E}t\mathcal{S}$, $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms in the outsider model. In contrast to the insider model, the classical results in the outsider model are stronger. For example, IND-CPA security of the encryption scheme is amplified to IND-CCA security in the $\mathcal{E}t\mathcal{S}$ paradigm if the signature scheme is sUF-CMA secure. Similar results hold in other two paradigms as well. The proof of these results assumes that the simulator can record adversary's signcryption queries in order to answer unsigncryption queries consistently. In fact such an assumption trivially holds in the classical setting.

The above results, however, do not naturally extend to the quantum setting, the main roadblock being the quantum no-cloning. In particular, the simulator cannot record adversary's prior signcryption queries and hence it becomes difficult to simulate unsigncryption queries which are responses of previous signcryption queries. In addition, there are technical issues in the existing definitions for unforgeability in the quantum setting [AMRS18, GYZ17], which create further hindrance in arguing full quantum security in the outsider model and in the symmetric setting of authenticated encryption as well. We also note that, the quantum security proof of authenticated encryption in the $\mathcal{E}t\mathcal{S}$ paradigm given in a recent paper [SJS16] has a logical gap. In particular, the simulation procedure records quantum queries which clearly violates no-cloning and the analysis that follows only holds in the classical setting.

These issues lead us to consider an intermediate setting, in which we analyze the quantum variant of classical results in the outsider model. The intermediate setting provides the adversary quantum access to unsigncryption oracle while signcryption oracle access remains classical. As mentioned earlier, the definition models the scenario where sender works on a classical machine while receiver may have access to a quantum machine. We leave full quantum security of generic authenticated encryption and signcryption constructions in the outsider model as an interesting open problem.

6.1 Two-User Setting

As a special case in the outsider model, the weak privacy (resp. unforgeability) of the encryption (resp. signature) scheme can be amplified to strong privacy (resp. unforgeability) under the strong security of signature (resp. encryption) in the two-user setting. Hence, we discuss them separately in Theorems 6.1 (for confidentiality) and 6.2 (for authenticity). We also note that, our results extend to the setting of authenticated encryption as well. To prove security in two-user setting, it is not necessary to append the sender and receiver identities while encrypting and signing in the constructions discussed in Section 4 and hence, we exclude them.

Theorem 6.1. *If the primitive encryption scheme* PKE *is* $\mathsf{pqIND\text{-}CPA}$ *secure and the signature scheme* PKS *is* $\mathsf{pqsUF\text{-}CMA}$ *(resp.* $\mathsf{pqwUF\text{-}CMA}$*) secure, then the signcryption scheme* SC *in the* $\mathcal{E}t\mathcal{S}$ *paradigm is* $\mathsf{IND\text{-}uqCCA}$ *(resp.* $\mathsf{IND\text{-}uqgCCA}$*) secure in the two user outsider-security model* ($\mathsf{IND\text{-}ouqCCA}$ *(resp.* $\mathsf{IND\text{-}ouqgCCA}$*) (c.f., Section 3.4)).*

Proof. Here, we only prove the $\mathsf{IND\text{-}uqgCCA}$ security of SC in the outsider model. The proof of $\mathsf{IND\text{-}uqCCA}$ follows similarly. Let $\mathsf{pk}_{\mathsf{S}^*}$ be the sender public key corresponding to the challenge. We define the equivalence relation $\mathcal{R}'$ for the induced encryption for SC to be $\mathcal{R}'(\mathsf{u}_1, \mathsf{u}_2) = \mathsf{True}$ if and only if $\mathsf{c}_1 = \mathsf{c}_2$ and $(\mathcal{V}(\mathsf{c}_1, \sigma_1, \mathsf{pk}_{\mathsf{S}^*}) = 1 \wedge \mathcal{V}(\mathsf{c}_2, \sigma_2, \mathsf{pk}_{\mathsf{S}^*}) = 1)$. It can be checked that $\mathcal{R}'$ is an unsigncryption-respecting relation over the signcryption texts.

Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{IND\text{-}uqgCCA}$ security of the signcryption scheme SC with probability at least ϵ. Let Forge denote the following event: $\exists$ an unsigncryption query made by $\mathcal{A}$ during its run, measuring query input of which yields with non-negligible probability, say μ, a tuple (c, σ) such that $\mathcal{V}(\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}^*}) = 1$ and c was not a result of any previous signcryption oracle or challenge query. In other words, if Forge happens then $\mathcal{A}$ breaks the $\mathsf{pqwUF\text{-}CMA}$ security of the underlying signature scheme PKS. Note that,

$$\begin{aligned}\epsilon \leq \Pr[\mathcal{A} \text{ succeeds}] - \frac{1}{2} &= \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \\ &\leq \Pr[\mathsf{Forge}] + \left(\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2}\right) \\ \Longrightarrow \Pr[\mathsf{Forge}] \geq \frac{\epsilon}{2} &\text{ or } \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}.\end{aligned}$$

Case 1: $\Pr[\mathsf{Forge}] \geq \frac{\epsilon}{2}$**.** Let q_u be the total number of unsigncryption queries allowed to the adversary $\mathcal{A}$. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{pqwUF\text{-}CMA}$ security of PKS with probability at least $\epsilon{\cdot}\mu/(2{\cdot}q_u)$. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and gives $\mathsf{pk}_{\mathsf{R}^*}$, $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$. $\mathcal{B}_1$ also samples $i \longleftarrow [q_u]$ and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_1$. $\mathcal{B}_1$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk}_{\mathsf{R}^*})$ and makes a signature oracle query on c^*. $\mathcal{CH}$ runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^*, \mathsf{sk}_{\mathsf{S}^*})$ and sends σ^* to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u}^* = (\mathsf{c}^*, \sigma^*)$ and sends the same to $\mathcal{A}$.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_1$ runs $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{m}, \mathsf{pk}_{\mathsf{R}^*})$ and makes a signature oracle query on c. $\mathcal{CH}$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{c}, \mathsf{sk}_{\mathsf{S}^*})$ and sends σ to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u} = (\mathsf{c}, \sigma)$ and sends u to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}_1$ halts the execution of $\mathcal{A}$, measures the input register for the query, and outputs (c, σ). Otherwise, $\mathcal{B}_1$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u})\rangle$$

where

$$f(\mathsf{u}) = \begin{cases} \perp & \text{if } \mathcal{R}'(\mathsf{u}^*, \mathsf{u}) = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_1$. ($\mathcal{B}_1$ does nothing with b').

Analysis: $\mathcal{B}_1$ outputs forgery as described in the above procedure. From the definition of Forge, $\mathcal{B}_1$ breaks the pqwUF-CMA security of PKS with probability at least $\epsilon \cdot \mu/(2 \cdot q_u)$.

Case 2: $\Pr[\mathcal{A}$ **succeeds** $\wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}$**.** We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the pqIND-CPA security of PKE with advantage negligibly close to $\frac{\epsilon}{2}$. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and gives $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$. $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_2$. $\mathcal{B}_2$ submits the message pair $(\mathsf{m}_0, \mathsf{m}_1)$ to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk}_{\mathsf{R}^*})$ and sends c^* to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^*, \mathsf{sk}_{\mathsf{S}^*})$, sets $\mathsf{u}^* := (\mathsf{c}^*, \sigma^*)$, adds $(\perp, \mathsf{u}^*)$ to list $\mathcal{L}$ (which is initially empty) and returns it to $\mathcal{A}$.

Signcryption queries: Let m be a signcryption query made by $\mathcal{A}$. $\mathcal{B}_2$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$, adds (m, u) to a list $\mathcal{L}$ and sends u to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u})\rangle$$

where

$$f(\mathsf{u}) = \begin{cases} \mathsf{m}' & \text{if } (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } \mathcal{R}'(\mathsf{u}, \mathsf{u}') = \mathsf{True} \\ \perp & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_2$. $\mathcal{B}_2$ forwards the same bit b' to $\mathcal{CH}$.

Analysis: We show that $\mathcal{B}$ simulates $\mathcal{A}$'s unsigncryption queries properly. The definition of $\overline{\mathsf{Forge}}$ says that for all unsigncryption queries made by $\mathcal{A}$, the probability that measuring query input yields a tuple (c, σ) such that $\mathcal{V}(\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}^*}) = 1$ and c was not a result of any previous signcryption oracle or challenge query in negligible. Since the total query magnitude of valid signcryption texts is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. □

Remark: As mentioned earlier, the quantum security proof of authenticated encryption in the $\mathcal{E}t\mathcal{S}$ paradigm given in a recent paper [SJS16] has a logical gap. In particular, the simulation procedure records quantum queries which clearly violates no-cloning and the analysis that follows only holds in the classical setting. We note that, our proof can be adapted to prove the confidentiality of the authenticated encryption construction based on the $\mathcal{E}t\mathcal{S}$ paradigm. However, our proof doesn't achieve full quantum security and the general problem still remains open.

Theorem 6.2. *If the primitive encryption scheme* PKE *is* IND-qCCA *secure (resp.* IND-qgCCA*) secure and the signature scheme* PKS *is* pqUF-NMA *secure, then the signcryption scheme* SC *in the* $\mathcal{S}t\mathcal{E}$ *paradigm is* sUF-uqCMA *(resp.* wUF-uqCMA*) secure in the two user outsider-security model* (sUF-ouqCMA (*resp.* wUF-ouqCMA) (*c.f., Section 3.4*)).

Proof. Here, we only prove the wUF-uqCMA security of SC in the outsider model. The proof of sUF-ouqCMA follows similarly. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is IND-qgCCA secure.

We use the standard hybrid argument. Let $\mathbf{Game_0}$ denote the original $\mathsf{wUF\text{-}ouqCMA}$ game of signcryption for adversary where all its queries are answered honestly. Let q_s be the number of signcryption queries made by the adversary. Let $\mathsf{m}_1, \ldots, \mathsf{m}_{q_s}$ be the messages and $\mathsf{u}_1, \ldots, \mathsf{u}_{q_s}$ be corresponding signcryption texts. Next, we define the hybrid games $\mathbf{Game_j}$, $1 \le j \le q_s$. Each $\mathbf{Game_j}$ is identical to $\mathbf{Game_0}$ except for the following: for the 1^{st} j signcryption queries, $\mathbf{Game_j}$ returns a random encryption of 0^{ℓ_m}, i.e., $\mathsf{u}_j \longleftarrow \mathcal{E}(0^{\ell_m}; \mathsf{pk}_{\mathsf{R}^*})$. Further, for a basis element u of any unsigncryption query, if u is equivalent to the result of any previous signcryption query m, then $\mathbf{Game_j}$ returns m. We denote $\mathsf{Succ}_j(\mathcal{A})$ to be the success probability of an adversary $\mathcal{A}$ in $\mathbf{Game_j}$. Note that $\mathbf{Game_{q_s}}$ answers all signcryption queries incorrectly. We make the following two claims:

- **Claim 1.** For any $1 \le j \le q_s$, $\mathbf{Game_{j-1}}$ and $\mathbf{Game_j}$ are indistinguishable under the $\mathsf{IND\text{-}qgCCA}$ security of the primitive encryption scheme PKE, i.e., for any quantum PPT adversary $\mathcal{A}$, $|\mathsf{Succ}_{j-1}(\mathcal{A}) - \mathsf{Succ}_j(\mathcal{A})| \le \mathsf{negl}(\lambda)$.

- **Claim 2.** For any quantum PPT adversary $\mathcal{A}$, there is a quantum PPT algorithm $\mathcal{B}$ such that $\mathsf{Succ}_{q_s}(\mathcal{A}) \le \mathsf{Adv}^{\mathsf{pqUF\text{-}NMA}}_{\mathcal{B},\mathsf{PKS}}(1^\lambda)$. Since PKS is $\mathsf{pqUF\text{-}NMA}$ secure, $\mathsf{Succ}_{q_s}(\mathcal{A}) \le \mathsf{negl}(\lambda)$.

Combining Claims 1 and 2, we get that $\mathsf{Succ}_0 \le (q_s + 1) \cdot \mathsf{negl}(\lambda)$ and hence the proof.

Proof of Claim 1. Let $\mathcal{A}$ be a quantum PPT adversary which can distinguish $\mathbf{Game_{j-1}}$ and $\mathbf{Game_j}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{IND\text{-}qgCCA}$ security of PKE with advantage at least $\epsilon/2$. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$, $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$. $\mathcal{B}_1$ simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Signcryption\ queries}$: Let m be any signcryption query made by $\mathcal{A}$. For the first $j-1$ queries, $\mathcal{B}_1$ answers with a random encryption of 0^{ℓ_m}. At the j^{th} query m_j, $\mathcal{B}_1$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}_j, \mathsf{sk}_{\mathsf{S}^*})$, prepares a challenge query $(\mathsf{m}_0, \mathsf{m}_1) \longleftarrow (\mathsf{m}_j \| \sigma, 0^{\ell_m})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk}_{\mathsf{R}^*})$ and sends c^* to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u} = \mathsf{c}^*$ and sends u to $\mathcal{A}$. After the j^{th} query, all the signcryption queries are answered properly. For all signcryption queries m, $\mathcal{B}_1$ also adds (m, u) to a list $\mathcal{L}$ (which is initially empty).

