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 studies signcryption of classical data in the quantum setting. Essentially, 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 ($\mathcal{C}t\mathcal{E}\&\mathcal{S}$). For doing that we define the confidentiality and authenticity of signcryption for classical data both in insider and outsider models against quantum adversaries. In the insider model, we show that the quantum variants of the classical results hold in the quantum setting. However, for arguing authenticity in outsider model of $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms, 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. Finally, we briefly discuss concrete instantiations in various paradigms utilizing 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, AGM18b]. 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 ($(\mathsf{(w/s)UF\text{-}CMA})$) and for encryption we use the standard definitions of indistinguishability under chosen plaintext attack ($\mathsf{IND\text{-}CPA}$) and indistinguishability under chosen ciphertext attack ($\mathsf{IND\text{-}CCA}$). We also take recourse to the notion of indistinguishability under generalized chosen ciphertext attack ($\mathsf{IND\text{-}gCCA}$)[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 $\mathsf{Hiding}, \mathsf{Binding}$ and $\mathsf{rConcealment}$[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 $\mathsf{sUF\text{-}CMA}$ and $\mathsf{IND\text{-}gCCA}$ security of the primitive signature scheme and encryption scheme respectively in the insider model. The $\mathcal{S}t\mathcal{E}$ paradigm preserves $\mathsf{wUF\text{-}CMA}$ and $\mathsf{IND\text{-}CCA}$ 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 $\mathsf{wUF\text{-}CMA}$ security and $\mathsf{IND\text{-}gCCA}$ security of the primitive signature scheme and encryption scheme respectively. In the two-user outsider model, it was shown in [ADR02] 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.

Key-Idea. For simplicity, let's consider two-user model, where there are only two users, one receiver and one sender. An adversary $\mathcal{A}$ may ask superposition queries to signcryption ($\mathcal{SC}$) (resp. unsigncryption ($\mathcal{US}$)) oracle by sending two registers $|\mathsf{m}, \mathsf{u_p}\rangle$ (resp. $|\mathsf{u}, \mathsf{m_p}\rangle$) for input and output, where the output register $\mathsf{u_p}$ (resp. $\mathsf{m_p}$) is initialized (possibly with arbitrary value) by $\mathcal{A}$. As a response, $\mathcal{A}$'s registers are updated with $|\mathsf{u}, \mathsf{m_p} \oplus \mathcal{US}(\mathsf{u})\rangle$ and $|\mathsf{m}, \mathsf{u_p} \oplus \mathcal{SC}(\mathsf{m})\rangle$ for unsigncryption and signcryption respectively. Depending on the underlying security model, a simulator $\mathcal{B}$ has to answer superposition queries to signcryption oracle or

[1] $\mathsf{IND\text{-}gCCA}$ notion is a generalization of $\mathsf{IND\text{-}CCA}$ 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, $\mathsf{rConcealment}$ ensures that given a commitment pair $(\mathsf{com}, \mathsf{decom})$ corresponding to a message m, it is difficult to produce $\mathsf{com}' \neq \mathsf{com}$ such that the pair $(\mathsf{com}', \mathsf{decom})$ opens to a valid message [NP16].

unsigncryption oracle or both. Typically, for simulating those queries, $\mathcal{B}$ gets a help of an external oracle, e.g., signature, decryption. In general, for answering the queries, $\mathcal{B}$ may need some auxiliary registers to store intermediate values which are either computed by the simulator itself or obtained from its external oracle. The internal auxiliary registers may get entangled with adversary's registers. If so, then before transferring the query registers to the adversary, the internal registers need to be uncomputed to avoid entangled attack [GHS16, Zha19a].

Zhandry [Zha19a] introduced an important technique, called *compressed oracle* which helps on-the-fly simulation in the context of QROM. This technique is applicable in many situations where the simulation would otherwise fail due to the no-cloning theorem. Based on the compressed oracle technique, Chevalier et al. [CEV20] recently proposed a generic framework that supports answering inverse (e.g., decryption) queries for probabilistic functions f. Briefly in this technique, when $\mathcal{A}$'s queries (x, z) are considered in the Fourier basis, the query information are recorded in the oracle's registers. While going back to the standard basis by applying quantum Fourier transformation on the output register of $\mathcal{A}$ and oracle, the legitimate answers are written to $\mathcal{A}$'s output register, and the oracle's registers are updated with the value $(x, r, f(x, r))$. This ensures recording a certain type of queries (e.g., encryption) of $\mathcal{A}$ and thereby enabling on-the-fly simulation of $\mathcal{A}$'s other type of queries (e.g., decryption). This whole process is oblivious to the adversary. Besides uncomputing registers, we rigorously use compressed oracle related result of [CEV20] to argue the quantum security of classical data in three well-known paradigms of signcryption.

In the insider unforgeability (resp. confidentiality) model, $\mathcal{A}$ is given superposition access to signcryption (resp. unsigncryption) oracle. For answering signcryption queries, $\mathcal{B}$ computes ciphertext or signature or some other values (e.g., components related to commitment) internally. If they are not part of the final output, then $\mathcal{B}$ has to uncompute those intermediate components either by making queries to its external signature oracle or by running algorithms (e.g., encryption, commit) locally using the same randomness as used to compute those intermediate components. In the former case, we face some problem due to randomized nature of the signature oracle. Even when, it is deterministic, $\mathcal{B}$ has to ask $2q$ signature queries when the adversary makes q signcryption queries. This creates a problem as the simulator has to submit $2q + 1$ message-signature pairs in one-more unforgeability model [BZ13]. This type of difficulty arises in the insider model of $\mathcal{S}t\mathcal{E}$ paradigm. However, if we simulate encryption using Type-2 unitary [GHS16], then we can resolve the above problem. Basically, this unitary will replace the contents (m and σ) by the output ciphertext. But, then it will create a further issue that the output ancilla register (controlled by $\mathcal{A}$) must be initialized with 0. However, in the compressed Fourier basis $\mathcal{B}$ only needs to work on the oracle's function register, i.e., oracle's output register (which contains signcryption text) which is initialized with 0 by the simulator. Therefore, the above issue can be resolved, if we use the compressed standard oracle. For answering unsigncryption queries, $\mathcal{B}$ also may have to store some internal components in auxiliary registers and it can uncompute those values either by making queries to its external oracle twice or by making some computations locally, e.g., signature verification. In this case, we do not face any problem as encountered in answering signcryption queries in $\mathcal{S}t\mathcal{E}$ paradigm.

In the outsider model, the adversary is given access to both the oracles, signcryption and unsigncryption. Since the outsider model is weaker than the insider model, we can expect that the security (privacy/authenticity) of the underlying target primitive gets amplified. So, the simulator may have to simulate the queries with a restricted[3] oracle or even without having access to any external oracles. Classically, it also relies on the security of the other primitives, say, encryption, signature and commitment schemes, in addition to the target primitive. For example, for lifting IND-CPA to IND-CCA security in $\mathcal{E}t\mathcal{S}$, it requires sUF-CMA security of the underlying signature scheme. The arguments work as follows:

[3] For example, decryption oracle in IND-gCCA model, where the queries are answered based on a relation (not necessarily equality) between the challenge ciphertext and the ciphertext involved in the underlying queries.

if an adversary asks a valid unsigncryption query, then either, the adversary produces a forgery of the underlying signature scheme or gets the signcryption text from the response of the previous signcryption oracle queries, in which case simulator simply stores all the message-signcryption text pairs, and answers the unsigncryption query. In case of $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm, the IND-CCA security is preserved under sUF-CMA security of the signature scheme, and relaxed-concealment and hiding properties of commitment scheme. The security proof involves hybrid game changes and some of the game changes require checking whether the queried signcryption text in the unsigncryption query matches a certain pattern with the stored signcryption texts. If so, it then breaks the underlying security (sUF-CMA and relaxed-concealment) of the corresponding primitives. Otherwise, the changes are unnoticed by the adversary.

Quantumly, we need to record message and signcryption text pairs in superposition in a database for on-the-fly simulation of unsigncryption queries. Using the compressed oracle framework [CEV20] for randomized functions, we can record message-signcryption text pairs in superposition in a database. This enables to answer unsigncryption queries (e.g., in $\mathcal{E}t\mathcal{S}$ paradigm) using the recorded messages. It also helps to check whether the signcryption texts appeared in the unsigncryption query match a certain pattern in the stored signcryption texts (of previous signcryption queries). For example, in $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm, we consider some game changes under sUF-qCMA security and relaxed-concealment property of the underlying signature and commitment schemes respectively. If such pattern exists, we can break the aforementioned security of the underlying primitives. By doing so, we ensure that an adversary cannot make an unsigncryption query such that simulator is unable to handle.

Our Contributions. In this paper, we initiate a formal study of quantum security of classical data in three well-known signcryption paradigms. 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 as in the classical counterpart. In the outsider model, we show that IND-CPA security can be lifted to IND-qCCA security in $\mathcal{E}t\mathcal{S}$ paradigm, and IND-qCCA security can be preserved in $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms.

Due to the style of our security models, we are unable to lift pqUF-NMA security to sUF-qCMA in $\mathcal{S}t\mathcal{E}$ paradigm (resp. preserve sUF-qCMA in $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms) in outsider model what we expected as analogues to classical setting. Nonetheless, we consider an intermediate setting for authenticity (which we call uqCMA attack model) 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. In the above setting, we lift pqwUF-CMA (resp. pqsUF-CMA) to sUF-uqCMA security in $\mathcal{S}t\mathcal{E}$ (resp. $\mathcal{C}t\mathcal{E}\&\mathcal{S}$) paradigm. Interestingly, our results in the multi-user outsider model strengthen the existing classical results to the best of our knowledge.

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[4] 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-qCCA (resp. IND-qgCCA) security, if the signature scheme is post quantum sUF-qCMA (resp. wUF-qCMA). While this is in line with the classical setting, our result

[4] 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.

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-qCCA security if the signature scheme is post quantum sUF-qCMA 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 security of the underlying encryption is preserved, if the corresponding signature is post quantum sUF-CMA secure. Also, the post quantum sUF-CMA security of the underlying signature is lifted to sUF-uqCMA, if the corresponding encryption is IND-qCCA secure. For both these results, we consider some properties of the commitment scheme. The last two results too hold 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. 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 & qrCon	qBinding
SC^i	IND-iqgCCA$^{5.1}$	(w/s)UF-iqCMA$^{5.2}$	IND-i(qg/q)CCA$^{5.3}$	wUF-iqCMA$^{5.4}$	IND-iqgCCA$^{5.5}$	wUF-iqCMA$^{5.6}$
E	IND-qgCCA	Same as Insider Model	Same as Insider Model	IND-qCCA	IND-qCCA	IND-qCCA
S	sUF-qCMA			pqwUF-CMA	sUF-qCMA	pqsUF-CMA
C	-			-	qHiding & qrCon	qfBinder & qrCon
SC^o	IND-oqCCA$^{6.1}$			sUF-ouqCMA$^{6.2}$	fM-IND-oqCCA$^{6.3}$	sUF-ouqCMA$^{6.4}$
E	pqIND-CPA	Same as Insider Model	Same as Insider Model	IND-(qg/q)CCA	Same as Multi-User Outsider	Same as Multi-User Outsider
S	(w/s)UF-qCMA			pqUF-NMA		
C	-			-		
SC^2	IND-(qg/q)CCA$^{6.5}$			(w/s)UF-ouqCMA$^{6.6}$		

The rows indexed by the abbreviations E, S and C denote the the assumptions on primitives schemes Encryption, Signature and Commitment. The hyphens appeared in the cells indexed by E, S and C indicate that the signcryption results do not depend on them. The rows indexed by the symbols SC^i, SC^o and SC^2 indicate corresponding achieved security of signcryption in multi-user insider, multi-user outsider and two-user outsider models respectively. The signcryption results highlighted by the gray background denote that the authenticity of signcryption is proven in the intermediate setting, where the signcryption oracle remains classical and the unsigncryption oracle can be quantumly accessed. 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.

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 a quantum setting. In a different line than ours, [AGM18b] gives definitions for confidentiality and authentication of *quantum* data followed by constructions realizing them. The same authors showed in [AGM18a] that signing a quantum state is impossible even if the security model is considered to be weaker one. It turns out that quantum signature scheme that handles quantum data is not possible unless the state is measured before sign which leaves only classical signature scheme to exist. On the other hand, the authors showed a positive result that signing a quantum state is possible if the state is first encrypted under receiver's public key. This notion essentially defines *quantum signcryption*, a quantum version of classical signcryption in encrypt-then-sign paradigm. However, in this paper, we study quantum security of classical data in three well-known paradigms of [ADR02].

Recently, the authors in [CEV20] investigated a quantum indistinguishability under quantum chosen-ciphertext attacks (qIND-qCCA) model using Zhandry's celebrated result [Zha19a] on recording quantum queries. They claimed that this is the first fully quantum indistinguishability model that extends the classical indistinguishability model (IND-qCCA) of [BZ13]. In that model, they provided a formal security proof of authenticated encryption in encrypt-then-mac paradigm [BN08] which was an open problem in [BZ13]. More often, the authenticated-encryption is considered to be a symmetric-key analogue of signcryption in two-user outsider models. Their work considers only confidentially of quantum data in encrypt-them-mac paradigm. However, we work on quantum security of classical data, but consider a variety of settings, e.g., three paradigms of signcryption [ADR02], insider/outsider and two/multi-user models.