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_1$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}_1$ then sends a decryption query consisting of 1^{st} and 3^{rd} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}, 0^{\ell_m} \oplus g(\mathsf{u})\rangle$$

where

$$g(\mathsf{u}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{u}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_1$. $\mathcal{B}_1$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p}, g(\mathsf{u})\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p} \oplus f(\Delta), g(\mathsf{u})\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m}' & \text{if } (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } \mathcal{R}(\mathsf{u}, \mathsf{u}') = \mathsf{True} \\ [g(\mathsf{u})]_1 & \text{if } \mathcal{V}([g(\mathsf{u})]_1, [g(\mathsf{u})]_2, \mathsf{pk}_{\mathsf{S}^*}) = 1 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, g(\mathsf{u}))$.

Note that the ancilla register is entangled with other registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}_1$ sends a decryption query consisting of 1^{st} and 3^{rd} register to $\mathcal{CH}$. Finally, $\mathcal{B}_1$ obtains the state $\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends $\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$. The resulting state is sent back to $\mathcal{A}$.

Forgery and Analysis: $\mathcal{A}$ outputs a forgery u. It checks if u is a valid signcryption text by making a decryption oracle query and then verifying the validity of the signature. It also checks if u is indeed a fresh forgery, i.e., $\forall(\mathsf{m}', \mathsf{u}') \in \mathcal{L}$, it holds that $\mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*}) \neq \mathsf{m}'$. If all the above conditions are true then $\mathcal{B}_1$ sends $b' = 0$, i.e., it guesses that u_j is the encryption of $\mathsf{m}_j \| \sigma$. From the simulation procedure, it is clear that if u_j is indeed the encryption of $\mathsf{m}_j \| \sigma$, then $\mathcal{A}$ was run in $\mathbf{Game_{j-1}}$ else it was run in $\mathbf{Game_j}$. From our assumption on the success probability of $\mathcal{A}$, we get that the $\mathcal{B}_1$ succeeds with advantage at least $\epsilon/2$ in breaking IND-qgCCA security of PKE.

Proof of Claim 2. Let $\mathcal{A}$ be a quantum PPT adversary which succeeds in $\mathbf{Game_{q_s}}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the pqUF-NMA security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$, forwards $\mathsf{pk}_{\mathsf{S}^*}$, $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_2$ answers with a random encryption of 0^{ℓ_m}.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\mathsf{u})\rangle$$

where

$$f(\mathsf{u}) = \begin{cases} \mathsf{m}' & \text{if } (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } \mathcal{R}(\mathsf{u}, \mathsf{u}') = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs a forgery u. $\mathcal{B}_2$ runs $(\mathsf{m}, \sigma) \longleftarrow \mathcal{D}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*})$ and sends (m, σ) as forgery to $\mathcal{CH}$.

Analysis: It is easy to see that $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries perfectly and it breaks the pqUF-NMA security of PKS with advantage at least ϵ. □

6.2 Multi-User Setting

It was acknowledged in [DZ10], that the IND-CPA (resp. UF-NMA) security of the base encryption (resp. signature) scheme in the $\mathcal{E}t\mathcal{S}$ (resp. $\mathcal{S}t\mathcal{E}$) paradigm does not amplify to IND-CCA (resp. sUF-CMA) security in the multi-user setting. The issue is that in the case of $\mathcal{E}t\mathcal{S}$ paradigm, if the primitive encryption scheme is malleable, then the adversary may be able to modify the ciphertext to replace the sender's identity and signature with that of its own. Hence [DZ10] notes that, it is important to assume that the underlying encryption scheme is non-malleable (or IND-CCA secure) to achieve CCA-secure signcryption. A similar issue arises in the context of $\mathcal{S}t\mathcal{E}$ paradigm because UF-NMA security of the base signature scheme does not imply non-malleable signatures.

Some of the results we prove in the multi-user outsider model are stronger than their known classical variants. In particular, Theorems 6.3, 6.4, 6.5 and 6.6 are stronger than the corresponding results in the classical setting. We note that these results hold in the classical setting as well and thus strengthen previously known results [ADR02, DZ10].

6.2.1 Encrypt-then-Sign

In Theorem 6.3, we show that non-malleability is not a *necessary* condition to achieve $\mathsf{IND\text{-}qCCA}$ security in $\mathcal{E}t\mathcal{S}$ paradigm. Essentially, $\mathsf{IND\text{-}qgCCA}$ security of the primitive encryption scheme ensures that the adversary cannot modify the ciphertext to replace sender's identity with its own and $\mathsf{pqsUF\text{-}CMA}$ security of the signature scheme implies that the adversary cannot produce a valid signcryption text corresponding to the identity of the sender in the challenge signcryption text. The proof closely follows the proof strategy of Theorem 6.1 and can be found in Appendix B.1.

Theorem 6.3. *If the primitive encryption scheme* PKE *is* $\mathsf{IND\text{-}qgCCA}$ *secure and the signature scheme* PKS *is* $\mathsf{pqsUF\text{-}CMA}$ *secure, then the signcryption scheme* SC *in the* $\mathcal{E}t\mathcal{S}$ *paradigm is* $\mathsf{IND\text{-}uqCCA}$ *secure in the multi user outsider-security model* ($\mathsf{fM\text{-}IND\text{-}ouqCCA}$ (*c.f., Section 3.4*)).

6.2.2 Sign-then-Encrypt

Our next result concerns with unforgeability in the $\mathcal{S}t\mathcal{E}$ paradigm. In a nutshell, Theorem 6.4 follows from the following argument: $\mathsf{IND\text{-}qCCA}$ security of the underlying encryption scheme implies that a signcryption text under the receiver's key used in the challenge is indistinguishable from a random signcryption text and $\mathsf{wUF\text{-}qCMA}$ property implies that the adversary cannot forge a valid signcryption text corresponding to the receiver and sender identities involved in the challenge. The proof closely follows the proof strategy of Theorem 6.2 and can be found in Appendix B.2.

Theorem 6.4. *If the primitive encryption scheme* PKE *is* $\mathsf{IND\text{-}qCCA}$ *secure and the signature scheme* PKS *is* $\mathsf{pqwUF\text{-}CMA}$ *secure, then the signcryption scheme* SC *in the* $\mathcal{S}t\mathcal{E}$ *paradigm is* $\mathsf{sUF\text{-}uqCMA}$ *secure in the multi user outsider-security model* ($\mathsf{fM\text{-}sUF\text{-}ouqCMA}$ (*c.f., Section 3.4*)).

6.2.3 Commit-then-Encrypt-and-Sign

We next discuss our results in the $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm. Recall that, in the insider security model $\mathsf{IND\text{-}CCA}$ (resp. $\mathsf{sUF\text{-}CMA}$) security of the base encryption (resp. signature) scheme is not preserved. Here, we show that both these notions are preserved in the outsider security model assuming that the commitment scheme satisfies some standard security properties. Theorem 6.5 states the quantum security of confidentiality of $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm. We only give a proof sketch here and the lemmas involved in the same are deferred to Appendices B.3, B.4, B.5 and B.6.

Theorem 6.5. *Suppose the primitive encryption scheme* PKE *is* $\mathsf{IND\text{-}qCCA}$ *secure, the signature scheme* PKS *is* $\mathsf{pqsUF\text{-}CMA}$ *secure and the commitment scheme* C *satisfies* $\mathsf{qrConcealment}$ *and* $\mathsf{qHiding}$ *properties. Further, assume that the size of the domain of all possible* com *is superpolynomial in the security parameter. Then the signcryption scheme* SC *in the* $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ *paradigm is* $\mathsf{IND\text{-}uqCCA}$ *secure in the multi user outsider-security model* ($\mathsf{fM\text{-}IND\text{-}ouqCCA}$ (*c.f., Section 3.4*)).

Proof Sketch. We prove security through a sequence of games. Let $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ denote the receiver and sender identities involved in the challenge respectively. Let q_s be the number of signcryption oracle queries made by $\mathcal{A}$ on $\mathsf{pk}_{\mathsf{R}^*}$ and $\{\mathsf{u}_i = (\mathsf{com}_i, \sigma_i, \mathsf{c}_i) : i \in [q_s]\}$ be the answers to the signcryption queries. Let $(\mathsf{u}^* = (\mathsf{com}^*, \sigma^*, \mathsf{c}^*), \mathsf{pk}_{\mathsf{S}^*})$ denote a challenge signcryption text and $\mathcal{L} = \{(\mathsf{com}_i, \sigma_i) | i \in [q_s]\} \cup \{(\mathsf{com}^*, \sigma^*)\}$. For a signcryption text $(\mathsf{u} = (\mathsf{com}, \sigma, \mathsf{c}), \mathsf{pk}_{\mathsf{S}})$, we define the following the events:

1. $\mathsf{erConceal} := [\mathsf{c} = \mathsf{c}^* \ \wedge\ (\mathsf{com}, \sigma) \in \mathcal{L} \wedge \mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*})) \neq \bot \ \wedge\ \mathsf{pk}_{\mathsf{S}} = \mathsf{pk}_{\mathsf{S}^*}]$.
2. $\mathsf{Forge} := [\mathcal{V}(\mathsf{com} \| \mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_{\mathsf{S}^*}) = 1 \ \wedge\ (\mathsf{com}, \sigma) \notin \mathcal{L} \ \wedge\ \mathsf{pk}_{\mathsf{S}} = \mathsf{pk}_{\mathsf{S}^*}]$.

We say that $\mathsf{erConceal}[\mathsf{u}, \mathsf{pk}_{\mathsf{S}}] = \mathsf{True}$ (resp. $\mathsf{Forge}[\mathsf{u}, \mathsf{pk}_{\mathsf{S}}] = \mathsf{True}$) if $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}})$ satisfies the event $\mathsf{erConceal}$ (resp. Forge).

$\mathbf{Game}_{\mathbf{Real}}$: The original fM-IND-ouqCCA game of signcryption.

$\mathbf{Game}_{\widetilde{\mathbf{Real}}}$: Same as $\mathbf{Game}_{\mathbf{Real}}$ except for the answers of unsigncryption queries after the challenge query. In particular, if a query $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}})$ satisfies the event $\mathsf{erConceal}$, then the challenger returns $\bot$ to the adversary.

$\mathbf{Game}_{\mathbf{0}}$: Same as $\mathbf{Game}_{\widetilde{\mathbf{Real}}}$ except for the answers of unsigncryption queries after the challenge query. If a query $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}})$ satisfies the event Forge, then the challenger returns $\bot$ to the adversary.

$\mathbf{Game}_{\mathbf{1}}$: Same as $\mathbf{Game}_{\mathbf{0}}$ except for the construction of challenge signcryption text, viz., $\mathsf{c}^* = \mathcal{E}(\mathsf{decom}_r \| \mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$, where decom_r is randomly sampled from the decommitment space.

Lemma 6.1. $\mathbf{Game}_{\mathbf{Real}}$ *and* $\mathbf{Game}_{\widetilde{\mathbf{Real}}}$ *are indistinguishable under the* qrConcealment *property of the commitment scheme* C.

Lemma 6.2. $\mathbf{Game}_{\widetilde{\mathbf{Real}}}$ *and* $\mathbf{Game}_{\mathbf{0}}$ *are indistinguishable under the* pqsUF-CMA *property of the primitive signature scheme* PKS.

Lemma 6.3. $\mathbf{Game}_{\mathbf{0}}$ *and* $\mathbf{Game}_{\mathbf{1}}$ *are indistinguishable under the* IND-qCCA *property of the primitive encryption scheme* PKE.

Lemma 6.4. *For any quantum PPT adversary $\mathcal{A}$, there is a quantum PPT algorithm $\mathcal{B}$ such that* $\mathsf{Adv}^{\mathbf{Game}_1}_{\mathcal{A},\mathsf{SC}}(1^\lambda) \le \mathsf{Adv}^{\mathsf{qHiding}}_{\mathcal{B},\mathsf{C}}(1^\lambda)$.

Theorem 6.6 concerns the quantum security of unforgeability in the $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm. The proof can be argued by partitioning the space of valid forgeries into two disjoint subsets. The first part consists of signcryption forgeries which result in a forgery for the base signature scheme (Lemma 6.5). To analyze the forgeries from the second partition one can define a sequence of indistinguishable games. Theorem 6.6 states that quantum security of unforgeability of $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm. We only give a proof sketch here and the lemmas involved in the same are deferred to Appendices B.7, B.8, B.9 and B.10.

Theorem 6.6. *If the primitive signature scheme* PKS *is* pqsUF-CMA *secure, the encryption scheme* PKE *is* IND-qCCA *secure and the commitment scheme* C *satisfies* qfBinder *property, then the signcryption scheme* SC *in the $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm is* sUF-uqCMA *secure in the multi user outsider-security model* (fM-sUF-ouqCMA (*c.f., Section 3.4*)).

Proof Sketch. Let $\mathcal{A}$ be a quantum PPT adversary that can break fM-sUF-ouqCMA security of the signcryption scheme SC with probability ϵ. Let q_s be the number of signcryption oracle queries made by $\mathcal{A}$ on the challenge identity $\mathsf{pk}_{\mathsf{R}^*}$ and $\{\mathsf{u}_i = (\mathsf{com}_i, \sigma_i, \mathsf{c}_i) : i \in [q_s]\}$ be the answers to the signcryption queries. Let $\widetilde{\mathsf{u}} = (\widetilde{\mathsf{com}}, \widetilde{\sigma}, \widetilde{\mathsf{c}})$ be a forgery produced by $\mathcal{A}$. Let Forge denote the event that $\forall i \in [q_s], (\mathsf{com}_i, \sigma_i) \neq (\widetilde{\mathsf{com}}, \widetilde{\sigma})$. Note that,

$$\epsilon \le \Pr[\mathcal{A} \text{ succeeds}] = \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}]$$

$$\implies \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] \ge \frac{\epsilon}{2} \text{ or } \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] \ge \frac{\epsilon}{2}.$$

Case 1: $\Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] \geq \frac{\epsilon}{2}$.

The following lemma shows that Case 1 will not happen.

Lemma 6.5. *If* PKS *is* pqsUF-CMA *secure, then* $\Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] < \frac{\epsilon}{2}$.

Case 2: $\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] \geq \frac{\epsilon}{2}$. Let $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ be the receiver and sender identities involved in the challenge respectively. We use the standard hybrid argument. Let q_s be the number of signcryption oracle queries made by the adversary on $\mathsf{pk}_{\mathsf{R}^*}$. Let $\mathsf{m}_1, \dots, \mathsf{m}_{q_s}$ be the messages and $\mathsf{u}_1, \dots, \mathsf{u}_{q_s}$ be corresponding signcryption texts.

$\mathbf{Game_{Real}}$: The original fM-sUF-ouqCMA game of signcryption.

Let $(\mathsf{u} = (\mathsf{com}, \sigma, \mathsf{c}), \mathsf{pk}_\mathsf{S})$ be a signcryption text appeared as a basic element in say, i^{th} unsigncryption query. Let i_s denote the number signcryption queries till the i^{th} unsigncryption query. Let the response of the j^{th} signcryption query be $\mathsf{u}_j = (\mathsf{com}_j, \sigma_j, \mathsf{c}_j)$ for $j \in [i_s]$. For such signcryption text $(\mathsf{u}, \mathsf{pk}_\mathsf{S})$, let srConceal denote the event that there exist an $j \in [i_s]$ such that $\mathsf{c} = \mathsf{c}_j$, $\mathsf{com} \neq \mathsf{com}_j$ and $\mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*})) \neq \perp$. We say that $\mathsf{srConceal}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True}$ if u satisfies the event srConceal.

$\mathbf{Game_0}$: Same as $\mathbf{Game_{Real}}$ except for the answers of unsigncryption queries. If $(\mathsf{u}, \mathsf{pk}_\mathsf{S})$ satisfies the event srConceal, then the challenger returns $\perp$ to the adversary.

Next, we define the hybrid games $\mathbf{Game_j}$, $1 \leq j \leq q_s$. Each $\mathbf{Game_j}$ is identical to $\mathbf{Game_0}$ except for the following changes:

- For the first j signcryption queries on $\mathsf{pk}_{\mathsf{R}^*}$, $\mathbf{Game_j}$ runs $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$, $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*}; \mathsf{pk}_{\mathsf{R}^*})$, where decom_r is sampled uniformly from the decommitment space. It returns $\mathsf{u} = (\mathsf{com}, \sigma, \mathsf{c})$ and adds (m, u) to a list $\mathcal{L}$.
- For a basis element $(\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_{\mathsf{S}^*})$ of any unsigncryption query, if the tuple $(\mathsf{m}, \mathsf{u}) \in \mathcal{L}$, then $\mathbf{Game_j}$ returns m. Otherwise, it returns $\mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_{\mathsf{S}^*})$.

We denote $\mathsf{Succ}_j(\mathcal{A})$ to be the success probability of an adversary $\mathcal{A}$ in $\mathbf{Game_j}$. Note that $\mathbf{Game_{q_s}}$ answers all signcryption queries on $\mathsf{pk}_{\mathsf{R}^*}$ incorrectly. It follows from the following lemmas that $\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}]$ is negligible and hence ϵ is negligible.

Lemma 6.6. $\mathbf{Game_{Real}}$ *and* $\mathbf{Game_0}$ *are indistinguishable under the* qrConcealment *property of the commitment scheme* C*.*

Lemma 6.7. *For any* $1 \leq j \leq q_s$*,* $\mathbf{Game_{j-1}}$ *and* $\mathbf{Game_j}$ *are indistinguishable under the* IND-qCCA *property of the primitive encryption scheme* PKE*, i.e., for any quantum PPT adversary* $\mathcal{A}$*,* $|\mathsf{Succ}_{j-1}(\mathcal{A}) - \mathsf{Succ}_j(\mathcal{A})| \leq \mathsf{negl}(\lambda)$.

Lemma 6.8. *For any quantum PPT adversary* $\mathcal{A}$*, there is a quantum PPT algorithm* $\mathcal{B}_3$ *such that* $\mathsf{Succ}_{q_s}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{qfBinder}}_{\mathcal{B}_3,\mathsf{PKS}}(1^\lambda)$*. Since,* C *has* qfBinder *property,* $\mathsf{Succ}_{q_s}(\mathcal{A}) \leq \mathsf{negl}(\lambda)$*.*

7 Instantiations

In previous sections, we have proved the security of signcryption schemes based on generic composition of PKE, PKS and commitment in various paradigms. If we consider the commitment scheme discussed in Section 6, it satisfies all the desired properties in QROM. Next, we recall some candidate encryption and signature schemes which can be used to instantiate signcryption schemes in various paradigms.

Candidates for post-quantum PKE. An isogeny based encryption scheme proposed in [JF11] is claimed to be secure in the standard model under the assumption that the hash function family is entropy smoothing. While we are not aware of any family of hash functions which is entropy smoothing in the quantum setting, using results from [BDF+11], the above encryption scheme can be proved pqIND-CPA secure in the quantum random oracle model. Many lattice based pqIND-CPA secure encryption schemes are also available in the literature, e.g., [CHK+16, CKLS16]. The same schemes in [CHK+16, CKLS16] were shown to be pqIND-CCA secure in the QROM using a quantum variant [TU16] of the Fujisaki-Okamoto transformation [FO13]. We note that the available quantum variants [TU16, HHK17, SXY18] of Fujisaki-Okamoto for getting pqIND-CCA secure KEM/PKE in the QROM are not only applicable to lattice based schemes, but also applicable to other schemes. After the third round of evaluation [NIS20] at NIST's post-quantum competition, 9 KEM/PKE candidates have been shortlisted, four of them are considered as finalists and the remaining are alternatives. Some of the PKE-candidates are SABER, NTRU (lattice-based) and HQC (code-based).

Candidates for post-quantum PKS. Six signature candidates have been shortlisted after the 3rd round of evaluation [NIS20] at NIST's post-quantum competition. Three of them are considered as finalists and the remaining are alternatives. There are two lattice-based candidates - CRYSTALS-DILITHIUM and FALCON, two multivariate-based candidates - Rainbow and GeMSS, one hash-based candidate - SPHINCS+, and the remaining one is miscellaneous candidate. Among these candidates, only FALCON and SPHINCS+ have the post-quantum security (in QROM). Besides the NIST post-quantum candidates, there are many lattice based pqwUF-CMA signatures available in the literature, for example, [CHKP10]. For isogeny based signature, one can consider the signature from [YAJ+17] which was proven pqsUF-CMA secure in the QROM using the conversion of [Unr15]. Moreover, by using the transformation from [ES15], we can get a pqsUF-CMA secure signature scheme in the QROM from a pqwUF-CMA secure signature scheme.

Candidates for quantum secure PKE. If Construction 4.11 from [BZ13] is applied to the basic IBE scheme of [ABB10], we get an IND-qCCA secure encryption scheme. We point out that all the pqIND-CPA secure PKE schemes trivially come under the class of quantum secure PKE as the encryption algorithm is public.

Candidates for quantum secure PKS. If Construction 3.10 from [BZ13] is instantiated with the signature schemes from [ABB10, CHKP10], we get wUF-qCMA secure signature schemes. If Construction 3.12 from [BZ13] is applied on [GPV08], it gives a wUF-qCMA signature scheme in the QROM. We remark that a sUF-qCMA secure signature schemes can be obtained by first applying the transformation [ES15] to the signature schemes in [ABB10, CHKP10, GPV08] followed by Construction 3.10 of [BZ13]. Since [ES15] gives signatures in the QROM, the above conversion provides sUF-qCMA security in the QROM.

References

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient Lattice (H)IBE in the Standard Model. In *EUROCRYPT*, volume 6110 of *LNCS*, pages 553–572. Springer, 2010.

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the Security of Joint Signature and Encryption. In *EUROCRYPT*, volume 2332 of *LNCS*, pages 83–107. Springer, 2002.

[AGM18] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable Quantum Encryption. In *EUROCRYPT*, volume 10822 of *LNCS*, pages 489–519. Springer, 2018.

[AMRS18] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-secure Message Authentication via Blind-unforgeability. *CoRR*, abs/1803.03761, 2018.

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding. In *FOCS*, pages 474–483. IEEE Computer Society, 2014.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and Weaknesses of Quantum Computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[BDF$^+$11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random Oracles in a Quantum World. In *ASIACRYPT*, volume 7073 of *LNCS*, pages 41–69. Springer, 2011.

[BN08] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Journal of Cryptology*, 21(4):469–491, 2008.

[BSZ07] Joonsang Baek, Ron Steinfeld, and Yuliang Zheng. Formal Proofs for the Security of Signcryption. *Journal of Cryptology*, 20(2):203–235, 2007.

[BZ13] Dan Boneh and Mark Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In *CRYPTO*, volume 8043 of *LNCS*, pages 361–379. Springer, 2013.

[CHK$^+$16] Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE. In *ICISC*, volume 10157 of *LNCS*, pages 51–74. Springer, 2016.

[CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai Trees, or How to Delegate a Lattice Basis. In *EUROCRYPT*, volume 6110 of *LNCS*, pages 523–552. Springer, 2010.

[CKLS16] Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yongsoo Song. Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR. *IACR Cryptology ePrint Archive*, 2016:1126, 2016.

[DZ10] Alexander W. Dent and Yuliang Zheng, editors. *Practical Signcryption.* Information Security and Cryptography. Springer, 2010.

[ES15] Edward Eaton and Fang Song. Making Existential-unforgeable Signatures Strongly Unforgeable in the Quantum Random-oracle Model. In *TQC*, volume 44 of *LIPIcs*, pages 147–162. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. *Journal of Cryptology*, 26(1):80–101, 2013.

[FTTY18] Atsushi Fujioka, Katsuyuki Takashima, Shintaro Terada, and Kazuki Yoneyama. Supersingular isogeny diffie-hellman authenticated key exchange. *IACR Cryptology ePrint Archive*, 2018:730, 2018.

[GHS16] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic Security and Indistinguishability in the Quantum World. In *CRYPTO*, volume 9816 of *LNCS*, pages 60–89. Springer, 2016.

[GM18] François Gérard and Keno Merckx. Post-Quantum Signcryption From Lattice-Based Signatures. *IACR Cryptology ePrint Archive*, 2018:56, 2018.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. In *STOC*, pages 197–206. ACM, 2008.

[GYZ17] Sumegha Garg, Henry Yuen, and Mark Zhandry. New Security Notions and Feasibility Results for Authentication of Quantum Data. In *CRYPTO*, volume 10402 of *LNCS*, pages 342–371. Springer, 2017.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A Modular Analysis of the Fujisaki-Okamoto Transformation. In *TCC*, volume 10677 of *LNCS*, pages 341–371. Springer, 2017.

[JF11] David Jao and Luca De Feo. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In *PQCRYPTO*, volume 7071 of *LNCS*, pages 19–34. Springer, 2011.

[MMS09] Takahiro Matsuda, Kanta Matsuura, and Jacob C. N. Schuldt. Efficient Constructions of Signcryption Schemes and Signcryption Composability. In *INDOCRYPT*, volume 5922 of *LNCS*, pages 321–342. Springer, 2009.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, NY, USA, 2000.

[NIS17] National Institute of Standards and Technology: Post-quantum crypto project. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/`, 2017. Accessed: 2018-05-10.

[NIS20] National Institute of Standards and Technology: Post-quantum crypto project. `https://csrc.nist.gov/publications/detail/nistir/8309/final`, 2020. Accessed: 2020-09-21.

[NP16] Mridul Nandi and Tapas Pandit. On the Security of Joint Signature and Encryption Revisited. *Journal of Mathematical Cryptology*, 10(3-4):181–221, 2016.