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. Finally, we conlcude in Section 8.

2 Preliminaries

2.1 Notations

For $m \in \mathbb{N}$, $[m]$ denotes the set $\{1, \dots, m\}$. 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 $str = str_1\|\dots\|str_n \in \{0,1\}^{t_1} \times \cdots \times \{0,1\}^{t_n}$, we use $[str]_i$ to represent the i^{th} component str_i. For a random variable X, its *collision entropy* is defined as $-\log \mathsf{Pr}[X = X']$, where X' has the same distribution as X, but independent of X.

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.

2.3 Quantum Query Recording Framework

In many classical security reductions, the simulator has to record the adversary's queries for a consistent response which may possibly involve computing an inverse function. In contrast, no-cloning theorem does not allow to record quantum queries. Zhandry [Zha19a] introduced a celebrated result on how to record quantum queries without disturbing adversary's view. He proposed an oracle technique, called compressed oracle which helps on-the-fly simulation in the setting of QROM. Using Zhandry's compressed oracle technique on recording queries, Chevalier et al. [CEV20] proposed a framework for probabilistic functions that supports answering inverse queries. Essentially, an adversary can query both the underlying function (say, encryption) and its inverse function (decryption). The probabilistic functions they considered include permutation, symmetric encryption and public-key encryption. Using the framework, they proposed a stronger realizable security model for privacy of quantum data and then they showed that IND-CPA security can be lifted to qIND-qCCA security assuming a sUF-qCMA secure MAC in the encrypt-then-mac paradigm and some other results. Next, we briefly discuss some key techniques presented in [CEV20] and closely follow the notations used by the authors.

Any randomized algorithm can be expressed by a function $f : \mathcal{X} \times \mathcal{R} \longrightarrow \mathcal{Y}$, where $\mathcal{X} = \{0,1\}^m$, $\mathcal{Y} = \{0,1\}^n$ and $\mathcal{R} = \{0,1\}^\ell$ are input domain, output domain and randomness domain respectively. In our context, the function f represents signcryption and its inverse function represents unsigncryption. The authors [CEV20] considered a number of oracles for f, standard oracle $\mathcal{O}_f$, Fourier oracle $\mathsf{FourierO}_f$, compressed Fourier oracle $\mathsf{CFourierO}_f$ and compressed standard oracle CStO_f, and showed the following important result.

Lemma 2.1 ([CEV20, Lemma 1-4]). *The oracles $\mathcal{O}_f$, $\mathsf{CFourierO}_f$ and CStO_f are perfectly indistinguishable.*

The standard oracle is implemented as $\mathcal{O}_f : \sum_{x,y} \psi_{x,y} |x, y\rangle \mapsto \sum_{x,y} \psi_{x,y} |x, y \oplus f(x;r)\rangle$, where r is a uniformly and independently sampled random coin. This is the same as answering using purification of the coin toss from adversary's point of view. That is, we can implement the oracle as follows: $\sum_{x,y} \psi_{x,y} |x, y\rangle \otimes \frac{1}{\sqrt{2^\ell}} \sum_r |r\rangle \mapsto \sum_{x,y} \psi_{x,y} |x, y \oplus f(x;r)\rangle \otimes \frac{1}{\sqrt{2^\ell}} \sum_r |r\rangle$.

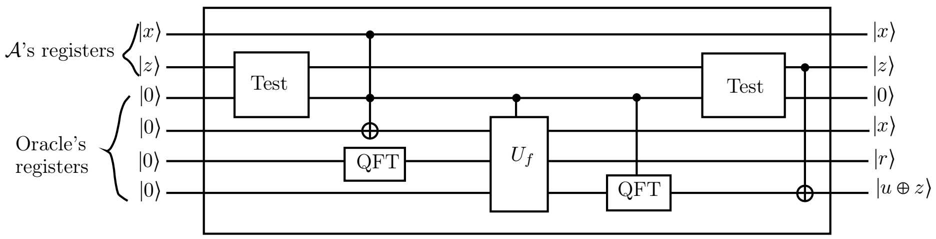


Figure 1: Quantum circuit implementing compressed Fourier oracle $\mathsf{CFourierO}_f$ (from [CEV20]).

The compressed Fourier oracle $\mathsf{CFourierO}_f$ works on $|x,z\rangle$, where $(x,z) \in \mathcal{X} \times \mathcal{Y}$ as follows:

$$\mathsf{CFourierO}_f\,|x,z\rangle = \begin{cases} |x,z\rangle\,\frac{1}{\sqrt{2^\ell}}\sum_r |r\rangle & \text{if } z = 0^n \\ |x,z\rangle \otimes |\phi_{x,z}\rangle & \text{if } z \neq 0^n, \end{cases}$$

where $|\phi_{x,z}\rangle = \dfrac{1}{\sqrt{2^\ell}}\sum_r\sum_u \dfrac{1}{\sqrt{2^n}}(-1)^{f(x;r)\cdot u}\,|x,r,z\oplus u\rangle$. For answering an f-query using $\mathsf{CFourierO}_f$ oracle, a number of unitary operations need to be performed and the number of function calls to U_f required is 3. This raises a problem in proving unforgeability of encrypt-then-sign/mac paradigm from the unforgeability of the underlying signature/mac scheme. The authors handled this issue by constructing a quantum circuit $\mathsf{CFourierO}_f$ (see Figure 1), where the number of function calls to U_f is only one. In the circuit, the first two registers are controlled by the adversary and the remaining ones (called oracle's registers) are handled by the simulator which are used to record the information related to adversary's queries. For detailed description of the circuit, refer to [CEV20].

If we apply QFT on the adversary's output register and oracle's output registers, then we can get back the standard oracle and the oracle's state will be in superposition of $(x,r,f(x;r))$. This is called as compressed standard oracle CStO_f. Let $\mathcal{D}$ denote the database that contains the tuples of the form $(x,r,f(x,r))$ in superposition. This database helps the simulator to answer queries to f^{-1} on some inputs which were output of previous f-queries. This typical scenario can be found in many classical reductions. Sometimes it is difficult for a simulator to handle f-queries (e.g., signcryption queries in insider model for $\mathcal{StE}$ paradigm) as the the adversary itself initializes the output ancilla register. Since $\mathcal{O}_f$ and CStO_f are perfectly indistinguishable and the output register of the unitary U_f appeared in the circuit of $\mathsf{CFourierO}_f$ (hence CStO_f) is initialized with $|0\rangle$, the aforementioned difficulty can be handled easily (see the proof of Theorem 5.4). This is another key feature of the circuit for CStO_f.

Let the notation $f : \mathsf{CStO}_f^{|r\rangle}[x \mapsto y]$ denote the compressed oracle of f, where r is the purification of randomness, x is the input and y is the output. Now, let us consider the following probabilistic function $f : \mathcal{X} \times \mathcal{R}_1 \times \mathcal{R}_2 \longrightarrow \mathcal{Y}$, where $\mathcal{R}_1$ and $\mathcal{R}_2$ are the domains of randomness which are controlled by the oracle. Here we consider the following implementations of compressed oracle of f:

1. $f : \mathsf{CStO}_f^{|r_1\rangle}[(x;r_2) \mapsto y]$, which considers purification of the randomness $r_1 \in \mathcal{R}_1$.

2. $f : \mathsf{CStO}_f^{|r_2\rangle}[(x;r_1) \mapsto y]$, which considers purification of the randomness $r_2 \in \mathcal{R}_2$.

3. $f : \mathsf{CStO}_f^{|r_1,r_2\rangle}[x \mapsto y]$, which considers purification of the randomness $(r_1,r_2) \in \mathcal{R}_1 \times \mathcal{R}_2$.

The following lemma says that purification of any random coin or all the random coins will give the same response.

Lemma 2.2 ([CEV20, Lemma 7]). $\mathsf{CStO}_f^{|r_1\rangle}[(x;r_2)\mapsto y]$, $f:\mathsf{CStO}_f^{|r_2\rangle}[(x;r_1)\mapsto y]$ *and* $f:\mathsf{CStO}_f^{|r_1,r_2\rangle}[x\mapsto y]$ *are perfectly indistinguishable.*

We may drop the superscript, input and output, when they are understood from the context and simply write CStO_f. Sometimes, we may drop only input and output and write $\mathsf{CStO}_f^{|r\rangle}$. While answering f-queries using compressed standard oracle CStO_f, the simulator may use some external oracle which is not controlled by itself, but it can purify the other coin toss locally. For example, there are two[5] randomness involved in the signcryption, one is used in encryption and other is used in signature generation. For answering signcryption-queries, the simulator may use either an encrypt-oracle or a sign-oracle. The above result basically says that it will not hamper the view of the adversary.

Here we briefly illustrate how to handle inverse queries as given in [CEV20]. Let $\mathsf{FindImage}$ be a function which takes a value $y\in\mathcal{Y}$ and $\mathcal{D}$ as input and outputs a value $x\in\mathcal{X}$ such that there exists $(x,r,y)\in\mathcal{D}$. Formally, $\mathsf{FindImage}$ is defined by

$$\mathsf{FindImage}(y,\mathcal{D})=\begin{cases}(1,x) & \text{if there exists } (x,r,y)\in\mathcal{D}\\ (0,0^m) & \text{otherwise.}\end{cases}$$

Next, we define a unitary operation $\mathsf{CInvO}_{f^{-1}}$ for answering f^{-1}-queries which works on $|y,z\rangle\otimes|\mathcal{D}\rangle$ as follows:

$$\mathsf{CInvO}_{f^{-1}}\,|y,z\rangle\otimes|\mathcal{D}\rangle=\begin{cases}|y,z\oplus w\rangle)\otimes|\mathcal{D}\rangle & \text{if } \mathsf{FindImage}(y,\mathcal{D})=(1,w)\\ \left|y,z\oplus f^{-1}(y)\right\rangle)\otimes|\mathcal{D}\rangle & \text{if } \mathsf{FindImage}(y,\mathcal{D})=(0,0^m).\end{cases}$$

Definition 1 ([CEV20]). *Let* $\mathcal{F}=\{f:\mathcal{X}\times\mathcal{K}\longrightarrow\mathcal{Y}\}$ *be a family of functions such that for each* $f\in\mathcal{F}$, *there is a function* $f^{-1}:\mathcal{Y}\times\mathcal{K}\longrightarrow\mathcal{X}$. *We say* $\mathcal{F}$ *is* δ*-almost invertible if*

$$\mathop{\mathbb{E}}_{k\in\mathcal{K}}\left[\max_{x\in\mathcal{X}}\Pr[f^{-1}(k,f(k,x))\neq x]\right]\leq\delta.$$

Here, f could be pseudorandom function, encryption or signcryption. The correctness of the signcryption scheme considered in this paper implies that $\delta=0$.

Lemma 2.3 ([CEV20, Lemma 8]). *For any quantum algorithm* $\mathcal{A}$ *(possibly unbounded)*

$$\left|\Pr\left[\mathcal{A}^{\mathcal{O}_f,\mathcal{O}_{f^{-1}}}()=1\right]-\Pr\left[\mathcal{A}^{\mathsf{CStO}_f,\mathsf{CInvO}_{f^{-1}}}()=1\right]\right|\leq\mathcal{O}(q_i\cdot\delta)$$

where q_i *is the number of inverse queries.*

The above lemma is very crucial for answering f^{-1}-queries using the information recorded while answering f-queries. It also ensures to extract out some related information from $\mathcal{D}$ that $\mathcal{A}$ already made queries to signcryption oracle, e.g., extracting q many message-signature pairs by measuring the database $\mathcal{D}$ for arguing one-more unforgeability (see Theorems 6.1 and 6.5) when $\mathcal{A}$ makes q many signcryption queries. Furthermore, it helps to find some particular structure in that database for arguing game changes under relaxed-concealment property or $\mathsf{sUF\text{-}qCMA}$ security in Theorem 6.3. For that we extend $\mathsf{FindImage}$ and $\mathsf{CInvO}_{f^{-1}}$ to capture some local computations on additional supplied information. This does not change the view of the adversary.

[5] For $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm, one additional randomness is used for commitment.

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 $\mathsf{IND\text{-}gCCA}$ security notion [ADR02] was not formalized in [BZ13]. However, it follows as a natural extension of the definition of $\mathsf{IND\text{-}qCCA}$ security. The security definitions of commitment and signcryption that we define, follow naturally from their classical counterparts [BSZ07, ADR02, MMS09, NP16]. In this section, we first briefly illustrate the quantum security of the primitives public-key encryption, signature and commitment as they are formally defined in Appendix A. Then, we formally give the abstract definition and security models of signcryption. We emphasize that our security models capture quantum security of classical data.

Security of PKE in the Quantum Setting. By $\mathsf{pqIND\text{-}X}$ security, where $\mathsf{X} \in \{\mathsf{CCA}, \mathsf{gCCA}, \mathsf{CPA}\}$, we mean post-quantum security, i.e., here the adversary is considered to be a PPT quantum algorithm and given classical access to decryption oracle (resp. decryption oracle with a generalized restriction[6] and no decryption oracle) and superposition access to random oracle (if there is any random oracle). By $\mathsf{IND\text{-}X}$ security, where $\mathsf{X} \in \{\mathsf{qCCA}, \mathsf{qgCCA}\}$, we mean quantum security of classical data, i.e., the PPT quantum adversary is provided superposition access to decryption oracle (resp. decryption oracle with a generalized restriction) and superposition access to random oracle (if there is any random oracle).

Security of PKS in the Quantum Setting. By $\mathsf{pq(w/s)UF\text{-}CMA}$ security, we mean post-quantum weak/strong unforgeability under classical chosen-message attack, where a PPT quantum adversary is given access to classical sign oracle and quantum random oracle (if there is any random oracle). The security model $\mathsf{pqUF\text{-}NMA}$ is a weaker model, where only oracle available to the adversary is the quantum random oracle (if there is any random oracle). By $\mathsf{(w/s)UF\text{-}qCMA}$ security, we mean quantum weak/strong unforgeability of classical data, i.e., a PPT quantum adversary is provided superposition access to sign oracle, in addition to superposition random oracle queries (if any). Further, if the adversary makes q sign queries, then it has to submit $(q+1)$ classical message-signature pairs as forgeries, and weak/strong comes in the sense that whether messages are distinct or message-signature pairs are pairwise distinct. This notion is also referred as *one-more unforgeability.*

Security of Commitment in the Quantum Setting. The hiding property ensures that a PPT adversary cannot distinguish com part of two distinct messages chosen by the adversary. The binding property says that once the sender commits a message, later cannot change his mind, i.e., a PPT adversary cannot produce $(\mathsf{com}, \mathsf{decom}, \mathsf{decom}')$ such that $(\mathsf{com}, \mathsf{decom})$ and $(\mathsf{com}, \mathsf{decom}')$ open in two different messages. The concealment property guarantees that a PPT adversary cannot produce $(\mathsf{com}, \mathsf{com}', \mathsf{decom})$ with $\mathsf{com} \neq \mathsf{com}'$ such that $(\mathsf{com}, \mathsf{decom})$ and $(\mathsf{com}', \mathsf{decom})$ open to two valid messages (not necessarily distinct). The relaxed-concealment is weaker version of concealment, where an adversary will be given $(\mathsf{com}, \mathsf{decom})$ for a message chosen by the adversary and the goal is to produce a different com' such that $(\mathsf{com}', \mathsf{decom})$ opens to a valid message. The properties $\mathsf{qHiding}$, $\mathsf{qBinding}$ and $\mathsf{qrConcealment}$ stand for quantum hiding, quantum binding and quantum relaxed-concealment respectively. These are defined to be the same as their classical counterpart (mentioned above) but the adversary is a PPT quantum algorithm. Also, we consider a new property called $\mathsf{qfBinder}$, where an adversary will be given com part of $(\mathsf{com}, \mathsf{decom})$ for a message

[6] In $\mathsf{IND\text{-}gCCA}$ model, for a decryption query on c the adversary gets the underlying plaintext (i.e., $\mathcal{D}(\mathsf{c}, \mathsf{sk})$), if c is not related (w.r.t some relation) to c^* (the challenge ciphertext), else gets $\perp$, unlike to $\mathsf{IND\text{-}CCA}$ model. When the relation is consider to be equality, then $\mathsf{IND\text{-}gCCA}$ becomes $\mathsf{IND\text{-}CCA}$ model.

chosen by the adversary and the goal is to produce a decom' (not necessarily different from decom) such that $(\mathsf{com}, \mathsf{decom}')$ opens to a valid message.

3.1 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 2. *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*

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

in $\mathsf{Exp}_{\mathcal{A},\mathsf{SC}}^{\mathsf{dM\text{-}IND\text{-}iCCA}}(\lambda)$ *defined in Figure 2 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* $\mathcal{US}(\mathsf{u}^*, \mathsf{sk}_{\mathsf{R}^*}, \mathsf{pk}_\mathsf{S})$.

Definition 3. *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:*

$$\sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle \longmapsto \sum_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u}, \mathsf{pk}_\mathsf{S})\rangle \quad (1)$$

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

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

Figure 2: Experiment for confidentiality (dynamic multi-user insider model)

where

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

The notion of dM-IND-iqgCCA can be defined in a similar way as in IND-qgCCA (Definition 16). 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 1 in the following way:

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

Definition 4. *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 5. *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*

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

in $\mathsf{Exp}^{\mathsf{dM\text{-}pqsUF\text{-}iCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 3 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.*

- 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 6. *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 message* $(\mathsf{m}^*, \mathsf{pk}_{\mathsf{R}^*})$ *corresponding to the forgery was not queried to the signcryption oracle.*

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

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

Figure 3: Experiment for unforgeability (dynamic multi-user insider model)

Definition 7. *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 4 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 and the underlying messages 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:*

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

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

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

Figure 4: Experiment for unforgeability (dynamic multi-user insider model)

Definition 8. *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 the underlying messages are 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 9. *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*

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

in $\mathsf{Exp}^{\mathsf{fM\text{-}IND\text{-}oqCCA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 5 is a negligible function in security parameter* 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) with natural restrictions that* $(\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*})$ *was never queried to* $\mathcal{O}^{\mathsf{q}}_{U}$*.*

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

$$\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \left|\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\right\rangle \longmapsto \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \left|\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p} \oplus f(\mathsf{u}, \mathsf{pk}_\mathsf{S})\right\rangle \tag{2}$$

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

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

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

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

Figure 5: 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 16). 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 2 in the following way:

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

Definition 10. *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 11. *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*

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

in $\mathsf{Exp}^{\mathsf{fM\text{-}sUF\text{-}oqCMA}}_{\mathcal{A},\mathsf{SC}}(\lambda)$ *defined in Figure 6 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:*

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

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

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

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

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

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

Definition 12. *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 fM-IND-ouqCCA, fM-IND-ouqgCCA in the confidentiality case and fM-sUF-ouqCMA, fM-wUF-ouqCMA in the authenticity case. Similarly, for the two-user model we call these definitions as IND-ouqCCA, IND-ouqgCCA in the confidentiality case and sUF-ouqCMA, wUF-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 4*)).

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 $b \xleftarrow{U} \{0,1\}$, 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 $\mathsf{u_{quant}} = \sum_{\mathsf{u,pk_S,m_p}} \psi_{\mathsf{u,pk_S,m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. Note that, the query $\mathsf{u_{quant}}$ consists of three registers $\mathsf{U} = (\mathsf{C}, \mathsf{S}), \mathsf{PK_S}$ and M. These registers 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 $\left|0^{\ell_m}\right\rangle$, to the query and obtains the state $\sum_{\mathsf{u,pk_S,m_p}} \psi_{\mathsf{u,pk_S,m_p}} \left|\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\right\rangle$. $\mathcal{B}$ 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

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

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 $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state

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

where

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

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

Note that the ancilla register is entangled with $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}$ uncomputes $g(\mathsf{c})$ by making decryption query on $|\mathsf{c}, g(\mathsf{c})\rangle$ to $\mathcal{CH}$ and sends the state $\sum_{\mathsf{u,pk_S,m_p}} \psi_{\mathsf{u,pk_S,m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. $\mathcal{B}$ 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. $\mathcal{V}(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_S}) = \mathsf{True}$
3. $\mathsf{pk_S} = \mathsf{pk_{S^*}}$

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* $\mathsf{sUF\text{-}qCMA}$ (*resp.* $\mathsf{wUF\text{-}qCMA}$) *secure, then the signcryption scheme* SC *in the* $\mathcal{E}t\mathcal{S}$ *paradigm is* $\mathsf{sUF\text{-}qCMA}$ (*resp.* $\mathsf{wUF\text{-}qCMA}$) *secure in dynamic multi user insider-security model* ($\mathsf{dM\text{-}sUF\text{-}iqCMA}$ (*resp.* $\mathsf{dM\text{-}wUF\text{-}iqCMA}$) (*c.f., Definitions 7, 8*)).

Proof. Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{dM\text{-}sUF\text{-}iqCMA}$ (resp. $\mathsf{dM\text{-}wUF\text{-}iqCMA}$) 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 $\mathsf{sUF\text{-}qCMA}$ (resp. $\mathsf{wUF\text{-}qCMA}$) security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ 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 $\mathsf{m}_{\mathsf{quant}} = \sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}\rangle$ be any signcryption query made by $\mathcal{A}$. Note that, the query $\mathsf{m}_{\mathsf{quant}}$ consists of three registers $\mathsf{M}, \mathsf{PK}_\mathsf{R}$ 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 $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{c}_\mathsf{p}, \sigma_\mathsf{p}, 0^{\ell_c}\rangle$. $\mathcal{B}$ chooses a randomness r_{enc} and applies the encryption operator which results in the following unitary transformation

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

$\mathcal{B}$ sends a signature query on $2^{nd}, 4^{th}$ and 5^{th} registers ($\mathsf{PK}_\mathsf{R}, \mathsf{S}$ and the ancilla register) to $\mathcal{CH}$. Here the ancilla register and 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 $\mathsf{c} = \mathcal{E}(\mathsf{m}||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R}; r_{\mathsf{enc}})$)

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

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

$$\sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{c}_\mathsf{p}, \sigma_\mathsf{p} \oplus \sigma, \mathsf{c}\rangle \longmapsto \sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{c}_\mathsf{p} \oplus \mathsf{c}, \sigma_\mathsf{p} \oplus \sigma, \mathsf{c}\rangle .$$

The resulting state can be equivalently written as

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

Note that $\mathcal{B}$ uncomputes the last register by applying encryption operator on 1^{st} and 4^{th} register using the same randomness r_{enc} to obtain the state $\sum\limits_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p} \oplus \mathsf{u}\rangle \otimes |0^{\ell_c}\rangle$, where $\mathsf{u} = \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$. 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 $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs $q+1$ forgeries $\{(\mathsf{u}_i, \mathsf{pk}_{\mathsf{R}i}, \mathsf{sk}_{\mathsf{R}i}) : i \in [q+1]\}$. $\mathcal{B}$ forwards $(\mathsf{c}_1||\mathsf{pk}_{\mathsf{R}1}, \sigma_1), \ldots, (\mathsf{c}_{q+1}||\mathsf{pk}_{\mathsf{R}q+1}, \sigma_{q+1})$ 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 $\mathcal{S}t\mathcal{E}$ paradigm cannot be achieved against insider adversaries [ADR02]. However, $\mathcal{S}t\mathcal{E}$ 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 $\mathcal{S}t\mathcal{E}$ 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 $\mathcal{S}t\mathcal{E}$ 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 3, 4*)).

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

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

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 $\mathcal{B}$. $\mathcal{B}$ 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 $\mathsf{u}_{\mathsf{quant}} = \sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. 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 $\sum\limits_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} \psi_{\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ 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 $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}$ uncomputes $g(\mathsf{u})$ by making decryption query on $|\mathsf{u}, g(\mathsf{u})\rangle$ to $\mathcal{CH}$ 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: 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 $\mathcal{StE}$ paradigm (Theorem 5.4). Recall that in the dM-wUF-iqCMA security model (c.f., Definition 8), 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. Note that here the simulator makes queries to its external sign oracle for answering the signcryption queries. In fact, the simulator prepares an ancilla register S (initialized with $|0\rangle$) and then supplies to its external oracle two input registers M and $\mathsf{PK_R}$, and the output register S where output signature will be recorded. The simulator then applies the unitary for encryption on input registers M, S and $\mathsf{PK_S}$, and output register U. After the completion of the unitary, the state of U (set by the adversary) will be XORed with the output signcryption text. This is the usual way how signcryption queries are handled. Note that this way the adversary's registers get entangled with the ancilla register S. We can uncompute S when 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. When the signature is deterministic, one can deal with this issue is just uncomputing the state contained in S by making sign query again on the registers M and S. However, for simulating q signcryption oracle queries the simulator has to make $2q$ signature oracle queries, thus rendering the simulation useless.

In [GHS16], the authors considered two types of unitary: Type-1 unitary (the usual one), where the state contained in the output register is XORed with the output and Type-2 unitary[7] , where the state of the input register is replaced by the output (in other words, there is no extra output register). In the

[7] For making the functions, like, encryption to be bijective, one has to keep additional bits apart from the input.