[SJS16] Vladimir Soukharev, David Jao, and Srinath Seshadri. Post-Quantum Security Models for Authenticated Encryption. In *PQCRYPTO*, volume 9606 of *LNCS*, pages 64–78. Springer, 2016.

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model. In *EUROCRYPT*, volume 10822 of *LNCS*, pages 520–551. Springer, 2018.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms. In *TCC*, volume 9816 of *LNCS*, pages 192–216. Springer, 2016.

[Unr15] Dominique Unruh. Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model. In *EUROCRYPT*, volume 9057 of *LNCS*, pages 755–784. Springer, 2015.

[Unr16] Dominique Unruh. Computationally Binding Quantum Commitments. In *EUROCRYPT*, volume 9666 of *LNCS*, pages 497–527. Springer, 2016.

[YAJ$^+$17] Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev. A Post-Quantum Digital Signature Scheme Based on Supersingular Isogenies. In *Financial Cryptography and Data Security*, volume 10322 of *LNCS*, pages 163–181. Springer, 2017.

[Zha18] Mark Zhandry. How to Record Quantum Queries, and Applications to Quantum Indifferentiability. *IACR Cryptology ePrint Archive*, 2018:276, 2018.

[Zhe97] Yuliang Zheng. Digital Signcryption or How to Achieve Cost(Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption). In *CRYPTO*, volume 1294 of *LNCS*, pages 165–179. Springer, 1997.

A Proofs in Insider Model

A.1 Proof of Lemma 5.2

Proof. Let q_u be the total number of unsigncryption queries made by the adversary $\mathcal{A}$. Let δ_i be the sum of amplitudes squared of those basic elements $(\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p})$ involved in the i^{th} unsigncryption query for which the event E is satisfied. Let $\delta = \sum_{i\in[q_u]} \delta_i$ be the sum of the probabilities. We claim that δ is negligible. Indeed, we can construct an adversary $\mathcal{B}$ which breaks the $\mathsf{qrConcealment}$ property of C with advantage δ/q_u^2. $\mathcal{B}$ simulates $\mathcal{A}$'s queries in the following way:

Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}$. $\mathcal{B}$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathcal{CK}$ to the adversary $\mathcal{A}$. $\mathcal{B}$ also samples $i \overset{\mathrm{U}}{\longleftarrow} [q_u]$ and simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ and submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ along with $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ to $\mathcal{B}$. $\mathcal{B}$ then samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and sends m_b to $\mathcal{CH}$. $\mathcal{CH}$ runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and gives $(\mathsf{com}^*, \mathsf{decom}^*)$ to $\mathcal{B}$. $\mathcal{B}$ executes $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}^* \| \mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$, $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^* \| \mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ and returns $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ to $\mathcal{A}$.

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}$ halts the execution of $\mathcal{A}$, measures the input register for the query, and outputs the register containing the string com. Otherwise, $\mathcal{B}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u}, \mathsf{pk_S}) = \begin{cases} \perp & \text{if } \mathcal{R}'((\mathsf{u}^*, \mathsf{pk_{S^*}}), (\mathsf{u}, \mathsf{pk_S})) = \mathsf{True} \vee \mathsf{E}[\mathsf{u}, \mathsf{pk_S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. ($\mathcal{B}$ does nothing with b').

$\mathsf{Analysis}$: The probability that com ($\mathcal{B}$'s output) satisfies $\mathsf{Open}(\mathsf{com}, \mathsf{decom}^*) \neq \perp$ is at least δ/q_u^2 (Since, $\mathsf{E} \implies \mathsf{Open}(\mathsf{com}, \mathsf{decom}^*) \neq \perp$). The $\mathsf{qrConcealment}$ property of C shows that δ is negligible. Since the total query magnitude of signcryption texts satisfying E is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1.

□

A.2 Proof of Lemma 5.3

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which can distinguish $\mathbf{Game_0}$ and $\mathbf{Game_1}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}$ which breaks the $\mathsf{IND\text{-}qgCCA}$ security of PKE with probability $\epsilon/2$. Let $\mathcal{CH}$ be the challenger for the primitive encryption scheme PKE which runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}$. $\mathcal{B}$ runs the setup algorithm of the commitment scheme and forwards the public commitment key $\mathcal{CK}$ and $\mathsf{pk_{R^*}}$ to $\mathcal{A}$. $\mathcal{B}$ simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ and submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ along with $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ to $\mathcal{B}$. $\mathcal{B}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$. Then it samples decom_r uniformly at random from the decommitment space, sets $(\mathsf{decom}_0||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_1||\mathsf{pk}_{\mathsf{S}^*}) \longleftarrow (\mathsf{decom}^*||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $\beta \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_\beta||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and sends it to $\mathcal{B}$. The simulator runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, sets $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ and returns it to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum\limits_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum\limits_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m} \oplus g(\mathsf{c})\rangle$$

where

$$g(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta), g(\mathsf{c})\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{Open}(\mathsf{com}, [g(\mathsf{c})]_1) & \text{if } \mathcal{V}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_\mathsf{S}) = 1 \wedge \mathsf{pk}_\mathsf{S} = [g(\mathsf{c})]_2 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, \mathsf{pk}_\mathsf{S}, g(\mathsf{c}))$.

Note that the ancilla register is entangled with other registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}$ sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. Finally, $\mathcal{B}$ obtains the following state

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle .$$

It discards the last register and sends $\sum\limits_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. If $b = b'$, $\mathcal{B}$ replies $\beta' = 0$ else returns $\beta' = 1$.

Analysis: The only difference between $\mathbf{Game_0}$ and $\mathbf{Game_1}$ is the construction of the challenge signcryption text. We will first show that all the unsigncryption queries are handled properly. It suffices to show that each of the basis element $|\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ is handled properly. The definition of $\mathcal{R}'$ states that a query $|\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ is legitimate if one of the following conditions is false:

1. $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$
2. $\mathsf{com} = \mathsf{com}^*$
3. $\mathcal{V}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_\mathsf{S}) = \mathsf{True}$
4. $\mathsf{pk}_\mathsf{S} = \mathsf{pk}_{\mathsf{S}^*}$

If condition 1 is false then $\mathcal{B}$ answers by making decryption query to $\mathcal{CH}$. If condition 3 or 4 is false then by the nature of construction, $(\mathsf{u}, \mathsf{pk_S})$ is an invalid query and $\mathcal{B}$ returns $\perp$ in this case. The only case to discuss is when condition 2 is false and conditions 1, 3 and 4 are true. Note that in the simulation $\mathcal{A}$ is given $\perp$ for this case. We divide this case into two sub cases: (a$_1$) E and (a$_2$) $[\mathsf{com}^* \neq \mathsf{com} \wedge \mathcal{R}(\mathsf{c}^*, \mathsf{c}) = \mathsf{True} \wedge \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) = \perp]$. By definition of $\mathbf{Game_0}$ and $\mathbf{Game_1}$, the adversary is returned $\perp$ if E occurs. So, the only sub case left is $[\mathsf{com}^* \neq \mathsf{com} \wedge \mathcal{R}(\mathsf{c}^*, \mathsf{c}) = \mathsf{True} \wedge \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) = \perp]$. Since, in this case $\mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) = \perp$, $\mathcal{A}$ will get $\perp$ as reply. From the challenge phase, it is straightforward that the challenge signcryption text is properly distributed. Therefore, all the answers to the oracle queries are perfectly simulated. The advantage of $\mathcal{B}$ in breaking $\mathsf{IND\text{-}qgCCA}$ security of the primitive encryption scheme PKE is given by

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IND-qgCCA}}_{\mathcal{B},\mathsf{PKE}}(1^\lambda) &= \left|\Pr\left[\beta = \beta'\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\beta = 0, \beta' = 0\right] + \Pr\left[\beta = 1, \beta' = 1\right] - \frac{1}{2}\right| \\
&= \left|\frac{1}{2}\Pr\left[\beta' = 0|\beta = 0\right] + \frac{1}{2}\Pr\left[\beta' = 1|\beta = 1\right] - \frac{1}{2}\right| \\
&= \left|\frac{1}{2}\Pr\left[\beta' = 0|\beta = 0\right] - \frac{1}{2}\Pr\left[\beta' = 0|\beta = 1\right]\right| \\
&= \left|\frac{1}{2}\Pr\left[b = b'|\beta = 0\right] - \frac{1}{2}\Pr\left[b = b'|\beta = 1\right]\right| \\
&= \frac{1}{2}\left|\mathsf{Adv}^{\mathbf{Game_0}}_{\mathcal{A},\mathsf{SC}}(1^\lambda) - \mathsf{Adv}^{\mathbf{Game_1}}_{\mathcal{A},\mathsf{SC}}(1^\lambda)\right|.
\end{aligned}$$

□

A.3 Proof of Lemma 5.4

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which has advantage ϵ in $\mathbf{Game_1}$. We construct a quantum PPT algorithm $\mathcal{B}$ which breaks the $\mathsf{qHiding}$ property of C with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}$. $\mathcal{B}$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}$ simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ and submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ along with $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}})$ to $\mathcal{B}$. $\mathcal{B}$ submits the same message pair $(\mathsf{m_0}, \mathsf{m_1})$ to the challenger $\mathcal{CH}$. $\mathcal{CH}$ then samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and sends com^* to $\mathcal{B}$. $\mathcal{B}$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ and $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_r||\mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$, where decom_r is randomly sampled from the decommitment space. $\mathcal{B}$ sets $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ and sends the same to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u_{quant}} = \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u}, \mathsf{pk_S}) = \begin{cases} \perp & \text{if } \mathcal{R}'((\mathsf{u}^*, \mathsf{pk_{S^*}}), (\mathsf{u}, \mathsf{pk_S})) = \mathsf{True} \vee \mathsf{E}[\mathsf{u}, \mathsf{pk_S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. $\mathcal{B}$ returns the same bit b' to $\mathcal{CH}$.

$\mathsf{Analysis}$: It is easy to see that $\mathcal{B}$ simulates $\mathcal{A}$'s queries perfectly and it breaks the $\mathsf{qHiding}$ property of C with advantage at least ϵ. □

A.4 Proof of Lemma 5.5

Proof. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{wUF\text{-}qCMA}$ security of PKS with probability at least $\frac{\epsilon}{2}$. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ and $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$.

$\mathsf{Signcryption\ queries}$: Let $\mathsf{m}_{\mathsf{quant}} = \sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}\rangle$ be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_1$ appends a ℓ_{cm} qubit ancilla register, containing the state $\left|0^{\ell_{cm}}\right\rangle$, to the query and obtains the state $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \left|\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}, 0^{\ell_{cm}}\right\rangle$. $\mathcal{B}_1$ chooses a randomness r_{com} and applies the following unitary transformation

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \left|\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}, 0^{\ell_{cm}}\right\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \left|\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}, 0^{\ell_{cm}} \oplus \mathsf{Commit}(\mathsf{m}; r_{com})\right\rangle.$$

The resulting state can be equivalently viewed as $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{com}_\mathsf{p}, \sigma_\mathsf{p}, \mathsf{c}_\mathsf{p}, \mathsf{com}, \mathsf{decom}\rangle$.

$\mathcal{B}_1$ sends a signature query consisting of 2^{nd}, 4^{th} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{com}_\mathsf{p}, \sigma_\mathsf{p}, \mathsf{c}_\mathsf{p}, \mathsf{com}, \mathsf{decom}\rangle$$

$$\updownarrow$$

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{com}_\mathsf{p}, \sigma_\mathsf{p} \oplus \mathcal{S}(\mathsf{com}||\mathsf{pk}_\mathsf{R}, \mathsf{sk}_{\mathsf{S}^*}), \mathsf{c}_\mathsf{p}, \mathsf{com}, \mathsf{decom}\rangle.$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_1$. $\mathcal{B}_1$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{com}_\mathsf{p}, \sigma_\mathsf{p} \oplus \mathcal{S}(\mathsf{com}||\mathsf{pk}_\mathsf{R}, \mathsf{sk}_{\mathsf{S}^*}), \mathsf{c}_\mathsf{p}, \mathsf{com}, \mathsf{decom}\rangle$$

$$\updownarrow$$

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{com}_\mathsf{p} \oplus \mathsf{com}, \sigma_\mathsf{p} \oplus \mathcal{S}(\mathsf{com}||\mathsf{pk}_\mathsf{R}, \mathsf{sk}_{\mathsf{S}^*}), \mathsf{c}_\mathsf{p} \oplus \mathcal{E}(\mathsf{decom}||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R}), \mathsf{com}, \mathsf{decom}\rangle.$$

The resulting state can be equivalently written as $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p} \oplus \mathsf{u}, \mathsf{com}, \mathsf{decom}\rangle$, where $\mathsf{u} = \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$. Note that $\mathcal{B}_1$ can unentangle the last two registers by applying commitment operator using the randomness r_{com} to obtain the state $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p} \oplus \mathsf{u}\rangle \otimes \left|0^{\ell_{cm}}\right\rangle$. It discards the last register and sends $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p} \oplus \mathsf{u}\rangle$ to $\mathcal{A}$.