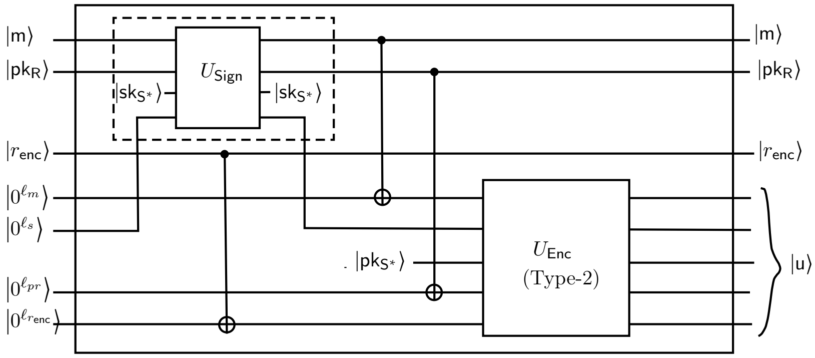


Figure 7: Quantum circuit implementing unitary U_{SC}, where the simulator makes signature queries to its external oracle (shown by dashed line) which is handled by the challenger of the underlying signature scheme and then it encrypts the message-signature pair using fresh randomness r_{enc}. Note that the unitary U_{SC} works in the usual way, i.e., Type-1 unitary (although U_{Enc} is implemented by Type-2 unitary [GHS16]).

aforementioned simulation, if we simulate encryption using Type-2 unitary, then the uncomputation issue (of S) can be resolved. But, it creates another issue: usual requirement is that at the end the state of U must be XORed with the output signcryption text – which is not possible due to Type-2 unitary. Essentially, the above discussion says that the simulator cannot answer a signcryption query, if the output register U of the adversary is not initialized with $|0\rangle$. That means, to make the simulation successful, we have to put a restriction on adversary's choice of initial state of U. However, if the simulator answers signcryption queries using compressed standard oracle technical of [CEV20], then the simulation will be successful without any restriction on adversary's choice. In fact, as per requirement given in compressed Fourier oracle $\mathsf{CFourierO}_f$ (c.f., Figure 1), the simulator needs only to deal with the situation where the output register (part of oracle's registers) is initialized with $|0\rangle$.

Theorem 5.4. *If the primitive signature scheme* PKS *is* wUF-qCMA *secure, then the signcryption scheme* SC *in the* $\mathcal{StE}$ *paradigm is* wUF-qCMA *secure in dynamic multi user insider-security model* (dM-wUF-iqCMA (*c.f., Definition 8*)).

Proof. Let $\mathcal{A}$ be a quantum PPT adversary that can break 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 wUF-qCMA security of PKS with advantage at least ϵ. Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ 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: Let r_{enc} be the randomness used in the encryption algorithm. The signcryption queries will be responded using compressed standard oracle $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{enc}}\rangle}$. This does not make any difference in $\mathcal{A}$'s view thanks to Lemmas 2.1 and 2.2. Based on the description of $\mathsf{CFourierO}_f$ in Section 2.3, it suffices to illustrate only how U_{SC} works. In fact, the implementation of U_{SC} is shown in Figure 7): it takes basis element $|\mathsf{m}, \mathsf{pk_R}, r_{\mathsf{enc}}, 0^{\ell_m}, 0^{\ell_s}, 0^{\ell_{ps}}, 0^{\ell_{pr}}, 0^{\ell_{r_{\mathsf{enc}}}}\rangle$ as input and outputs $|\mathsf{m}, \mathsf{pk_R}, r_{\mathsf{enc}}, \mathsf{u}\rangle$, where $\ell_u = \ell_m + \ell_s + \ell_{ps} + \ell_{pr} + \ell_{r_{\mathsf{enc}}}$, and ℓ_u, ℓ_m, ℓ_s, ℓ_{ps}, ℓ_{pr} and $\ell_{r_{\mathsf{enc}}}$ denote the lengths of signcryption text, plaintext, signature, $\mathsf{pk_{S^*}}$, $\mathsf{pk_R}$ and randomness of encryption algorithm respectively.

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

$\mathcal{B}$ forwards the set $\{([(\mathcal{D}(\mathsf{u}_i, \mathsf{sk}_{\mathsf{R}i}))]_1 \| \mathsf{pk}_{\mathsf{R}_i}, [\mathcal{D}(\mathsf{u}_i, \mathsf{sk}_{\mathsf{R}i}))]_2) : i \in [q+1]\}$ 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 B.1, B.2 and B.3.

Theorem 5.5. *If the primitive encryption scheme* PKE *is* IND-qgCCA *secure and the commitment scheme* C *satisfies* qHiding *and* qrConcealment *properties, then the signcryption scheme* SC *in the $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigm is* IND-qgCCA *secure in the dynamic multi user insider-security model* (dM-IND-iqgCCA (*c.f., Definition 4*)).

Proof Sketch. 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 $\mathcal{R}'((\mathsf{u}_1, \mathsf{pk}_{\mathsf{S}_1}), (\mathsf{u}_2, \mathsf{pk}_{\mathsf{S}_2})) = \mathsf{True}$ 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

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

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 dM-IND-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* qrConcealment *property of the commitment scheme* C.

Lemma 5.3. $\mathbf{Game_0}$ *and* $\mathbf{Game_1}$ *are indistinguishable under the* IND-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*

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

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 B.4 and B.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 8*)).

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 $(\mathsf{com}_1, \mathsf{pk}_{\mathsf{R}_1}), \ldots, (\mathsf{com}_{q+1}, \mathsf{pk}_{\mathsf{R}_{q+1}})$ are pairwise distinct. Note that,

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

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

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, $\mathsf{IND\text{-}CPA}$ security of the encryption scheme is amplified to $\mathsf{IND\text{-}CCA}$ security in the $\mathcal{E}t\mathcal{S}$ paradigm if the signature scheme is $\mathsf{sUF\text{-}CMA}$ 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. In quantum setting, the same was known to be not true in general due to quantum no-cloning, until the recent result [Zha19a] on recording quantum queries. Using the techniques [Zha19a, CEV20] of recording quantum queries, we handle the confidentiality of $\mathcal{E}t\mathcal{S}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms.

Although the quantum oracle queries can be recorded using the above mentioned techniques, we face some other issue in preserving $\mathsf{sUF\text{-}qCMA}$ security of the underling signature scheme in $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms. Note that we also assume $\mathsf{IND\text{-}qCCA}$ security of primitive encryption scheme. For arguing security, we have to consider some hybrid game changes (like in classical reduction) under $\mathsf{IND\text{-}qCCA}$ security of the encryption scheme. The number of such games equals the number of signcryption queries. In this process, the output signcryption texts of the signcryption oracle are changed from the original form to a special form one by one under $\mathsf{IND\text{-}qCCA}$ security of the encryption scheme. In particular, when signcryption query is classical, the ciphertext part (produced by the underlying encryption scheme) of the signcryption text for the query message is changed by the encryption of 0 (resp. decommitment chosen uniformly from decommitment space) in case of $\mathcal{S}t\mathcal{E}$ (resp. $\mathcal{C}t\mathcal{E}\&\mathcal{S}$). For this purpose, classical indistinguishability (i.e., $\mathsf{IND\text{-}qCCA}$) of the encryption scheme is sufficient. Now, if we allow signcryption queries to be in superposition, then we need qIND-qCCA security (i.e., indistinguishability of quantum data). However, the only realizable qIND-qCCA security models [AGM18b, CEV20] follow the style of real-or-random game which do not fit in our reductions.

The issue leads 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.

In Section 6.1, we discuss the security of the paradigms in the multi-user outsider models. Although all the results in multi-user models are also true in two-user models, in Section 6.2, we show some improvement for privacy and authenticity of $\mathcal{E}t\mathcal{S}$ and $\mathcal{S}t\mathcal{E}$ in the two-user outsider models respectively.

6.1 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 6.1, 6.2, 6.3 and 6.4 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].

6.1.1 Encrypt-then-Sign

In Theorem 6.1, we show that non-malleability is not a *necessary* condition to achieve IND-qCCA security in $\mathcal{E}t\mathcal{S}$ paradigm. Essentially, IND-qgCCA security of the primitive encryption scheme ensures that the adversary cannot modify the ciphertext to replace sender's identity with its own and pqsUF-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.

Theorem 6.1. *Suppose the primitive encryption scheme* PKE *is* IND-qgCCA *secure and the signature scheme* PKS *is* sUF-qCMA *secure. Further, assume that the ciphertext has superlogarithmic collision-entropy in the security parameter. Then the signcryption scheme* SC *in the* $\mathcal{E}t\mathcal{S}$ *paradigm is* IND-qCCA *secure in the multi-user outsider-security model* (fM-IND-oqCCA (*c.f., Section 3.1*)).

Proof. We use the compressed oracle technique [CEV20] for answering signcryption and unsigncryption queries. Let $r = (r_{\mathsf{enc}}, r_{\mathsf{sign}})$ denote the randomness of the signcryption algorithm. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is IND-qgCCA secure.

Let $\mathcal{A}$ be a quantum PPT adversary that can break fM-IND-oqCCA security of the signcryption scheme SC with probability at least ϵ. Let $\mathsf{pk}_{\mathsf{R}^*}$ and $\mathsf{pk}_{\mathsf{S}^*}$ 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

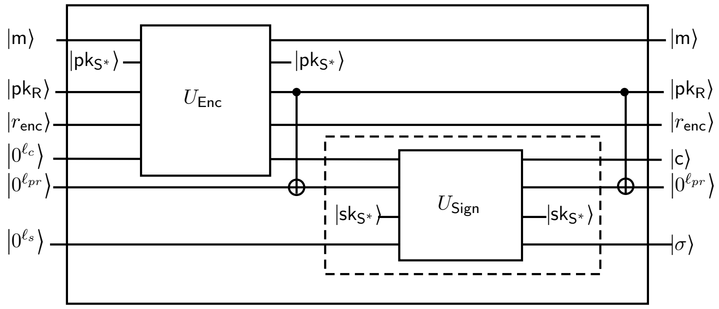


Figure 8: Quantum circuit implementing unitary U_{SC}, where the unitary bounded by dashed line is handled by the challenger of the underlying signature scheme.

its run, measuring query input of which yields with non-negligible probability, say μ, a tuple $(\mathsf{c}, \sigma, \mathsf{pk}_{\mathsf{S}^*})$ such that $\mathcal{V}(\mathsf{c}||\mathsf{pk}_{\mathsf{R}^*}, \sigma, \mathsf{pk}_{\mathsf{S}^*}) = 1$ and (c, σ) was not a result of challenge query or any previous signcryption oracle query on $\mathsf{pk}_{\mathsf{R}^*}$. In other words, if Forge happens then $\mathcal{A}$ breaks the sUF-qCMA security of the underlying signature scheme PKS. Note that,

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

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 sUF-qCMA 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 $i \overset{\text{U}}{\longleftarrow} [q_u]$ 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 $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_{\mathsf{R}^*})$ and makes a signature oracle query on $\mathsf{c}^*||\mathsf{pk}_{\mathsf{R}^*}$. $\mathcal{CH}$ runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{c}^*||\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ and sends σ^* to $\mathcal{B}_1$. $\mathcal{B}_1$ sets $\mathsf{u}^* = (\mathsf{c}^*, \sigma^\star)$ and sends the same to $\mathcal{A}$.

Signcryption queries: Let $\mathsf{m}_\mathsf{quant} = \sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} |\mathsf{m}, \mathsf{pk}_\mathsf{R}, \mathsf{u}_\mathsf{p}\rangle$ be any signcryption query made by $\mathcal{A}$. This will be answered using $\mathsf{CStO}_{\mathcal{SC}}^{|r_\mathsf{enc}\rangle}$ oracle, where unitary $U_{\mathcal{SC}}$ used in $\mathsf{CStO}_{\mathcal{SC}}$ is implemented as shown in Figure 8. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r_\mathsf{enc}\rangle}$ will be updated with the tuple of the form $(\mathsf{m}||\mathsf{pk}_\mathsf{R}, r_\mathsf{enc}, \mathsf{u})$ in superposition and adversary's registers will be updated with the desired output.