$\mathsf{Forgery}$: $\mathcal{A}$ outputs $q+1$ forgeries $\{(\mathsf{u}_i = (\mathsf{com}_i, \sigma_i, \mathsf{c}_i), \mathsf{pk}_{\mathsf{R}i}, \mathsf{sk}_{\mathsf{R}i}) : i \in [q+1]\}$. $\mathcal{B}_1$ then forwards $(\mathsf{com}_1||\mathsf{pk}_{\mathsf{R}1}, \sigma_1), \ldots, (\mathsf{com}_{q+1}||\mathsf{pk}_{\mathsf{R}q+1}, \sigma_{q+1})$ as forgeries to $\mathcal{CH}$.

$\mathsf{Analysis}$: It is clear that $\mathcal{B}_1$ breaks $\mathsf{wUF\text{-}qCMA}$ security of PKS with probability at least $\frac{\epsilon}{2}$. □

A.5 Proof of Lemma 5.6

Proof. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the $\mathsf{qBinding}$ property of C with advantage at least $\frac{\epsilon}{2}$. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}_2$. Then, $\mathcal{B}_2$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and returns commitment key $\mathcal{CK}$ and $\mathsf{pk_{S^*}}$ to the adversary $\mathcal{A}$. $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: Let $\mathsf{m_{quant}} = \sum\limits_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}\rangle$ be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} \psi_{\mathsf{m},\mathsf{pk_R},\mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p} \oplus \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R})\rangle .$$

The resulting state is sent back to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs $q+1$ forgeries $\{(\mathsf{u}_i = (\mathsf{com}_i, \sigma_i, \mathsf{c}_i), \mathsf{pk}_{\mathsf{R}i}, \mathsf{sk}_{\mathsf{R}i}) : i \in [q+1]\}$. $\mathcal{B}_2$ identifies the tuple with $\mathsf{com}_i = \mathsf{com}_j$ and forwards $(\mathsf{com}_i, \mathsf{decom}_i, \mathsf{decom}_j)$ to $\mathcal{CH}$, where $\mathsf{decom}_i = [\mathcal{D}(\mathsf{c}_i, \mathsf{sk}_{\mathsf{R}i})]_1$ and $\mathsf{decom}_j = [\mathcal{D}(\mathsf{c}_j, \mathsf{sk}_{\mathsf{R}j})]_1$. Note that $\mathsf{dM\text{-}wUF\text{-}iqCMA}$ security of SC ensures that $\mathsf{Open}(\mathsf{com}_i, \mathsf{decom}_i) \neq \mathsf{Open}(\mathsf{com}_i, \mathsf{decom}_j)$.

Analysis: It is clear that $\mathcal{B}_2$ breaks $\mathsf{qBinding}$ property of C with probability at least $\frac{\epsilon}{2}$. □

B Proofs in Multi-User Outsider Model

B.1 Proof of Theorem 6.3

Proof. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is $\mathsf{IND\text{-}qgCCA}$ secure.

Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{fM\text{-}IND\text{-}ouqCCA}$ security of the signcryption scheme SC with probability at least ϵ. Let $\mathsf{pk_{R^*}}$ and $\mathsf{pk_{S^*}}$ denote the receiver and sender identities involved in the challenge respectively. Let Forge denote the following event: $\exists$ an unsigncryption query made by $\mathcal{A}$ during its run, measuring query input of which yields with non-negligible probability, say μ, a tuple $(\mathsf{c}, \sigma, \mathsf{pk_{S^*}})$ such that $\mathcal{V}(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_{S^*}}) = 1$ and (c, σ) was not a result of challenge query or any previous signcryption oracle query on $\mathsf{pk_{R^*}}$. In other words, if Forge happens then $\mathcal{A}$ breaks the $\mathsf{pqsUF\text{-}CMA}$ security of the underlying signature scheme PKS. Note that,

$$\begin{aligned}\epsilon \leq \Pr[\mathcal{A} \text{ succeeds}] - \frac{1}{2} &= \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \\ &\leq \Pr[\mathsf{Forge}] + \left(\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2}\right) \\ \Longrightarrow \Pr[\mathsf{Forge}] \geq \frac{\epsilon}{2} &\text{ or } \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}.\end{aligned}$$

Case 1: $\Pr[\mathsf{Forge}] \geq \frac{\epsilon}{2}$. Let q_u be the total number of unsigncryption queries allowed to the adversary $\mathcal{A}$. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{pqsUF\text{-}CMA}$ security of PKS with probability at least $\epsilon{\cdot}\mu/(2{\cdot}q_u)$. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and sends $\mathsf{pk_{S^*}}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and gives $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ to $\mathcal{A}$. $\mathcal{B}_1$ also samples $i \overset{\text{U}}{\longleftarrow} [q_u]$ and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_1$. $\mathcal{B}_1$ samples $b \overset{\text{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b||\mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$ and makes a signature oracle query on $\mathsf{c}^*||\mathsf{pk_{R^*}}$. $\mathcal{CH}$ runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ and sends σ^* to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u}^* = (\mathsf{c}^*, \sigma^*)$ and sends the same to $\mathcal{A}$.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity $\mathsf{pk_R}$. $\mathcal{B}_1$ runs $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{m}||\mathsf{pk_{S^*}}, \mathsf{pk_R})$ and makes a signature oracle query on $\mathsf{c}||\mathsf{pk_R}$. $\mathcal{CH}$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{c}||\mathsf{pk_R}, \mathsf{sk_{S^*}})$ and sends σ to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u} = (\mathsf{c}, \sigma)$ and sends u to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}_1$ halts the execution of $\mathcal{A}$, measures the input register for the query, and outputs $(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma)$. Otherwise, $\mathcal{B}_1$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u}, \mathsf{pk_S}) = \begin{cases} \perp & \text{if } (\mathsf{u}, \mathsf{pk_S}) = (\mathsf{u}^*, \mathsf{pk_{S^*}}) \\ \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_1$. ($\mathcal{B}_1$ does nothing with b').

Analysis: $\mathcal{B}_1$ outputs forgery as described in the above procedure. From the definition of Forge, $\mathcal{B}_1$ breaks the pqsUF-CMA security of PKS with probability at least $\epsilon \cdot \mu/(2 \cdot q_u)$.

Case 2: $\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\text{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}$. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the IND-qgCCA security of PKE with advantage negligibly close to $\frac{\epsilon}{2}$. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and gives $\mathsf{pk_{R^*}}$ and $\mathsf{pk_{S^*}}$ to $\mathcal{A}$. $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ submits the message pair $(\mathsf{m_0}||\mathsf{pk_{S^*}}, \mathsf{m_1}||\mathsf{pk_{S^*}})$ to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b||\mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$ and sends c^* to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$, sets $\mathsf{u}^* := (\mathsf{c}^*, \sigma^*)$ and returns it to $\mathcal{A}$.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity $\mathsf{pk_R}$. $\mathcal{B}_2$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R})$, adds (m, u) to a list $\mathcal{L}$ (which is initially empty) and sends u to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_2$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of 1^{st} and 5^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m} \oplus g(\mathsf{c})\rangle$$

where

$$g(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True} \\ \mathcal{D}(\mathsf{c}, \mathsf{sk_{R^*}}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_2$. $\mathcal{B}_2$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta), g(\mathsf{c})\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m} & \text{if } (\mathsf{u}, \mathsf{pk_S}) \neq (\mathsf{u}^*, \mathsf{pk_{S^*}}) \wedge \mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True} \wedge (\mathsf{m}, \mathsf{u}) \in \mathcal{L} \\ [g(\mathsf{c})]_1 & \text{if } \mathcal{V}(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_S}) = 1 \wedge \mathsf{pk_S} = [g(\mathsf{c})]_2 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, g(\mathsf{c}), \mathsf{pk_S})$.

Note that the ancilla register is entangled with the 1^{st} four registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}_2$ again sends a decryption query consisting of 1^{st} and 5^{th} register to $\mathcal{CH}$ to unentangle the ancilla register. Finally, $\mathcal{B}_2$ obtains the state $\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends $\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_2$. $\mathcal{B}_2$ returns the same bit b' to $\mathcal{CH}$.

Analysis: We show that $\mathcal{B}_2$ simulates $\mathcal{A}$'s unsigncryption queries properly. The definition of $\overline{\mathsf{Forge}}$ says that for all unsigncryption queries made by $\mathcal{A}$, the probability that measuring query input yields a tuple $(\mathsf{c}, \sigma, \mathsf{pk_{S^*}})$ such that $\mathsf{pk_S} = \mathsf{pk_{S^*}}$, $\mathcal{V}(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_{S^*}}) = 1$ and (c, σ) was not a result of challenge query or any previous signcryption oracle query on $\mathsf{pk_{R^*}}$ is negligible. For a valid basis element $(\mathsf{u}, \mathsf{pk_S})$, $\mathcal{B}_2$ answers incorrectly (returns $\perp$) if u was not a result of any previous signcryption query and $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$. But $\mathcal{R}(\mathsf{c}, \mathsf{c}^*) = \mathsf{True}$ implies that for u to be valid, it is necessary that $\mathsf{pk_S} = \mathsf{pk_{S^*}}$. Since the total query magnitude of such signcryption texts is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. □

B.2 Proof of Theorem 6.4

Proof. Let $\mathsf{pk_{R^*}}$ and $\mathsf{pk_{S^*}}$ be the receiver and sender identities involved in the challenge respectively. We use the standard hybrid argument. Let $\mathbf{Game_0}$ denote the original $\mathsf{fM\text{-}sUF\text{-}ouqCMA}$ game of signcryption for adversary where all its queries are answered honestly. Let q_s be the number of signcryption oracle queries made by the adversary on $\mathsf{pk_{R^*}}$. Let $\mathsf{m}_1, \ldots, \mathsf{m}_{q_s}$ be the messages and $\mathsf{u}_1, \ldots, \mathsf{u}_{q_s}$ be corresponding signcryption texts. Next, we define the hybrid games $\mathbf{Game_j}$, $1 \le j \le q_s$. Each $\mathbf{Game_j}$ is identical to $\mathbf{Game_0}$ except for the following: for the 1^{st} j signcryption queries on $\mathsf{pk_{R^*}}$, $\mathbf{Game_j}$ returns a random encryption of 0^{ℓ_m}, i.e., $\mathsf{u}_j \longleftarrow \mathcal{E}(0^{\ell_m}; \mathsf{pk_{R^*}})$. Further, for a basis element $(\mathsf{u}, \mathsf{pk_{S^*}})$ of any unsigncryption query, if u is the result of any previous signcryption query $(\mathsf{m}, \mathsf{pk_{R^*}})$, then $\mathbf{Game_j}$ returns m. We denote $\mathsf{Succ}_j(\mathcal{A})$ to be the success probability of an adversary $\mathcal{A}$ in $\mathbf{Game_j}$. Note that $\mathbf{Game_{q_s}}$ answers all signcryption queries on $\mathsf{pk_{R^*}}$ incorrectly.

We make two claims:

1. For any $1 \le j \le q_s$, $\mathbf{Game_{j-1}}$ and $\mathbf{Game_j}$ are indistinguishable under the $\mathsf{IND\text{-}qCCA}$ property of the primitive encryption scheme PKE, i.e., for any quantum PPT adversary $\mathcal{A}$,
$$|\mathsf{Succ}_{j-1}(\mathcal{A}) - \mathsf{Succ}_j(\mathcal{A})| \le \mathsf{negl}(\lambda).$$
2. For any quantum PPT adversary $\mathcal{A}$, there is a quantum PPT algorithm $\mathcal{B}$ such that $\mathsf{Succ}_{q_s}(\mathcal{A}) \le \mathsf{Adv}^{\mathsf{pqwUF\text{-}CMA}}_{\mathcal{B},\mathsf{PKS}}(1^\lambda)$. Since PKS is $\mathsf{pqwUF\text{-}CMA}$ secure, $\mathsf{Succ}_{q_s}(\mathcal{A}) \le \mathsf{negl}(\lambda)$.

Combining claims 1 and 2, we get that $\mathsf{Succ}_0 \le (q_s + 1) \cdot \mathsf{negl}(\lambda)$ and hence the proof.

Proof of Claim 1. Let $\mathcal{A}$ be a quantum PPT adversary which can distinguish $\mathbf{Game_{j-1}}$ and $\mathbf{Game_j}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{IND\text{-}qCCA}$ security of PKE with advantage at least $\epsilon/2$. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_\mathcal{E}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_\mathcal{S}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ to $\mathcal{A}$. $\mathcal{B}_1$ simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Signcryption\ queries}$: Let $(\mathsf{m}, \mathsf{pk_R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk_R} \neq \mathsf{pk_{R^*}}$, $\mathcal{B}_1$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R})$ and sends u to $\mathcal{A}$. For the first $j-1$ queries on $\mathsf{pk_{R^*}}$, $\mathcal{B}_1$ answers with a random encryption of 0^{ℓ_m}. At the j^{th} query $(\mathsf{m}_j, \mathsf{pk_{R^*}})$, $\mathcal{B}_1$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}_j \| \mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$, prepares a challenge query $(\mathsf{m_0}, \mathsf{m_1}) \longleftarrow (\mathsf{m}_j \| \sigma \| \mathsf{pk_{S^*}}, 0^{\ell_m})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk_{R^*}})$ and sends c^* to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u} = \mathsf{c}^*$ and sends u to $\mathcal{A}$. After the j^{th} query on $\mathsf{pk_{R^*}}$, all the signcryption queries are answered properly. For all signcryption queries $(\mathsf{m}, \mathsf{pk_{R^*}})$, $\mathcal{B}_1$ also adds (m, u) to a list $\mathcal{L}$ (which is initially empty).

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u_{quant}} = \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_1$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle$. $\mathcal{B}_1$ then sends a decryption query consisting of 1^{st} and 4^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m} \oplus g(\mathsf{u})\rangle$$

where

$$g(\mathsf{u}) = \begin{cases} \perp & \text{if } \mathsf{u} = \mathsf{c}^* \\ \mathcal{D}(\mathsf{u}, \mathsf{sk_{R^*}}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_1$. $\mathcal{B}_1$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}, g(\mathsf{u})\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta), g(\mathsf{u})\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m}' & \text{if } \mathsf{pk_S} = \mathsf{pk_{S^*}} \wedge (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } \mathsf{u} = \mathsf{u}' \\ [g(\mathsf{u})]_1 & \text{if } \mathcal{V}([g(\mathsf{u})]_1 \| \mathsf{pk_{R^*}}, [g(\mathsf{u})]_2, \mathsf{pk_S}) = 1 \wedge \mathsf{pk_S} = [g(\mathsf{u})]_3 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, \mathsf{pk_S}, g(\mathsf{u}))$.

Note that the ancilla register is entangled with other registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}_1$ sends a decryption query consisting of 1^{st} and 4^{th} register to $\mathcal{CH}$. Finally, $\mathcal{B}_1$ obtains the state $\sum_{\mathsf{u}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends $\sum_{\mathsf{u}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

$\mathsf{Forgery\ and\ Analysis}$: $\mathcal{A}$ outputs a forgery u. $\mathcal{B}_1$ checks if $\forall (\mathsf{m}', \mathsf{u}') \in \mathcal{L}$, $\mathsf{u} \neq \mathsf{u}'$. Then it checks if u is a valid signcryption text by making a decryption oracle query and then verifying the validity of the signature. If the above conditions are true then $\mathcal{B}_1$ sends $b' = 0$, i.e., it guesses that u_j is the encryption of $\mathsf{m}_j \| \sigma \| \mathsf{pk_{S^*}}$. From the simulation procedure, it is clear that if u_j is indeed the encryption of $\mathsf{m}_j \| \sigma \| \mathsf{pk_{S^*}}$, then $\mathcal{A}$ was run in $\mathbf{Game_{j-1}}$ else it was run in $\mathbf{Game_j}$. From our assumption on the success probability of $\mathcal{A}$, we get that the $\mathcal{B}_1$ succeeds with advantage at least $\epsilon/2$ in breaking IND-qCCA security of PKE.

Proof of Claim 2. Let $\mathcal{A}$ be a quantum PPT adversary which succeeds in $\mathbf{Game_{q_s}}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the pqwUF-CMA security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and sends $\mathsf{pk_{S^*}}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$, forwards $\mathsf{pk_{S^*}}$, $\mathsf{pk_{R^*}}$ to $\mathcal{A}$ and simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Signcryption\ queries}$: Let $(\mathsf{m}, \mathsf{pk_R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk_R} \neq \mathsf{pk_{R^*}}$, $\mathcal{B}_2$ sends a signature query on $\mathsf{m}||\mathsf{pk_R}$ to $\mathcal{CH}$. $\mathcal{CH}$ then runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}||\mathsf{pk_R}, \mathsf{sk_{S^*}})$ and sends σ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs $\mathsf{u} \longleftarrow \mathcal{E}(\mathsf{m}||\sigma||\mathsf{pk_{S^*}}, \mathsf{pk_R})$ and sends u to $\mathcal{A}$. Otherwise, $\mathcal{B}_2$ answers with a random encryption of 0^{ℓ_m} on $\mathsf{pk_{R^*}}$. For all signcryption queries $(\mathsf{m}, \mathsf{pk_{R^*}})$, $\mathcal{B}_2$ also adds (m, u) to a list $\mathcal{L}$ (which is initially empty).

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta)\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m}' & \text{if } \mathsf{pk_S} = \mathsf{pk_{S^*}} \wedge (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } \mathsf{u} = \mathsf{u}' \\ \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, \mathsf{pk_S})$.

The resulting state is sent back to $\mathcal{A}$.

$\mathsf{Forgery}$: $\mathcal{A}$ outputs a forgery u. $\mathcal{B}_2$ runs $(\mathsf{m}||\sigma||\mathsf{pk_{S^*}}) \longleftarrow \mathcal{D}(\mathsf{u}, \mathsf{sk_{R^*}})$ and sends $(\mathsf{m}||\mathsf{pk_{R^*}}, \sigma)$ as forgery to $\mathcal{CH}$.

$\mathsf{Analysis}$: It is easy to see that $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries perfectly and it breaks the $\mathsf{pqwUF\text{-}CMA}$ security of PKS with advantage at least ϵ. □

B.3 Proof of Lemma 6.1

Proof. Let q_u be the total number of unsigncryption queries made by the adversary $\mathcal{A}$. Let δ_i be the sum of amplitudes squared of those basic elements $(\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p})$ involved in the i^{th} unsigncryption query for which the event $\mathsf{erConceal}$ is satisfied. Let $\delta = \sum_{i \in [q_u]} \delta_i$ be the sum of the probabilities. We claim that δ is negligible. Indeed, we can construct an adversary $\mathcal{B}_1$ which breaks the $\mathsf{qrConcealment}$ property of the underlying commitment scheme with advantage $(1-t) \cdot \delta/q_u^2$, for some negligible t defined later. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda), (\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ and $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}_1$ creates a list $\mathcal{L}$ which is initially empty. It also picks $i \overset{\mathrm{U}}{\longleftarrow} [q_u]$ and simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and sends m_b to the challenger $\mathcal{CH}$. $\mathcal{CH}$ then runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and sends $(\mathsf{com}^*, \mathsf{decom}^*)$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ and $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}^*||\mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$. It adds $(\mathsf{com}^*, \sigma^*)$ to $\mathcal{L}$ and sends the challenge signcryption text $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ to $\mathcal{A}$.

$\mathsf{Signcryption\ queries}$: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity $\mathsf{pk_R}$. $\mathcal{B}_1$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk_{S^*}}, \mathsf{pk_R})$ and sends u to $\mathcal{A}$. If $\mathsf{pk_R} = \mathsf{pk_{R^*}}$, $\mathcal{B}_1$ adds (com, σ) to $\mathcal{L}$.

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}_1$ halts the execution of $\mathcal{A}$, measures the input register for the query, and submits the corresponding com to $\mathcal{CH}$. Otherwise, $\mathcal{B}_1$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u},\mathsf{pk_S}) = \begin{cases} \perp & \text{if } (\mathsf{u},\mathsf{pk_S}) = (\mathsf{u}^*,\mathsf{pk_{S^*}}) \vee \mathsf{erConceal}[\mathsf{u},\mathsf{pk_S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u},\mathsf{sk_{R^*}},\mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_1$. ($\mathcal{B}_1$ does nothing with b').

Analysis: With probability δ/q_u^2, the measurement outcome $(\mathsf{u},\mathsf{pk_S})$ satisfies the event erConceal, i.e., $\mathsf{c} = \mathsf{c}^*$, $(\mathsf{com},\sigma) \in \mathcal{L}$, $\mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk_{R^*}})) \neq \perp$ and $\mathsf{pk_S} = \mathsf{pk_{S^*}}$. If $(\mathsf{com},\sigma) = (\mathsf{com}^*,\sigma^*)$, then $(\mathsf{u},\mathsf{pk_S}) = (\mathsf{u}^*,\mathsf{pk_{S^*}})$ and $\perp$ is returned to $\mathcal{A}$. W.l.o.g, assume that $(\mathsf{com},\sigma) \in \mathcal{L} \setminus \{(\mathsf{com}^*,\sigma^*)\}$. Since, (com,σ) and $(\mathsf{com}^*,\sigma^*)$ are two distinct entries in the list $\mathcal{L}$, they are generated using fresh random coins, in particular fresh random coins involved in the commitment part. So, $\Pr[\mathsf{com} = \mathsf{com}^*] \leq t$ - a negligible quantity, where $t = 4/|\mathcal{D}_{\mathsf{Com}}|$ and $\mathcal{D}_{\mathsf{Com}}$ is the domain of all possible com. Therefore, $\Pr[\mathsf{com} \neq \mathsf{com}^*] > (1-t)$ and $(\mathsf{com},\mathsf{com}^*,\mathsf{decom}^*)$ is a witness for breaking qrConcealment property if $(\mathsf{u},\mathsf{pk_S})$. The advantage of breaking qrConcealment property is at least $(1-t)\cdot\delta/q_u^2$, a contradiction. So, δ is negligible. Since the total query magnitude of signcryption texts satisfying erConceal is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. □

B.4 Proof of Lemma 6.2

Proof. Let q_u be the total number of unsigncryption queries made by the adversary $\mathcal{A}$. Let δ_i be the sum of amplitudes squared of those basic elements $(\mathsf{u},\mathsf{pk_S},\mathsf{m_p})$ involved in the i^{th} unsigncryption query for which the event Forge is satisfied. Let $\delta = \sum_{i\in[q_u]}\delta_i$ be the sum of the probabilities. We claim that δ is negligible. Indeed, we can construct an adversary $\mathcal{B}_2$ which breaks the pqsUF-CMA security of PKS with advantage δ/q_u^2. $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries in the following way:

Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ first runs $(\mathsf{pk_{S^*}},\mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and gives $\mathsf{pk_{S^*}}$to $\mathcal{B}_2$. $\mathcal{B}_2$ runs the setup of the commitment scheme, $(\mathsf{pk_{R^*}},\mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and forwards the public commitment key $\mathcal{CK}$, $\mathsf{pk_{S^*}}$ and $\mathsf{pk_{R^*}}$ to $\mathcal{A}$. $\mathcal{B}_2$ also samples $i \overset{\mathrm{U}}{\longleftarrow} [q_u]$, creates a list $\mathcal{L}$ (initially empty) and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_2$. $\mathcal{B}_2$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $(\mathsf{com}^*,\mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and sends a signature query on $\mathsf{com}^*||\mathsf{pk_{R^*}}$ to $\mathcal{CH}$. $\mathcal{CH}$ runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}},\mathsf{sk_{S^*}})$ and returns σ^* to $\mathcal{B}_2$. $\mathcal{B}_2$ executes $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}^*||\mathsf{pk_{S^*}},\mathsf{pk_{R^*}})$, adds $(\mathsf{com}^*,\sigma^*)$ to $\mathcal{L}$ and returns $\mathsf{u}^* := (\mathsf{com}^*,\sigma^*,\mathsf{c}^*)$ to $\mathcal{A}$.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity $\mathsf{pk_R}$. $\mathcal{B}_2$ runs $(\mathsf{com},\mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$ and sends a signature query on $\mathsf{com}||\mathsf{pk_R}$ to $\mathcal{CH}$. $\mathcal{CH}$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk_R},\mathsf{sk_{S^*}})$ and returns σ to $\mathcal{B}_2$. $\mathcal{B}_2$ executes $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}||\mathsf{pk_{S^*}},\mathsf{pk_R})$ and returns $\mathsf{u} := (\mathsf{com},\sigma,\mathsf{c})$ to $\mathcal{A}$. If $\mathsf{pk_R} = \mathsf{pk_{R^*}}$, $\mathcal{B}_2$ adds (com,σ) to $\mathcal{L}$.

Unsigncryption queries: Let $\mathsf{u_{quant}} = \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}_2$ halts the execution of $\mathcal{A}$, measures the input register for the query, and outputs a forgery $(\mathsf{com}||\mathsf{pk_{R^*}},\sigma)$. Otherwise, $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p} \oplus f(\mathsf{u},\mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u},\mathsf{pk_S}) = \begin{cases} \perp & \text{if } (\mathsf{u},\mathsf{pk_S}) = (\mathsf{u}^*,\mathsf{pk_{S^*}}) \vee \mathsf{erConceal}[\mathsf{u},\mathsf{pk_S}] = \mathsf{True} \vee \mathsf{Forge}[\mathsf{u},\mathsf{pk_S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u},\mathsf{sk_{R^*}},\mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_2$. ($\mathcal{B}_2$ does nothing with b').