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 $\mathcal{A}$. 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 let (c, σ) be the outcome. Then $\mathcal{B}_1$ measures each state of the database $\mathcal{D}$ and outputs $\{(\mathsf{c}||\mathsf{pk}_{\mathsf{R}^*}, \sigma)\} \cup \{(\mathsf{c}^*||\mathsf{pk}_{\mathsf{R}^*}, \sigma^*)\} \cup \{(\mathsf{c}_k||\mathsf{pk}_\mathsf{R}^{(k)}, \sigma_k) : k \in [q_s]\}$, where $\mathsf{u}_k = (\mathsf{c}_k, \sigma_k)$ is the k^{th} signcryption text for receiver identity $\mathsf{pk}_\mathsf{R}^{(k)}$ after measuring $\mathcal{D}$ and q_s is the number of signcryption queries till i^{th} unsigncryption query. Otherwise, $\mathcal{B}_1$ applies the following unitary transformation

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

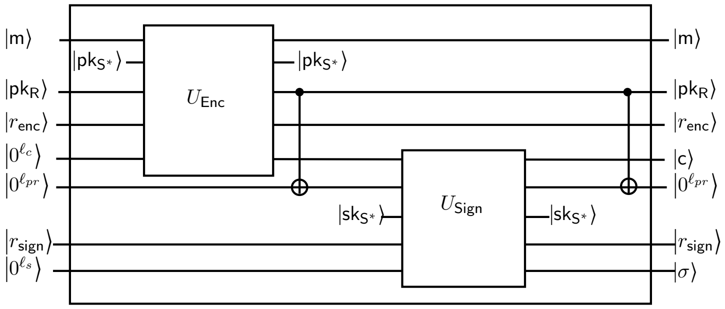


Figure 9: Quantum circuit implementing unitary U_{SC}, where both the unitary operations U_{Enc} and U_{Sign} are handled by the simulator.

where

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

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: Based on Lemma 2.1, we can replace $\mathcal{O}_{\mathcal{SC}}$ by $\mathsf{CStO}^{|r\rangle}_{\mathcal{SC}}$ (which purifies r). Further, the oracles $\mathsf{CStO}^{|r\rangle}_{\mathcal{SC}}$ and $\mathsf{CStO}^{|r_{\mathsf{enc}}\rangle}_{\mathcal{SC}}$ are equivalent thanks to Lemma 2.2. Therefore, all the signcryption queries are answered perfectly from adversary's point of view. By the definition of Forge, $(\mathsf{c}||\mathsf{pk_{R^*}}, \sigma) \notin \{(\mathsf{c}^*||\mathsf{pk_{R^*}}, \sigma^*)\} \cup \{(\mathsf{c}_k||\mathsf{pk}^{(k)}_{\mathsf{R}}, \sigma_k) : k \in [q_s]\}$. Moreover, since each time the ciphertexts in the signcryption queries (including challenge) are answered by sampling fresh randomness, so by assumption the collision probability of any two ciphertexts in $\{\mathsf{c}^*\} \cup \{\mathsf{c}_k : k \in [q_s]\}$ is negligible. Therefore, except with some negligible probability, all (q_s+2) pairs that $\mathcal{B}_1$ outputs are distinct. Hence, $\mathcal{B}_1$ breaks the $\mathsf{sUF\text{-}qCMA}$ security of PKS with probability at least $\epsilon \cdot \mu/(2 \cdot q_u)$.

Case 2: $\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}$. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the $\mathsf{IND\text{-}qgCCA}$ 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 $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ then runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$ 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 m_0 and 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 $b \overset{\mathsf{U}}{\longleftarrow} \{0,1\}$, 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 $\mathsf{m_{quant}} = \sum_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} \psi_{\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}} |\mathsf{m}, \mathsf{pk_R}, \mathsf{u_p}\rangle$ be any signcryption query made by $\mathcal{A}$. This will be answered using $\mathsf{CStO}^{|r\rangle}_{\mathcal{SC}}$ oracle, where the unitary $U_{\mathcal{SC}}$ used in $\mathsf{CStO}_{\mathcal{SC}}$ is implemented as shown in Figure 9. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}^{|r\rangle}_{\mathcal{SC}}$ will be updated with the tuple of the form $(\mathsf{m}||\mathsf{pk_R}, r, \mathsf{u})$ in superposition and $\mathcal{A}$'s registers will be updated with the desired output.

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 $\mathcal{A}$. $\mathcal{B}_2$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{c}, \sigma, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of 1^{st} and 5^{th} register to $\mathcal{CH}$.

$\mathcal{CH}$ applies the following unitary transformation

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

where

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

Let $\Delta := (\mathsf{u},\mathsf{pk_S},g(\mathsf{c}))$. Now we use $\widetilde{\mathsf{CInvO}}_{\mathcal{US}}$ for extracting related plaintexts from the database $\mathcal{D}$ and the supplied information $g(\mathsf{c})$ provided u passes some sanity checking. For doing that we first define a specialized search function $\mathsf{FindImage}^*$ which will work on $(\Delta,\mathcal{D})$:

$$\mathsf{FindImage}^*(\Delta,\mathcal{D}) = \begin{cases} (1,\mathsf{m}) & \text{if } \mathsf{Flag}_1 = \mathsf{True} \\ (1,[g(\mathsf{c})]_1) & \text{if } \mathsf{Flag}_2 = \mathsf{True} \\ (0,0^{\ell_m}) & \text{otherwise,} \end{cases}$$

where

- $\mathsf{Flag}_1 := (\mathsf{u},\mathsf{pk_S}) \neq (\mathsf{u}^*,\mathsf{pk_{S^*}}) \wedge \mathcal{R}(\mathsf{c},\mathsf{c}^*) = \mathsf{True} \wedge \exists(\mathsf{m},r) \text{ s.t } (\mathsf{m}||\mathsf{pk_{R^*}},r,\mathsf{u}) \in \mathcal{D}$
- $\mathsf{Flag}_2 := (\mathsf{u},\mathsf{pk_S}) \neq (\mathsf{u}^*,\mathsf{pk_{S^*}}) \wedge \mathcal{R}(\mathsf{c},\mathsf{c}^*) = \mathsf{False} \wedge \mathcal{V}(\mathsf{c}||\mathsf{pk_{R^*}},\sigma,\mathsf{pk_S}) = 1 \wedge \mathsf{pk_S} = [g(\mathsf{c})]_2$.

The oracle $\widetilde{\mathsf{CInvO}}_{\mathcal{US}}$ works on basis element $|\Delta,\mathsf{m_p}\rangle$ and $\mathcal{D}$ as follows:

$$\widetilde{\mathsf{CInvO}}_{\mathcal{US}}\,|\mathsf{u},\mathsf{pk_S},\mathsf{m_p},g(\mathsf{c})\rangle \otimes |\mathcal{D}\rangle = \begin{cases} |\mathsf{u},\mathsf{pk_S},\mathsf{m_p}\oplus\mathsf{m},g(\mathsf{c})\rangle \otimes |\mathcal{D}\rangle & \text{if } \mathsf{FindImage}^*(\Delta,\mathcal{D}) = (1,\mathsf{m}) \\ \left|\mathsf{u},\mathsf{pk_S},\boxed{\mathsf{m_p}\oplus\perp},g(\mathsf{c})\right\rangle \otimes |\mathcal{D}\rangle & \text{if } \mathsf{FindImage}^*(\Delta,\mathcal{D}) = (0,0^{\ell_m}). \end{cases}$$

Before returning the answer to $\mathcal{A}$, $\mathcal{B}_2$ uncomputes $g(\mathsf{c})$ by making decryption query on $|\mathsf{c},g(\mathsf{c})\rangle$ to $\mathcal{CH}$.

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

Analysis: First note that the actual oracles $(\mathcal{O}_{\mathcal{SC}},\mathcal{O}_{\mathcal{US}})$ are replaced by $(\mathsf{CStO}_{\mathcal{SC}},\widetilde{\mathsf{CInvO}}_{\mathcal{US}})$. Further, the oracle $\widetilde{\mathsf{CInvO}}_{\mathcal{US}}$ does some extra computations on the additional information $g(\mathsf{c})$, as compared to $\mathsf{CInvO}_{\mathcal{US}}$ and the same extra computations also applicable to the original oracle $\mathcal{O}_{\mathcal{US}}$. Therefore, the aforementioned replacement of the oracles does not change $\mathcal{A}$'s view thanks to Lemma 2.3. We show that $\mathcal{B}_2$ simulates $\mathcal{A}$'s unsigncryption queries properly. Basically, we have to give the justification of the answer (in the box) using $\widetilde{\mathsf{CInvO}}_{\mathcal{US}}$, if $\mathcal{A}$ asks a valid query. In fact, 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. □

6.1.2 Sign-then-Encrypt

Our next result concerns with unforgeability in the $\mathcal{StE}$ paradigm. In a nutshell, Theorem 6.2 follows from the following argument: IND-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.

Theorem 6.2. *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 3.1*)).

Proof. 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 $\mathbf{Game_0}$ 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 $\mathsf{pk}_{\mathsf{R}^*}$. 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 $\mathsf{pk}_{\mathsf{R}^*}$, $\mathbf{Game_j}$ returns a random encryption of 0^{ℓ_m}, i.e., $\mathsf{u}_j \longleftarrow \mathcal{E}(0^{\ell_m}; \mathsf{pk}_{\mathsf{R}^*})$. Further, for a basis element $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}^*})$ of any unsigncryption query, if u is the result of any previous signcryption query $(\mathsf{m}, \mathsf{pk}_{\mathsf{R}^*})$, 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 $\mathsf{pk}_{\mathsf{R}^*}$ 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 $\mathsf{Succ}_{q_s}(\mathcal{A}) \le \mathsf{Adv}^{\mathsf{pqwUF-CMA}}_{\mathcal{B},\mathsf{PKS}}(1^\lambda)$. 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 $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ 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 $(\mathsf{m}, \mathsf{pk}_\mathsf{R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} \ne \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_1$ runs $\mathsf{u} \longleftarrow \mathcal{SC}(\mathsf{m}, \mathsf{sk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. For the first $j-1$ queries on $\mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_1$ answers with a random encryption of 0^{ℓ_m}. At the j^{th} query $(\mathsf{m}_j, \mathsf{pk}_{\mathsf{R}^*})$, $\mathcal{B}_1$ runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}_j \| \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$, prepares a challenge query $(\mathsf{m}_0, \mathsf{m}_1) \longleftarrow (\mathsf{m}_j \| \sigma \| \mathsf{pk}_{\mathsf{S}^*}, 0^{\ell_m})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{m}_b, \mathsf{pk}_{\mathsf{R}^*})$ 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 on $\mathsf{pk}_{\mathsf{R}^*}$, all the signcryption queries are answered properly. For all signcryption queries $(\mathsf{m}, \mathsf{pk}_{\mathsf{R}^*})$, $\mathcal{B}_1$ also adds (m, u) to a list $\mathcal{L}$ (which is initially empty).

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

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

where

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

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

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

where

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

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

Note that the ancilla register is entangled with $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}_1$ uncomputes $g(\mathsf{u})$ by making decryption query on $|\mathsf{u}, g(\mathsf{u})\rangle$ to $\mathcal{CH}$ and sends the state $\sum_{\mathsf{u},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{m}_\mathsf{p}} |\mathsf{u}, \mathsf{m}_\mathsf{p} \oplus f(\Delta)\rangle$ to $\mathcal{A}$.

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 $\mathsf{m}_j || \sigma || \mathsf{pk}_{\mathsf{S}^*}$. From the simulation procedure, it is clear that if u_j is indeed the encryption of $\mathsf{m}_j || \sigma || \mathsf{pk}_{\mathsf{S}^*}$, 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 $\mathcal{B}_1$ 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 $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_\mathcal{S}(1^\lambda)$ 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 $(\mathsf{m}, \mathsf{pk}_\mathsf{R})$ be any signcryption query made by $\mathcal{A}$. If $\mathsf{pk}_\mathsf{R} \neq \mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{B}_2$ sends a signature query on $\mathsf{m}||\mathsf{pk}_\mathsf{R}$ to $\mathcal{CH}$. $\mathcal{CH}$ then runs $\sigma \longleftarrow \mathcal{S}(\mathsf{m}||\mathsf{pk}_\mathsf{R}, \mathsf{sk}_{\mathsf{S}^*})$ and sends σ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs $\mathsf{u} \longleftarrow \mathcal{E}(\mathsf{m}||\sigma||\mathsf{pk}_{\mathsf{S}^*}, \mathsf{pk}_\mathsf{R})$ and sends u to $\mathcal{A}$. Otherwise, $\mathcal{B}_2$ answers with a random encryption of 0^{ℓ_m} on $\mathsf{pk}_{\mathsf{R}^*}$. For all signcryption queries $(\mathsf{m}, \mathsf{pk}_{\mathsf{R}^*})$, $\mathcal{B}_2$ also adds (m, u) to a list $\mathcal{L}$ (which is initially empty).

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 $\mathcal{A}$. $\mathcal{B}_2$ 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

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

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

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

Forgery: $\mathcal{A}$ outputs a forgery u. $\mathcal{B}_2$ runs $(\mathsf{m}||\sigma||\mathsf{pk}_{\mathsf{S}^*}) \longleftarrow \mathcal{D}(\mathsf{u}, \mathsf{sk}_{\mathsf{R}^*})$ and sends $(\mathsf{m}||\mathsf{pk}_{\mathsf{R}^*}, \sigma)$ 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 pqwUF-CMA security of PKS with advantage at least ϵ. □

6.1.3 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 6.3 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 C.1, C.2, C.3 and C.4. Note that here we do not consider the intermediate security model, i.e., the following theorem guarantees the confidentiality even if $\mathcal{A}$ is allowed to ask both queries in superposition.