$\mathsf{Analysis}$: The event Forge implies that probability that $(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma)$ satisfies $\mathcal{V}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_{\mathsf{S}^*}) = 1$ is at least δ/q_u^2. The $\mathsf{pqsUF\text{-}CMA}$ property of PKS shows that δ is negligible. Since the total query magnitude of signcryption texts satisfying Forge is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. □

B.5 Proof of Lemma 6.3

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which can distinguish $\mathbf{Game_0}$ and $\mathbf{Game_1}$ with probability ϵ. We construct a quantum PPT algorithm $\mathcal{B}_3$ which breaks the $\mathsf{IND\text{-}qCCA}$ security of PKE with probability $\epsilon/2$. Let $\mathcal{CH}$ be the challenger for the primitive encryption scheme PKE which runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{B}_3$. $\mathcal{B}_3$ runs the setup algorithm of the commitment scheme, $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$, and forwards the public commitment key $\mathcal{CK}$, $\mathsf{pk}_{\mathsf{S}^*}$ and $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{A}$. $\mathcal{B}_3$ creates a list $\mathcal{L}$ and simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_3$. $\mathcal{B}_3$ then samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$. Then it samples decom_r randomly from the decommitment space, sets $(\mathsf{decom}_0||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_1||\mathsf{pk}_{\mathsf{S}^*}) \longleftarrow (\mathsf{decom}^*||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $\beta \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_\beta||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and sends it to $\mathcal{B}_3$. The simulator runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, sets $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$, adds $(\mathsf{com}^*, \sigma^*)$ to $\mathcal{L}$ and returns it to $\mathcal{A}$.

$\mathsf{Signcryption\ queries}$: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity pk_R. $\mathcal{B}_3$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} = \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_3$ adds (com, σ) to $\mathcal{L}$.

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_3$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}_3$ then sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m} \oplus g(\mathsf{c})\rangle$$

where

$$g(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathsf{c} = \mathsf{c}^* \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_3$. $\mathcal{B}_3$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta), g(\mathsf{c})\rangle$$

where

$$f(\Delta) = \begin{cases} \perp & \text{if } (\mathsf{u}, \mathsf{pk}_\mathsf{S}) = (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*}) \lor \mathsf{erConceal}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True} \lor \mathsf{Forge}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True} \\ \mathsf{Open}(\mathsf{com}, [g(\mathsf{c})]_1) & \text{if } \mathsf{c} \neq \mathsf{c}^* \land \mathcal{V}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_\mathsf{S}) = 1 \land \mathsf{pk}_\mathsf{S} = [g(\mathsf{c})]_2 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, \mathsf{pk}_\mathsf{S}, g(\mathsf{c}))$.

Note that the ancilla register is entangled with other registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the EtU technique to unentangle the ancilla register: $\mathcal{B}_3$ sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. Finally, $\mathcal{B}_3$ obtains the state $\sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \left|\mathsf{com},\sigma,\mathsf{c},\mathsf{pk_S},\mathsf{m_p} \oplus f(\Delta)\right\rangle \otimes \left|0^{\ell_m}\right\rangle$. It discards the last register and sends $\sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \left|\mathsf{u},\mathsf{pk_S},\mathsf{m_p} \oplus f(\Delta)\right\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_3$. If $b = b'$, $\mathcal{B}_3$ replies $\beta' = 0$ else returns $\beta' = 1$.

Analysis: The only difference between $\mathbf{Game_0}$ and $\mathbf{Game_1}$ is the construction of the challenge signcryption text. We will first show that all the unsigncryption queries are handled properly. It suffices to show that each of the basis element $\left|\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\right\rangle$ is handled properly. By definition, a query $\left|\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\right\rangle$ is legitimate if $(\mathsf{u},\mathsf{pk_S}) \neq (\mathsf{u}^*,\mathsf{pk_{S^*}})$. We consider the following cases:

1. $\mathsf{Forge}[\mathsf{u},\mathsf{pk_S}] = \mathsf{True}$
2. $\mathsf{Forge}[\mathsf{u},\mathsf{pk_S}] = \mathsf{False} \land \mathsf{c} \neq \mathsf{c}^*$
3. $\mathsf{Forge}[\mathsf{u},\mathsf{pk_S}] = \mathsf{False} \land \mathsf{c} = \mathsf{c}^*$

In case 1, by definition of $\mathbf{Game_0}$ and $\mathbf{Game_1}$, the adversary is returned $\perp$ if Forge happens. In case 2, $\mathcal{B}_3$ answers correctly by making a decryption query to $\mathcal{CH}$. Only case 3 is left to analyze. In simulation, $\mathcal{A}$ is given $\perp$ for this case. We divide this case into two sub cases: (a_1) $\mathcal{V}(\mathsf{com}||\mathsf{pk_{R^*}},\sigma,\mathsf{pk_{S^*}}) = 0 \lor \mathsf{pk_S} \neq \mathsf{pk_{S^*}}$, ($\mathrm{a}_2$) $(\mathsf{com},\sigma) \in \mathcal{L} \land \mathcal{V}(\mathsf{com}||\mathsf{pk_{R^*}},\sigma,\mathsf{pk_{S^*}}) = 1 \land \mathsf{pk_S} = \mathsf{pk_{S^*}}$. It is easy to see that the sub case (a_1) correspond to invalid signcryption texts. If $\mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk_{R^*}})) = \perp$, then $\mathcal{A}$ will get $\perp$ as a reply. W.l.o.g, assume that $\mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk_{R^*}})) \neq \perp$. Now, case ($\mathrm{a}_2$) implies that $(\mathsf{u},\mathsf{pk_S})$ will satisfy the event $\mathsf{erConceal}$. So, $\mathcal{A}$ will get $\perp$ as response according to the definition of $\mathbf{Game}_{\widetilde{\mathbf{Real}}}$. From the challenge phase, it is straightforward that the challenge signcryption text is properly distributed. Therefore, all the answers to the oracle queries are perfectly simulated. The advantage of $\mathcal{B}_3$ in breaking $\mathsf{IND\text{-}qCCA}$ security of the primitive encryption scheme PKE is given by

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IND-qCCA}}_{\mathcal{B},\mathsf{PKE}}(1^\lambda) &= \left|\Pr\left[\beta = \beta'\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\beta = 0, \beta' = 0\right] + \Pr\left[\beta = 1, \beta' = 1\right] - \frac{1}{2}\right| \\
&= \left|\frac{1}{2}\Pr\left[\beta' = 0|\beta = 0\right] + \frac{1}{2}\Pr\left[\beta' = 1|\beta = 1\right] - \frac{1}{2}\right| \\
&= \left|\frac{1}{2}\Pr\left[\beta' = 0|\beta = 0\right] - \frac{1}{2}\Pr\left[\beta' = 0|\beta = 1\right]\right| \\
&= \left|\frac{1}{2}\Pr\left[b = b'|\beta = 0\right] - \frac{1}{2}\Pr\left[b = b'|\beta = 1\right]\right| \\
&= \frac{1}{2}\left|\mathsf{Adv}^{\mathbf{Game_0}}_{\mathcal{A},\mathsf{SC}}(1^\lambda) - \mathsf{Adv}^{\mathbf{Game_1}}_{\mathcal{A},\mathsf{SC}}(1^\lambda)\right|.
\end{aligned}$$

□

B.6 Proof of Lemma 6.4

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which has advantage ϵ in $\mathbf{Game_1}$. We construct a quantum PPT algorithm $\mathcal{B}_4$ which breaks the $\mathsf{qHiding}$ property of C with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}_4$. $\mathcal{B}_4$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda), (\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$, $\mathsf{pk}_{\mathsf{S}^*}$ and $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}_4$ creates a list $\mathcal{L}$ (initially empty) and simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ submits two equal length messages m_0 and m_1 to $\mathcal{B}_4$. $\mathcal{B}_4$ submits the same message pair $(\mathsf{m}_0, \mathsf{m}_1)$ to the challenger $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and sends com^* to $\mathcal{B}_4$. $\mathcal{B}_4$ then runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^* || \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_r || \mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$, where decom_r is randomly sampled from the decommitment space. $\mathcal{B}_4$ adds $(\mathsf{com}^*, \sigma^*)$ to $\mathcal{L}$ and sends the challenge signcryption text $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ to $\mathcal{A}$.

Signcryption queries: Let m be any signcryption query made by $\mathcal{A}$ corresponding to receiver identity pk_R. $\mathcal{B}_4$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} = \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_4$ adds (com, σ) to $\mathcal{L}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_4$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u}, \mathsf{pk}_\mathsf{S})\rangle$$

where

$$f(\mathsf{u}, \mathsf{pk}_\mathsf{S}) = \begin{cases} \perp & \text{if } (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*}) = (\mathsf{u}, \mathsf{pk}_\mathsf{S}) \vee \mathsf{erConceal}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True} \vee \mathsf{Forge}[(\mathsf{u}, \mathsf{pk}_\mathsf{S})] = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_\mathsf{S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}_4$. $\mathcal{B}_4$ returns the same bit b' to $\mathcal{CH}$.

Analysis: It is easy to see that $\mathcal{B}_4$ simulates $\mathcal{A}$'s queries perfectly and it breaks the $\mathsf{qHiding}$ property of C with advantage at least ϵ. □

B.7 Proof of Lemma 6.5

Proof. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the $\mathsf{pqsUF\text{-}CMA}$ security of PKS with probability at least $\frac{\epsilon}{2}$. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$, the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$, $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ to $\mathcal{A}$.

Signcryption queries: Let $(\mathsf{m}, \mathsf{pk}_\mathsf{R})$ be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_1$ runs $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$ and sends a signature oracle query on $\mathsf{com} || \mathsf{pk}_\mathsf{R}$ to $\mathcal{CH}$. $\mathcal{CH}$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{com} || \mathsf{pk}_\mathsf{R}, \mathsf{sk}_{\mathsf{S}^*})$ and sends σ to $\mathcal{B}_1$. $\mathcal{B}_1$ then runs $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom} || \mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$, sets $\mathsf{u} := (\mathsf{com}, \sigma, \mathsf{c})$ and sends u to $\mathcal{A}$.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_1$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus \mathcal{US}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_\mathsf{S})\rangle$$

The resulting state is sent back to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs a forgery $\widetilde{\mathsf{u}} = (\widetilde{\mathsf{com}}, \widetilde{\sigma}, \widetilde{\mathsf{c}})$. $\mathcal{B}_1$ forwards $(\widetilde{\mathsf{com}} || \mathsf{pk}_{\mathsf{R}^*}, \widetilde{\sigma})$ as forgery to $\mathcal{CH}$.

Analysis: It is clear that $\mathcal{B}_1$ breaks $\mathsf{pqsUF\text{-}CMA}$ security of PKS with probability at least $\frac{\epsilon}{2}$. □

B.8 Proof of Lemma 6.6

Proof. Let q_s and q_u be the total number of signcryption and unsigncryption queries made by the adversary $\mathcal{A}$ respectively. Let δ_i be the sum of amplitudes squared of those basic elements $(\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p})$ involved in the i^{th} unsigncryption query for which the event $\mathsf{srConceal}$ is satisfied. Let $\delta = \sum_{i \in [q_u]} \delta_i$ be the sum of the probabilities. We claim that δ is negligible. Indeed, we can construct an adversary $\mathcal{B}_2$ which breaks the $\mathsf{qrConcealment}$ property of the underlying commitment scheme with advantage $(\delta \cdot i_s)/(q_s^2 \cdot q_u^2)$, where i_s is as defined in the proof sketch of Theorem 6.6. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda), (\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ and $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}_2$ creates a list $\mathcal{L}$ which is initially empty. It also picks $i \overset{\mathrm{U}}{\longleftarrow} [q_u]$ and $j_* \overset{\mathrm{U}}{\longleftarrow} [q_s]$ and simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: Let m_j be the j^{th} signcryption query made by $\mathcal{A}$ corresponding to receiver identity $\mathsf{pk_R}$. Then the j^{th} query is handled un the following way:

1. $(j = j_*)$: $\mathcal{B}_2$ forwards m_j to $\mathcal{CH}$. $\mathcal{CH}$ runs $(\mathsf{com}_j, \mathsf{decom}_j) \longleftarrow \mathsf{Commit}(\mathsf{m}_j)$ and sends $(\mathsf{com}_j, \mathsf{decom}_j)$ to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $\sigma_j \longleftarrow \mathcal{S}(\mathsf{com}_j \| \mathsf{pk_R}, \mathsf{sk_{S^*}})$ and $\mathsf{c}_j \longleftarrow \mathcal{E}(\mathsf{decom}_j \| \mathsf{pk_{S^*}}, \mathsf{pk_R})$ and returns $\mathsf{u}_j = (\mathsf{com}_j, \sigma_j, \mathsf{c}_j)$ to $\mathcal{A}$.

2. $(j \neq j_*)$: $\mathcal{B}_2$ runs $\mathsf{u}_j \longleftarrow \mathcal{SC}(\mathsf{m}_j, \mathsf{sk_{S^*}}, \mathsf{pk_R})$ and sends u_j to $\mathcal{A}$.

If $\mathsf{pk_R} = \mathsf{pk_{R^*}}$, $\mathcal{B}_2$ adds $(\mathsf{com}_j, \sigma_j)$ to $\mathcal{L}$.

Unsigncryption queries: Let $\mathsf{u_{quant}} = \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query with $j_* \leq i_s$, $\mathcal{B}_2$ halts the execution of $\mathcal{A}$, measures the input register for the query, and submits the corresponding com to $\mathcal{CH}$. If $j_* > i_s$, then $\mathcal{B}_2$ aborts. Otherwise, $\mathcal{B}_2$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\mathsf{u}, \mathsf{pk_S})\rangle$$

where

$$f(\mathsf{u}, \mathsf{pk_S}) = \begin{cases} \perp & \text{if } \mathsf{srConceal}[\mathsf{u}, \mathsf{pk_S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S}) & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs a forgery $\widetilde{u}$. ($\mathcal{B}_2$ does nothing with $\widetilde{u}$).

Analysis: With probability $\delta/(q_s \cdot q_u^2)$, the measurement outcome u satisfies the following: $\mathsf{c} = \mathsf{c}_j$, $\mathsf{com} \neq \mathsf{com}_j$ and $\mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk_{R^*}})) \neq \perp$. Therefore, $(\mathsf{com}, \mathsf{com}_j, \mathsf{decom}_j)$ is a witness for breaking $\mathsf{qrConcealment}$ property if $(\mathsf{u}, \mathsf{pk_S})$. The advantage of breaking $\mathsf{qrConcealment}$ property is $(\delta \cdot i_s)/(q_s^2 \cdot q_u^2)$, a contradiction. So, δ is negligible. Since the total query magnitude of signcryption texts satisfying $\mathsf{srConceal}$ is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. □

B.9 Proof of Lemma 6.7

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which can distinguish $\mathbf{Game_{j-1}}$ and $\mathbf{Game_j}$ with probability ϵ'. We construct a quantum PPT algorithm $\mathcal{B}_3$ which breaks the $\mathsf{IND\text{-}qCCA}$ security of PKE with advantage at least $\epsilon'/2$. Let $\mathcal{CH}$ be the challenger for the encryption scheme PKE. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{B}_3$. $\mathcal{B}_3$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$, the setup algorithm of the commitment scheme and forwards the public commitment key $\mathcal{CK}$, $\mathsf{pk}_{\mathsf{S}^*}$ and $\mathsf{pk}_{\mathsf{R}^*}$ to $\mathcal{A}$. $\mathcal{B}_3$ creates a list $\mathcal{L}$ (initially empty) simulates $\mathcal{A}$'s queries as described below.

Signcryption queries: Let $(\mathsf{m}, \mathsf{pk}_\mathsf{R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} \neq \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_3$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. Otherwise, $\mathcal{B}_3$ does the following:

- (First $j-1$ queries). $\mathcal{B}_3$ runs $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$, $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*}; \mathsf{pk}_{\mathsf{R}^*})$, where decom_r is sampled uniformly from the decommitment space. $\mathcal{B}_3$ sets $\mathsf{u} = (\mathsf{com}, \sigma, \mathsf{c})$, adds (m, u) to $\mathcal{L}$ and sends u to $\mathcal{A}$.

- (j^{th} query). $\mathcal{B}_3$ first runs $(\mathsf{com}_j, \mathsf{decom}_j) \longleftarrow \mathsf{Commit}(\mathsf{m}_j)$. Then it samples decom_r randomly from the decommitment space, sets $(\mathsf{decom}_0||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_1||\mathsf{pk}_{\mathsf{S}^*}) \longleftarrow (\mathsf{decom}_j||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\text{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_b||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and sends it to $\mathcal{B}_3$. $\mathcal{B}_3$ runs $\sigma_j \longleftarrow \mathcal{S}(\mathsf{com}_j||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, sets $\mathsf{u}^* := (\mathsf{com}_j, \sigma_j, \mathsf{c}^*)$ and returns it to $\mathcal{A}$. $\mathcal{B}_3$ also adds $(\mathsf{m}_j, \mathsf{u}^*)$ to $\mathcal{L}$.

- (Last $(q_s - j)$ queries). All the signcryption queries are answered properly.

Unsigncryption queries: Let $\mathsf{u}_{\mathsf{quant}} = \sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_3$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}_3$ then sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

$$\sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m} \oplus g(\mathsf{c})\rangle$$

where

$$g(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathsf{c} = \mathsf{c}^* \\ \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*}) & \text{otherwise.} \end{cases}$$

$\mathcal{CH}$ sends the resulting state to $\mathcal{B}_3$. $\mathcal{B}_3$ then applies the following transformation on the obtained state

$$\sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, g(\mathsf{c})\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta), g(\mathsf{c})\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m}' & \text{if } \exists (\mathsf{m}', \mathsf{u}') \in \mathcal{L} \text{ s.t. } (\mathsf{com}, \mathsf{c}, \mathsf{pk}_\mathsf{S}) = (\mathsf{com}', \mathsf{c}', \mathsf{pk}_{\mathsf{S}^*}) \wedge \mathcal{V}(\mathsf{com}'||\mathsf{pk}_{\mathsf{R}^*}, \sigma', \mathsf{pk}_\mathsf{S}) = 1 \\ \perp & \text{if } \mathsf{srConceal}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True} \\ \mathsf{Open}(\mathsf{com}, [g(\mathsf{c})]_1) & \text{if } \mathcal{V}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_\mathsf{S}) = 1 \wedge \mathsf{pk}_\mathsf{S} = [g(\mathsf{c})]_2 \\ \perp & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u}, \mathsf{pk}_\mathsf{S}, g(\mathsf{c}))$.

Note that the ancilla register is entangled with other registers. To perfectly simulate $\mathcal{A}$'s view, simulator can use the *EtU* technique to unentangle the ancilla register: $\mathcal{B}_3$ sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. Finally, $\mathcal{B}_3$ obtains the state $\sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle \otimes |0^{\ell_m}\rangle$. It discards the last register and sends $\sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

$\mathsf{Forgery}$: $\mathcal{A}$ outputs a forgery $\widetilde{\mathsf{u}}$. $\mathcal{B}_3$ checks if $\widetilde{\mathsf{u}}$ is a valid signcryption text by making a decryption oracle query and then verifying the validity of the signature. Suppose, it is a valid signcryption text and $\widetilde{\mathsf{m}}$ is the underlying plaintext. $\mathcal{B}_3$ then checks if $\forall(\widetilde{\mathsf{m}},\widetilde{\mathsf{u}}) \notin \mathcal{L}$. If the above conditions are true then $\mathcal{B}_3$ sends $b' = 0$, i.e., it guesses that c^* is the encryption of $\mathsf{decom}_j||\mathsf{pk}_{\mathsf{S}^*}$, else sends $b' = 1$.

$\mathsf{Analysis}$: First note that the sole purpose of introducing the event $\mathsf{srConceal}$ is to handle unsigncryption queries on $(\mathsf{u},\mathsf{pk}_\mathsf{S})$ whose ciphertext part is c^*, because $\mathcal{B}_3$ will get $\bot$ against c^* from the decryption oracle. This case will come under the 2nd condition of the evaluation of $f(\Delta)$. Essentially, we give a justification of $f(\Delta) = \bot$ when $\mathsf{srConceal}[\mathsf{u},\mathsf{pk}_\mathsf{S}] = \mathsf{True}$. Now, $\mathsf{srConceal}[\mathsf{u},\mathsf{pk}_\mathsf{S}] = \mathsf{True}$ implies that $\exists j \in [i_s]$ such that $\mathsf{c} = \mathsf{c}_j$, $\mathsf{com} \neq \mathsf{com}_j$ and $\mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk}_{\mathsf{R}^*})) \neq \bot$, where $\mathsf{u}_j = (\mathsf{com}_j,\sigma_j,\mathsf{c}_j)$ is the reply of j^{th} signcryption query (including challenge). If u_j is a proper signcryption text, then $\mathcal{A}$ will get $\bot$ as a response according to the definition of $\mathbf{Game_{Real}}$. Otherwise, c_j will be the ciphertext of a randomly chosen decommitment decom_r, and therefore $\mathcal{A}$ gets $\mathsf{Open}(\mathsf{com}_j,\mathsf{decom}_r) = \bot$ as a response.

From the simulation procedure, it is clear that $\mathcal{B}_3$ simulates unsigncryption queries correctly. Also, if c^* is indeed the encryption of $\mathsf{decom}_j||\mathsf{pk}_{\mathsf{S}^*}$, then $\mathcal{A}$ was run in $\mathbf{Game_{j-1}}$ else it was run in $\mathbf{Game_j}$. From our assumption on the success probability of $\mathcal{A}$, we get that the $\mathcal{B}_3$ succeeds with advantage at least $\epsilon'/2$ in breaking IND-qCCA security of PKE. □

B.10 Proof of Lemma 6.8

Proof. Let $\mathcal{A}$ be a quantum PPT adversary which can succeed in $\mathbf{Game_{q_s}}$ with probability ϵ'. We construct a quantum PPT algorithm $\mathcal{B}_4$ which breaks the qfBinder property of C with advantage at least $\frac{\epsilon'}{2}$. Let $\mathcal{CH}$ be the challenger for the commitment scheme C. $\mathcal{CH}$ first runs the setup algorithm of the commitment scheme and gives the public commitment key $\mathcal{CK}$ to $\mathcal{B}_4$. Then, $\mathcal{B}_4$ runs $(\mathsf{pk}_{\mathsf{S}^*},\mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_\mathcal{S}(1^\lambda)$, $(\mathsf{pk}_{\mathsf{R}^*},\mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_\mathcal{E}(1^\lambda)$ and returns commitment key $\mathcal{CK}$, $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ to the adversary $\mathcal{A}$. $\mathcal{B}_4$ also creates a list $\mathcal{L}$ (initially empty), samples $i \overset{\mathrm{U}}{\longleftarrow} [q_s]$ and simulates $\mathcal{A}$'s queries as described below.

$\mathsf{Signcryption\ queries}$: Let $(\mathsf{m},\mathsf{pk}_\mathsf{R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} \neq \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_4$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m},\mathsf{sk}_{\mathsf{S}^*},\mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. If it is the i^{th} signcryption query on $\mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_4$ forwards m to $\mathcal{CH}$. $\mathcal{CH}$ then runs $(\mathsf{com},\mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$ and sends com to $\mathcal{B}_4$. $\mathcal{B}_4$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk}_{\mathsf{R}^*},\mathsf{sk}_{\mathsf{S}^*})$ and $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*},\mathsf{pk}_{\mathsf{R}^*})$, where decom_r is uniformly sampled from the decommitment space. $\mathcal{B}_4$ then sets $\mathsf{u} = (\mathsf{com},\sigma,\mathsf{c})$, adds (m,u) to $\mathcal{L}$ and sends u to $\mathcal{A}$. Otherwise, $\mathcal{B}_4$ runs $(\mathsf{com},\mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$, $\sigma \longleftarrow \mathcal{S}(\mathsf{com}||\mathsf{pk}_\mathsf{R},\mathsf{sk}_{\mathsf{S}^*})$ and $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}_r||\mathsf{pk}_{\mathsf{S}^*},\mathsf{pk}_{\mathsf{R}^*})$, where decom_r is uniformly sampled from the decommitment space. $\mathcal{B}_4$ then sets $\mathsf{u} = (\mathsf{com},\sigma,\mathsf{c})$, adds (m,u) to $\mathcal{L}$ and sends u to $\mathcal{A}$.

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. $\mathcal{B}_4$ applies the following unitary transformation

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle$$

where

$$f(\Delta) = \begin{cases} \mathsf{m}' & \text{if } \exists(\mathsf{m}',\mathsf{u}') \in \mathcal{L} \text{ s.t. } (\mathsf{com},\mathsf{c},\mathsf{pk}_\mathsf{S}) = (\mathsf{com}',\mathsf{c}',\mathsf{pk}_{\mathsf{S}^*}) \wedge \mathcal{V}(\mathsf{com}'||\mathsf{pk}_{\mathsf{R}^*},\sigma',\mathsf{pk}_\mathsf{S}) = 1 \\ \bot & \text{if } \mathsf{srConceal}[\mathsf{u},\mathsf{pk}_\mathsf{S}] = \mathsf{True} \\ \mathcal{US}(\mathsf{u},\mathsf{sk}_{\mathsf{R}^*},\mathsf{pk}_\mathsf{S}) & \text{otherwise,} \end{cases}$$

and $\Delta = (\mathsf{u},\mathsf{pk}_\mathsf{S})$.

The resulting state is sent back to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs a forgery $\widetilde{\mathsf{u}}$. $\mathcal{B}_4$ forwards decom to $\mathcal{CH}$.

Analysis: It is clear that $\mathcal{B}_4$ breaks qfBinder property of C with probability at least $\epsilon'/(2 \cdot q_s)$. □