Theorem 6.3. *Suppose the primitive encryption scheme* PKE *is* $\mathsf{IND\text{-}qCCA}$ *secure, the signature scheme* PKS *is* $\mathsf{sUF\text{-}qCMA}$ *secure and the commitment scheme* C *satisfies* $\mathsf{qrConcealment}$ *and* $\mathsf{qHiding}$ *properties. Further, assume that* com *has superlogarithmic collision-entropy in the security parameter. Then the signcryption scheme* SC *in the* $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ *paradigm is* $\mathsf{IND\text{-}qCCA}$ *secure in the multi-user outsider-security model* ($\mathsf{fM\text{-}IND\text{-}oqCCA}$ *(c.f., Section 3.1)).*

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 $\mathsf{u}_{\mathsf{quant}} = \sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} |\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}\rangle$ be any unsigncryption query and let q_s be the number of signcryption oracle queries made by $\mathcal{A}$ on $\mathsf{pk}_{\mathsf{R}^*}$ till the unsigncryption query on $\mathsf{u}_{\mathsf{quant}}$. Let $(\mathsf{u} = (\mathsf{com},\sigma,\mathsf{c}),\mathsf{pk}_\mathsf{S})$ be any basic element of $\mathsf{u}_{\mathsf{quant}}$. 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 the signcryption text $(\mathsf{u} = (\mathsf{com},\sigma,\mathsf{c}),\mathsf{pk}_\mathsf{S})$, we define the following events:

1. $\mathsf{erConceal} := [\mathsf{c} = \mathsf{c}^* \ \wedge\ (\mathsf{com},\sigma) \in \mathcal{L}\ \wedge \mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk}_{\mathsf{R}^*}) \neq \perp \wedge\ \mathsf{pk}_\mathsf{S} = \mathsf{pk}_{\mathsf{S}^*}]$.
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 $\mathsf{fM\text{-}IND\text{-}oqCCA}$ 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 $\perp$ 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 $\perp$ 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* $\mathsf{qrConcealment}$ *property of the commitment scheme* C.

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

Lemma 6.3. $\mathbf{Game}_{\mathbf{0}}$ *and* $\mathbf{Game}_{\mathbf{1}}$ *are indistinguishable under the* $\mathsf{IND\text{-}qCCA}$ *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* $\mathsf{Adv}^{\mathbf{Game_1}}_{\mathcal{A},\mathsf{SC}}(1^\lambda) \leq \mathsf{Adv}^{\mathsf{qHiding}}_{\mathcal{B},\mathsf{C}}(1^\lambda)$.

Theorem 6.4 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 6.4 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 C.5, C.6, C.7 and C.8.

Theorem 6.4. *If the primitive signature scheme* PKS *is* $\mathsf{pqsUF\text{-}CMA}$ *secure, the encryption scheme* PKE *is* $\mathsf{IND\text{-}qCCA}$ *secure and the commitment scheme* C *satisfies* $\mathsf{qfBinder}$ *and* $\mathsf{qrConcealment}$ *properties, then the signcryption scheme* SC *in the* $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ *paradigm is* $\mathsf{sUF\text{-}uqCMA}$ *secure in the multi user outsider-security model* ($\mathsf{fM\text{-}sUF\text{-}ouqCMA}$ (*c.f., Section 3.1*)).

Proof Sketch. Let $\mathcal{A}$ be a quantum PPT adversary that can break $\mathsf{fM\text{-}sUF\text{-}ouqCMA}$ 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,

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

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

The following lemma shows that Case 1 will not happen.

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

Case 2: $\mathsf{Pr}[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] \geq \frac{\epsilon}{2}$. 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 $\mathsf{m}_1, \ldots, \mathsf{m}_{q_s}$ be the messages and $\mathsf{u}_1, \ldots, \mathsf{u}_{q_s}$ be corresponding signcryption texts.

$\mathbf{Game_{Real}}$: The original $\mathsf{fM\text{-}sUF\text{-}ouqCMA}$ 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 $\mathsf{srConceal}$ 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 $\mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*})) \neq \bot$. We say that $\mathsf{srConceal}[\mathsf{u}, \mathsf{pk}_\mathsf{S}] = \mathsf{True}$ if u satisfies the event $\mathsf{srConceal}$.

$\mathbf{Game_0}$: Same as $\mathbf{Game_{Real}}$ except for the answers of unsigncryption queries. If $(\mathsf{u}, \mathsf{pk}_\mathsf{S})$ satisfies the event $\mathsf{srConceal}$, then the challenger returns $\bot$ 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 $\Pr[\mathcal{A}$ 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,* $\mathsf{Succ}_{q_s}(\mathcal{A}) \leq \mathsf{negl}(\lambda)$.

6.2 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 6.5 (for confidentiality) and 6.6 (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. The proofs closely follow the proof strategy of Theorems 6.1 and 6.2 and can be found in Appendices D.1 and D.2 respectively.

Theorem 6.5. *Suppose the primitive encryption scheme* PKE *is* pqIND-CPA *secure and the signature scheme* PKS *is* sUF-qCMA (*resp.* wUF-qCMA) *secure. Further, assume that the ciphertext has superlogarithmic collision-entropy in the security parameter. Then the signcryption scheme* SC *in the* $\mathcal{E}t\mathcal{S}$ *paradigm is* IND-qCCA (*resp.* IND-qgCCA) *secure in the two-user outsider-security model* (IND-oqCCA (*resp.* IND-oqgCCA) (*c.f., Section 3.1*)).

Theorem 6.6. *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 3.1*)).

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.

8 Conclusion

In this paper, we have formally studied quantum security of classical data in three well-known paradigms, $\mathcal{E}t\mathcal{S}$, $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$. We have shown that our results in the insider model is in the same line as in the classical setting. For showing the quantum security in the outsider models, we have utilized the quantum recording technique of Chevalier et al. [CEV20]. In the multi-user outsider model, our results strengthen the known classical results. For showing authenticity in $\mathcal{S}t\mathcal{E}$ and $\mathcal{C}t\mathcal{E}\&\mathcal{S}$ paradigms in the outsider model, we had to consider an intermediate setting, where the adversary is given classical access to signcryption oracle and superposition access to unsigncryption oracle. The full quantum security of classical data, where both the oracles are accessible in superposition remains as an open problem.

Acknowledgement. We would like to thank Dr. Christian Majenz for his comments on the earlier version of this report which helped us in polishing our work.

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.

[AGM18a] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Can you sign a quantum state?, 2018.

[AGM18b] Gorjan Alagic, Tommaso Gagliardoni, and Christian Majenz. Unforgeable Quantum Encryption. In *EUROCRYPT*, volume 10822 of *LNCS*, pages 489–519. Springer, 2018.

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In *EUROCRYPT*, volume 12107 of *LNCS*, pages 788–817. Springer, 2020.

[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.

[CEV20] Céline Chevalier, Ehsan Ebrahimi, and Quoc-Huy Vu. On Security Notions for Encryption in a Quantum World. Cryptology ePrint Archive, Report 2020/237, 2020.

[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.

[Zha19a] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *CRYPTO*, volume 11693 of *LNCS*, pages 239–268. Springer, 2019.

[Zha19b] Mark Zhandry. Quantum Lightning Never Strikes the Same State Twice. In *EUROCRYPT*, volume 11478 of *LNCS*, pages 408–438. Springer, 2019.

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

A Security Models

A.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 13. *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 10 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* $\mathcal{D}(\mathsf{c}, \mathsf{sk})$.

$\underline{\mathsf{Exp}^{\mathsf{pqIND\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda)\text{:}}$

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

Figure 10: Experiment for confidentiality (pqIND-CCA security)

Definition 14. *A public key encryption scheme* PKE = $(\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be post-quantum indistinguishable under chosen plaintext attack* (pqIND-CPA) *if it satisfies the same definition as* pqIND-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 15 ([BZ13])**.** *A public key encryption scheme* PKE = $(\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be indistinguishable under a quantum chosen ciphertext attack* (IND-qCCA) *if it satisfies the same definition as* pqIND-CCA *with the exception that the adversary is provided superposition access to decryption oracle* $\mathcal{O}_D^{\mathsf{q}}$ *(described below).*

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

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

where

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

Now, we consider the IND-qgCCA notion of security which is the quantum analogue of IND-gCCA security [ADR02]. It is defined in a way similar to IND-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:

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

Definition 16. *A public key encryption scheme* PKE = $(\mathcal{G}_{\mathcal{E}}, \mathcal{E}, \mathcal{D})$ *is said to be* IND-qgCCA *secure, if there exists some efficient decryption-respecting relation* $\mathcal{R}$ *w.r.t. which it is* qCCA *secure.*

Remark: Recently, some security models, like real-or-random [AGM18b, CEV20] have been proposed to handle indistinguishability of quantum data. However, we follow the unforgeability model of [BZ13] as we primarily focus on the quantum security of classical data.

A.2 Public Key Signature

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

- $\mathcal{G_S}$: 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 $(\mathsf{pk}, \mathsf{sk}) \longleftarrow \mathcal{G_S}(1^\lambda)$ 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 17. *A signature scheme* $\mathsf{PKS} = (\mathcal{G_S}, \mathcal{S}, \mathcal{V})$ *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*

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

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 18. *A signature scheme* $\mathsf{PKS} = (\mathcal{G_S}, \mathcal{S}, \mathcal{V})$ *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 19. *A signature scheme* $\mathsf{PKS} = (\mathcal{G_S}, \mathcal{S}, \mathcal{V})$ *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*.*

Now we define q-one-more uniforgeability (q-OMF) model [BZ13], where q is the number of sign queries. This model allows an adversary $\mathcal{A}$ to query the signature oracle on quantum superposition of several classical input values. The principle of quantum no-cloning forbids the challenger from recording $\mathcal{A}$'s queries. The adversary $\mathcal{A}$ can easily produce q message signature pairs by sampling from the superposition returned by the challenger in response to the signing queries. Hence, the requirement that $\mathcal{A}$ has to output $q+1$ forgeries is enforced in the definition. In the following, we formally define one-more uniforgeability.

Definition 20 ([BZ13]). *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is strongly existentially unforgeable under quantum chosen message attack* ($\mathsf{sUF\text{-}qCMA}$) *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 21 ([BZ13]). *A signature scheme* $\mathsf{PKS} = (\mathcal{G}_{\mathcal{S}}, \mathcal{S}, \mathcal{V})$ *is weakly existentially unforgeable under a quantum chosen message attack* ($\mathsf{wUF\text{-}qCMA}$) *if it satisfies the same definition as* $\mathsf{sUF\text{-}qCMA}$*, except the requirement that the* $q+1$ *message-signature pairs should have distinct messages.*

Remark: The OMF model has some weakness as explained in [GYZ17, Zha19b, AMRS20]. As a remedy, the authors in [AMRS20] proposed a new security model, called *blind-unforgeability* (q-BU), where an adversary $\mathcal{A}$ is allowed to ask q many queries from whole message space $\mathcal{M}$ except an ϵ-fraction subset B of $\mathcal{M}$ and then $\mathcal{A}$ has to produce a forgery for a message from B. Currently, this model is considered to be the stronger model than all existing models. However, in this paper we work on the OMF model of [BZ13] and extend it in the setting of signcryption.

A.3 Commitment

Commitment Scheme. A non-interactive commitment (C) scheme consists of three PPT algorithms: $\mathsf{CSetup}, \mathsf{Commit}$ 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 $(\mathsf{com}, \mathsf{decom})$, where com and decom are the commitment and decommitment of m respectively.
- Open: It takes as input a pair $(\mathsf{com}, \mathsf{decom})$ 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

$$\mathsf{Open}(\mathsf{Commit}(\mathsf{m}, \mathcal{CK}), \mathcal{CK})^8 = \mathsf{m}.$$

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

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

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

in $\mathsf{Exp}^{\mathsf{qHiding}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 11 is a negligible function in security parameter* λ*.*

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

- $\mathcal{CK} \longleftarrow \mathsf{CSetup}(1^\lambda)$
- $(\mathsf{m}_0, \mathsf{m}_1, st) \longleftarrow \mathcal{A}_1(1^\lambda, \mathcal{CK})$
- $b \overset{\mathrm{U}}{\longleftarrow} \{0, 1\}$
- $(\mathsf{com}^*, \mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$
- $b' \longleftarrow \mathcal{A}_2(1^\lambda, \mathcal{CK}, \mathsf{com}^*, st)$

Figure 11: Experiment for $\mathsf{qHiding}$

Definition 23. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* $\mathsf{qBinding}$ *property, if for any quantum PPT algorithm* $\mathcal{A}$ *the advantage*

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

in $\mathsf{Exp}^{\mathsf{qBinding}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 12 is a negligible function in security parameter* λ*.*

Definition 24. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* $\mathsf{qfBinder}$ *property, if for any quantum PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

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

in $\mathsf{Exp}^{\mathsf{qfBinder}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 12 is a negligible function in security parameter* λ*.*

Definition 25. *A commitment scheme* $\mathsf{C} = (\mathsf{CSetup}, \mathsf{Commit}, \mathsf{Open})$ *is said to have* $\mathsf{qrConcealment}$ *property, if for any quantum PPT algorithm* $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage*

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

in $\mathsf{Exp}^{\mathsf{qrConcealment}}_{\mathcal{A},\mathsf{C}}(\lambda)$ *defined in Figure 13 is a negligible function in security parameter* λ*.*

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

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

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

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

Figure 12: Experiment for $\mathsf{qBinding}$ and $\mathsf{qfBinder}$

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

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

Figure 13: Experiment for $\mathsf{qrConcealment}$

B Omitted Proofs in Insider Model

B.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 $\mathsf{u_{quant}} = \sum_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ 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').

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. □

B.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 $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ 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.

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 $(\mathsf{decom_0}||\mathsf{pk_{S^*}}, \mathsf{decom_1}||\mathsf{pk_{S^*}}) \longleftarrow (\mathsf{decom}^*||\mathsf{pk_{S^*}}, \mathsf{decom}_r||\mathsf{pk_{S^*}})$ and sends the same to $\mathcal{CH}$. $\mathcal{CH}$ samples $\beta \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$ and runs $\mathsf{c}^* \longleftarrow \mathcal{E}(\mathsf{decom}_\beta||\mathsf{pk_{S^*}}, \mathsf{pk_{R^*}})$ and sends it to $\mathcal{B}$. The simulator runs $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$, sets $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ and returns it 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 $\mathcal{A}$. $\mathcal{B}$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk_S}, \mathsf{m_p}, 0^{\ell_m}\rangle$. $\mathcal{B}$ then sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

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

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 $\mathcal{B}$. $\mathcal{B}$ then applies the following transformation on the obtained state

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

where

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

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

Note that the ancilla register is entangled with $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}$ uncomputes $g(\mathsf{c})$ by making decryption query on $|\mathsf{c}, g(\mathsf{c})\rangle$ to $\mathcal{CH}$ and sends the state $\sum\limits_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{pk_S},\mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p} \oplus f(\Delta)\rangle$ 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 $|\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ is handled properly. The definition of $\mathcal{R}'$ states that a query $|\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ is legitimate if one of the following conditions is false:

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

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

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

□

B.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 $(\mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$, $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}$ simulates $\mathcal{A}$'s queries as described below.

Challenge query: $\mathcal{A}$ generates sender's key pair $(\mathsf{pk}_{\mathsf{S}^*}, \mathsf{sk}_{\mathsf{S}^*})$ 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 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 $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^* \| \mathsf{pk}_{\mathsf{R}^*}, \mathsf{sk}_{\mathsf{S}^*})$ 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. $\mathcal{B}$ sets $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ and sends the same 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 $\mathcal{A}$. $\mathcal{B}$ 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

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

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

Guess: $\mathcal{A}$ sends a guess b' to $\mathcal{B}$. $\mathcal{B}$ 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 $\mathsf{qHiding}$ property of C with advantage at least ϵ. □

B.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 $\mathcal{A}$.

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

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

$$\mapsdown$$

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

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

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

$$\mapsdown$$

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

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

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

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

B.5 Proof of Lemma 5.6

Proof. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the 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 $(\mathsf{pk}_{\mathsf{S}^*},\mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_\mathcal{S}(1^\lambda)$ and returns commitment key $\mathcal{CK}$ and $\mathsf{pk}_{\mathsf{S}^*}$ to the adversary $\mathcal{A}$. $\mathcal{B}_2$ simulates $\mathcal{A}$'s queries as described below.
Signcryption queries: Let $\mathsf{m}_{\mathsf{quant}} = \sum_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \psi_{\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}} \left|\mathsf{m},\mathsf{pk}_\mathsf{R},\mathsf{u}_\mathsf{p}\right\rangle$ be any signcryption query made by $\mathcal{A}$. $\mathcal{B}_2$ applies the following unitary transformation

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

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 dM-wUF-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 qBinding property of C with probability at least $\frac{\epsilon}{2}$. □

C Omitted Proofs in Multi-User Outsider Model

C.1 Proof of Lemma 6.1

Proof. Let r be the randomness for the signcryption algorithm. The signcryption queries will be responded using compressed standard oracle $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$. This does not make any change in $\mathcal{A}$'s view thanks to Lemma

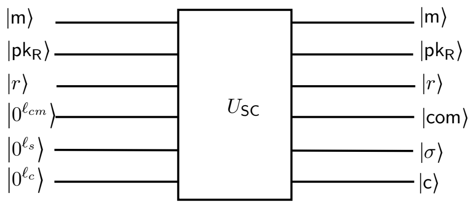


Figure 14: Quantum circuit implementing unitary U_{SC}, where all the internal oracles are handled by the simulator.

2.1. Let $\mathcal{D}$ be the database associated with $\mathsf{CStO}_{\mathcal{SC}}$. 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 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 qrConcealment property of the underlying commitment scheme with advantage δ / q_u^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 $\mathcal{B}_1$. $\mathcal{B}_1$ runs $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda), (\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ and $\mathcal{CK}$ to $\mathcal{A}$. It also picks $i \overset{\mathrm{U}}{\longleftarrow} [q_u]$ and 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 $\mathcal{B}_1$. $\mathcal{B}_1$ 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 sends the challenge signcryption text $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ to $\mathcal{A}$. $\mathcal{B}_1$ also adds $(\bot, \bot, \mathsf{u}^*)$ to the database $\mathcal{D}$.

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 $\mathcal{A}$. This will be answered using $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ oracle, where the implementation of the unitary for signcryption $U_{\mathcal{SC}}$ is given in Figure 14. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ will be updated with the tuple of the form $(\mathsf{m} || \mathsf{pk_R}, r, \mathsf{u})$ in superposition and $\mathcal{A}$'s registers will be updated with the desired output.

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, $\mathcal{B}_1$ halts the execution of $\mathcal{A}$, measures the input register for the query, and submits the corresponding com to $\mathcal{CH}$. Otherwise, $\mathcal{B}_1$ answers in the following way: First, define a search function Find over the database $\mathcal{D}$ which basically implements $\mathsf{erConceal}[\mathsf{u}, \mathsf{pk_S}]$.

$$\mathsf{Find}(\mathsf{u} || \mathsf{pk_S}, \mathcal{D}) = \begin{cases} 1 & \mathsf{c} = \mathsf{c}^* \wedge \mathsf{pk_S} = \mathsf{pk_{S^*}} \wedge (*, *, (\mathsf{com}, \sigma, *)) \in \mathcal{D} \\ 0 & \text{otherwise,} \end{cases}$$

where the $*$'s in the tuple $(*, *, (\mathsf{com}, \sigma, *)$ denote any value. The oracle $\mathcal{O_{US}}^*$ works on $|\mathsf{u} || \mathsf{pk_S}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle$ as follows:

$$\mathcal{O_{US}}^* |\mathsf{u} || \mathsf{pk_S}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle = \begin{cases} |\mathsf{u} || \mathsf{pk_S}, \mathsf{m_p} \oplus \bot\rangle) \otimes |\mathcal{D}\rangle & \text{if } (\mathsf{u}, \mathsf{pk_S}) = (\mathsf{u}^*, \mathsf{pk_{S^*}}) \vee \mathsf{Find}(\mathsf{u} || \mathsf{pk_S}, \mathcal{D}) = 1 \\ |\mathsf{u} || \mathsf{pk_S}, \mathsf{m_p} \oplus \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S})\rangle) \otimes |\mathcal{D}\rangle & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$. Note that $\mathcal{O_{US}}^*$ does not use the recorded message $\mathsf{m} || \mathsf{pk_R}$, only uses signcryption text u stored in $\mathcal{D}$ to check whether erConceal holds or not. We emphasize that the unsigncryption queries are answered in legitimate way until erConceal occurs. Even, if erConceal is true, then also it is handled perfectly as discussed in analysis.

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

$\mathsf{Analysis}$: With probability δ/q_u^2, the measurement outcome $(\mathsf{u},\mathsf{pk_S})$ satisfies the event $\mathsf{erConceal}$, i.e., $\mathsf{c} = \mathsf{c}^*$, $(\mathsf{com},\sigma) \in \mathcal{L}$, $\mathsf{Open}(\mathsf{com},\mathcal{D}(\mathsf{c},\mathsf{sk_{R^*}})) \neq \bot$ 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 $\bot$ is returned to $\mathcal{A}$. W.l.o.g, assume that $(\mathsf{com},\sigma) \in \mathcal{L} \smallsetminus \{(\mathsf{com}^*,\sigma^*)\}$. 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. By assumption, $\Pr[\mathsf{com} \neq \mathsf{com}^*]$ is negligible. Therefore, $(\mathsf{com},\mathsf{com}^*,\mathsf{decom}^*)$ is a witness for breaking $\mathsf{qrConcealment}$ property. The advantage of breaking $\mathsf{qrConcealment}$ property is at least δ/q_u^2, a contradiction. So, δ is negligible. Since the total query magnitude of signcryption texts satisfying $\mathsf{erConceal}$ is negligible, it is known that the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1.

□

C.2 Proof of Lemma 6.2

Proof. Let $r = (r_{\mathsf{com}}, r_{\mathsf{enc}}, r_{\mathsf{sign}})$ be the randomness for the signcryption algorithm. Here the signcryption queries will be responded using compressed standard oracle $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{com}},r_{\mathsf{enc}}\rangle}$. This does not make any change in $\mathcal{A}$'s view thanks to Lemmas 2.1 and 2.2. Let $\mathcal{D}$ be the database associated with $\mathsf{CStO}_{\mathcal{SC}}$. 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 $\mathsf{sUF\text{-}qCMA}$ security of PKS with advantage δ/q_u^2.

Let $\mathcal{CH}$ be the challenger for the signature scheme PKS. $\mathcal{CH}$ first runs $(\mathsf{pk_{S^*}},\mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and gives $\mathsf{pk_{S^*}}$ to $\mathcal{B}_2$. $\mathcal{B}_2$ runs the setup of the commitment scheme, $(\mathsf{pk_{R^*}},\mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda)$ and forwards the public commitment key $\mathcal{CK}$, $\mathsf{pk_{S^*}}$ and $\mathsf{pk_{R^*}}$ to $\mathcal{A}$. $\mathcal{B}_2$ also samples $i \xleftarrow{\text{U}} [q_u]$ 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 $\mathcal{B}_2$. $\mathcal{B}_2$ samples $b \xleftarrow{\text{U}} \{0,1\}$, runs $(\mathsf{com}^*,\mathsf{decom}^*) \longleftarrow \mathsf{Commit}(\mathsf{m}_b)$ and sends a signature query on $\mathsf{com}^*||\mathsf{pk_{R^*}}$ to $\mathcal{CH}$. $\mathcal{CH}$ computes $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}},\mathsf{sk_{S^*}})$ 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 $\mathcal{A}$. $\mathcal{B}_2$ also adds $(\bot,\bot,\mathsf{u}^*)$ to the database $\mathcal{D}$.

$\mathsf{Signcryption\ queries}$: 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 $\mathcal{A}$. This will be answered using $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{com}},r_{\mathsf{enc}}\rangle}$ oracle, where the implementation of the unitary for signcryption $U_{\mathcal{SC}}$ is given in Figure 15. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{com}},r_{\mathsf{enc}}\rangle}$ will be updated with the tuple of the form $(\mathsf{m}||\mathsf{pk_R},(r_{\mathsf{com}},r_{\mathsf{enc}}),\mathsf{u})$ in superposition and $\mathcal{A}$'s registers will be updated with the desired output.

$\mathsf{Unsigncryption\ queries}$: 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 $\mathcal{A}$. If it is the i^{th} unsigncryption query, $\mathcal{B}_2$ halts the execution of $\mathcal{A}$ and measures the input register for the query. Let $(\mathsf{com}||\mathsf{pk_{R^*}},\sigma)$ be the output of the measurement. Then $\mathcal{B}_2$ measures each state of the database $\mathcal{D}$ and outputs $\{(\mathsf{com}||\mathsf{pk_{R^*}},\sigma)\} \cup \{\mathsf{com}^*||\mathsf{pk_{R^*}},\sigma^*)\} \cup \{(\mathsf{com}_k||\mathsf{pk}_{\mathsf{R}}^{(k)},\sigma_k) : k \in [q_s]\}$, where $(\mathsf{u}_k = (\mathsf{com}_k,\sigma_k,\mathsf{c}_k),\mathsf{pk}_{\mathsf{R}}^{(k)})$ is the k^{th} signcryption and receiver's identity pair after measuring $\mathcal{D}$, and q_s is the number of signcryption queries till i^{th} unsigncryption query. Otherwise, $\mathcal{B}_2$ answers in the following way: First, define a search function Find over the database $\mathcal{D}$ which basically implements $\mathsf{Forge}[\mathsf{u},\mathsf{pk_S}]$ and

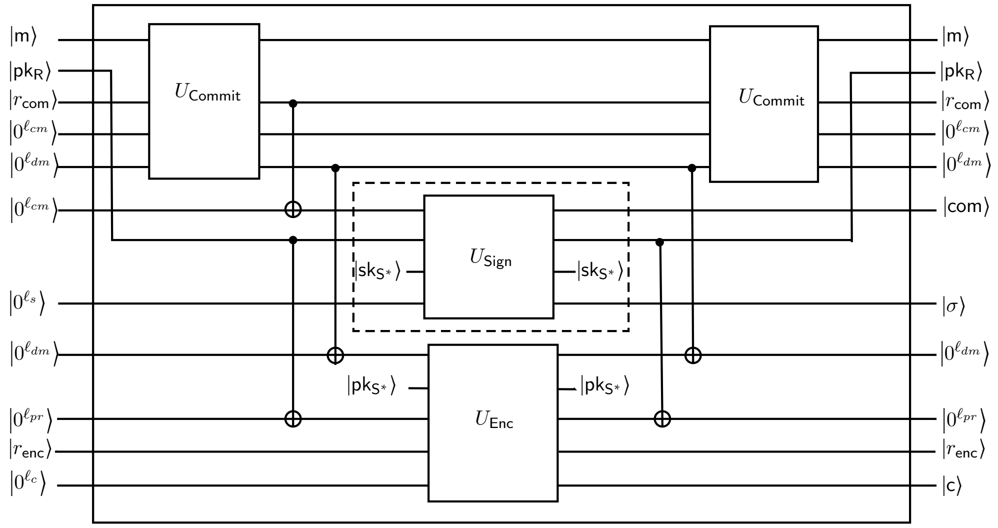


Figure 15: Quantum circuit implementing unitary U_{SC}, where both the unitary operations U_{Commit} and U_{Enc} are handled by the simulator, but U_{Sign} is handled by the challenger of the underlying signature scheme.

erConceal$[\mathsf{u}, \mathsf{pk_S}]$ together.

$$\mathsf{Find}(\mathsf{u}||\mathsf{pk_S}, \mathcal{D}) = \begin{cases} 1 & \mathsf{c} = \mathsf{c}^* \wedge \mathsf{pk_S} = \mathsf{pk_{S^*}} \wedge (*, *, (\mathsf{com}, \sigma, *)) \in \mathcal{D} \\ 1 & \mathcal{V}(\mathsf{com}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_{S^*}}) = 1 \wedge \mathsf{pk_S} = \mathsf{pk_{S^*}} \wedge (*, *, (\mathsf{com}, \sigma, *)) \notin \mathcal{D} \\ 0 & \text{otherwise.} \end{cases}$$

The oracle $\mathcal{O_{US}}^*$ works on $|\mathsf{u}||\mathsf{pk_S}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle$ as follows:

$$\mathcal{O_{US}}^* |\mathsf{u}||\mathsf{pk_S}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle = \begin{cases} |\mathsf{u}||\mathsf{pk_S}, \mathsf{m_p} \oplus \perp\rangle) \otimes |\mathcal{D}\rangle & \text{if } (\mathsf{u}, \mathsf{pk_S}) = (\mathsf{u}^*, \mathsf{pk_{S^*}}) \vee \mathsf{Find}(\mathsf{u}||\mathsf{pk_S}, \mathcal{D}) = 1 \\ |\mathsf{u}||\mathsf{pk_S}, \mathsf{m_p} \oplus \mathcal{US}(\mathsf{u}, \mathsf{sk_{R^*}}, \mathsf{pk_S})\rangle) \otimes |\mathcal{D}\rangle & \text{otherwise.} \end{cases}$$

The resulting state is sent back to $\mathcal{A}$. Similar to Lemma 6.1, the unsigncryption queries are answered in legitimate way based on the analysis below.

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

Analysis: We have to show that $\mathcal{A}$'s queries are handled perfectly. It suffices to justify why $\mathsf{m_p} \oplus \perp$ is returned when the 2nd condition of Find is true. If we can show that δ is negligible, then the advantage of $\mathcal{A}$ is only changed by negligible amount by using Lemma 5.1. Moreover, since each time the commitment part of the signcryption queries (including challenge) are answered by sampling fresh random coin r_{com}, so by assumption the collision probability of any two commitments in $\{\mathsf{com}^*\} \cup \{\mathsf{com}_k : k \in [q_s]\}$ is negligible. So, except with some negligible probability, all the pairs in the output of $\mathcal{B}_2$ are distinct. The number of signature queries is $q_s + 1$, whereas the number of forgeries is $q_s + 2$. Hence, $\mathcal{B}_2$ breaks the sUF-qCMA security of PKS with probability at least δ/q_u^2. The sUF-qCMA 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. □

C.3 Proof of Lemma 6.3

Proof. Let r be the randomness used in the signcryption algorithm. Here the signcryption queries will be responded using compressed standard oracle $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$. This does not make any change in $\mathcal{A}$'s view thanks to Lemma 2.1. 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 $\mathcal{A}$. $\mathcal{B}_3$ 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 $\mathsf{u}^* \coloneqq (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ and returns it to $\mathcal{A}$. $\mathcal{B}_3$ also adds $(\bot, \bot, \mathsf{u}^*)$ to the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}$.

$\mathsf{Signcryption\ queries}$: It is handled similar to Lemma 6.1.

$\mathsf{Unsigncryption\ queries}$: 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

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

$\mathcal{CH}$ 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

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

In the above expression $\Delta = (\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, g(\mathsf{c}))$ and description of Find is the same as defined in the proof of Lemma 6.2. Before returning the answer to $\mathcal{A}$, $\mathcal{B}_3$ uncomputes $g(\mathsf{c})$ by making decryption query on $|\mathsf{c}, g(\mathsf{c})\rangle$ to $\mathcal{CH}$.

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

$\mathsf{Analysis}$: 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. By definition, a query $|\mathsf{u}, \mathsf{pk}_{\mathsf{S}}, \mathsf{m}_{\mathsf{p}}\rangle$ is legitimate if $(\mathsf{u}, \mathsf{pk}_{\mathsf{S}}) \neq (\mathsf{u}^*, \mathsf{pk}_{\mathsf{S}^*})$. We consider the following cases:

1. $\mathsf{Forge}[\mathsf{u}, \mathsf{pk}_{\mathsf{S}}] = \mathsf{True}$

2. $\mathsf{Forge}[\mathsf{u}, \mathsf{pk}_{\mathsf{S}}] = \mathsf{False} \land \mathsf{c} \neq \mathsf{c}^*$

3. $\mathsf{Forge}[\mathsf{u}, \mathsf{pk_S}] = \mathsf{False} \wedge \mathsf{c} = \mathsf{c}^*$

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$_1$) $\mathcal{V}(\mathsf{com}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_{S^*}}) = 0 \vee \mathsf{pk_S} \neq \mathsf{pk_{S^*}}$, (a$_2$) $(\mathsf{com}, \sigma) \in \mathcal{L} \wedge \mathcal{V}(\mathsf{com}||\mathsf{pk_{R^*}}, \sigma, \mathsf{pk_{S^*}}) = 1 \wedge \mathsf{pk_S} = \mathsf{pk_{S^*}}$. 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 (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

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

□

C.4 Proof of Lemma 6.4

Proof. As in previous lemmas, the signcryption queries will be responded using compressed standard oracle $\mathsf{CStO}^{|r\rangle}_{\mathcal{SC}}$, where r is randomness used in the signcryption algorithm. This does not make any change in $\mathcal{A}$'s view thanks to Lemma 2.1. 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 $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G_E}(1^\lambda), (\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G_S}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$, $\mathsf{pk_{S^*}}$ 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.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ submits two equal length messages $\mathsf{m_0}$ and $\mathsf{m_1}$ 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 $\sigma^* \longleftarrow \mathcal{S}(\mathsf{com}^*||\mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ 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. $\mathcal{B}_4$ adds $(\mathsf{com}^*, \sigma^*)$ to $\mathcal{L}$ and sends the challenge signcryption text $\mathsf{u}^* := (\mathsf{com}^*, \sigma^*, \mathsf{c}^*)$ to $\mathcal{A}$. $\mathcal{B}_4$ also adds $(\perp, \perp, \mathsf{u}^*)$ to the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}$.

$\mathsf{Signcryption\ queries}$: It is handled similar to Lemma 6.1.

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

$$f(\mathsf{u},\mathsf{pk}_\mathsf{S}) = \begin{cases} \perp & \text{if } (\mathsf{u}^*,\mathsf{pk}_{\mathsf{S}^*}) = (\mathsf{u},\mathsf{pk}_\mathsf{S}) \vee \mathsf{Find}(\mathsf{u}||\mathsf{pk}_\mathsf{S},\mathcal{D}) = 1 \\ \mathcal{US}(\mathsf{u},\mathsf{sk}_{\mathsf{R}^*},\mathsf{pk}_\mathsf{S}) & \text{otherwise.} \end{cases}$$

Here the description of Find is the same as defined in the proof of Lemma 6.2. 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 qHiding property of C with advantage at least ϵ. □

C.5 Proof of Lemma 6.5

Proof. We construct a quantum PPT algorithm $\mathcal{B}_1$ which breaks the pqsUF-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 pqsUF-CMA security of PKS with probability at least $\frac{\epsilon}{2}$. □

C.6 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 $(\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p})$ involved in the i^{th} unsigncryption query for which the event 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 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 6.4. 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 $(\mathsf{pk}_{\mathsf{R}^*},\mathsf{sk}_{\mathsf{R}^*}) \longleftarrow \mathcal{G}_\mathcal{E}(1^\lambda), (\mathsf{pk}_{\mathsf{S}^*},\mathsf{sk}_{\mathsf{S}^*}) \longleftarrow \mathcal{G}_\mathcal{S}(1^\lambda)$ and sends $\mathsf{pk}_{\mathsf{R}^*}$, $\mathsf{pk}_{\mathsf{S}^*}$ and $\mathcal{CK}$ to $\mathcal{A}$. $\mathcal{B}_2$ creates a list $\mathcal{L}$ which is initially empty. It also picks $i \xleftarrow{U} [q_u]$ and $j_* \xleftarrow{U} [q_s]$ 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 $\mathsf{u_{quant}} = \sum\limits_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} \psi_{\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}} |\mathsf{u}, \mathsf{pk_S}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. If it is the i^{th} unsigncryption query 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

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

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 $\mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk_{R^*}})) \neq \bot$. 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. □

C.7 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 $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ and sends $\mathsf{pk_{R^*}}$ to $\mathcal{B}_3$. $\mathcal{B}_3$ runs $(\mathsf{pk_{S^*}}, \mathsf{sk_{S^*}}) \longleftarrow \mathcal{G}_{\mathcal{S}}(1^\lambda)$, the setup algorithm of the commitment scheme and forwards the public commitment key $\mathcal{CK}$, $\mathsf{pk_{S^*}}$ and $\mathsf{pk_{R^*}}$ to $\mathcal{A}$. $\mathcal{B}_3$ creates a list $\mathcal{L}$ (initially empty) simulates $\mathcal{A}$'s queries as described below.

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

- (First $j-1$ queries). $\mathcal{B}_3$ runs $(\mathsf{com}, \mathsf{decom}) \longleftarrow \mathsf{Commit}(\mathsf{m})$, $\sigma \longleftarrow \mathcal{S}(\mathsf{com} || \mathsf{pk_{R^*}}, \mathsf{sk_{S^*}})$ and $\mathsf{c} \longleftarrow \mathcal{E}(\mathsf{decom}_r || \mathsf{pk_{S^*}}; \mathsf{pk_{R^*}})$, 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 $b \overset{\mathrm{U}}{\longleftarrow} \{0,1\}$, 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.

$\mathsf{Unsigncryption\ queries}$: 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 $\left|0^{\ell_m}\right\rangle$, to the query and obtains the state $\sum_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \psi_{\mathsf{u},\mathsf{pk}_\mathsf{S},\mathsf{m}_\mathsf{p}} \left|\mathsf{com}, \sigma, \mathsf{c}, \mathsf{pk}_\mathsf{S}, \mathsf{m}_\mathsf{p}, 0^{\ell_m}\right\rangle$. $\mathcal{B}_3$ then sends a decryption query consisting of 3^{rd} and 6^{th} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

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

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 $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}_3$ uncomputes $g(\mathsf{u})$ by making decryption query on $|\mathsf{u}, g(\mathsf{u})\rangle$ to $\mathcal{CH}$ 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 $\mathcal{A}$.

$\mathsf{Forgery}$: $\mathcal{A}$ 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 $\perp$ 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 $f(\Delta) = \perp$ 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 $\mathsf{Open}(\mathsf{com}, \mathcal{D}(\mathsf{c}, \mathsf{sk}_{\mathsf{R}^*})) \neq \perp$, 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 $\perp$ 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. □

C.8 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.

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 $\mathcal{A}$.

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 $\epsilon'/(2 \cdot q_s)$. □

D Omitted Proofs in Two-User Outsider Model

D.1 Proof of Theorem 6.5

Proof. Here, we only prove the IND-qgCCA security of SC in the outsider model. The proof of IND-qCCA follows similarly. We use the compressed oracle technique [CEV20] for answering signcryption and

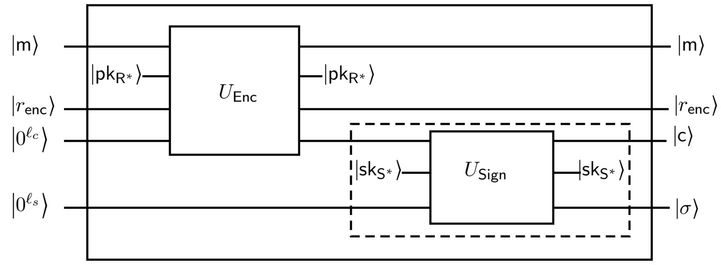

$|\mathsf{m}\rangle$
$|r_{\mathsf{enc}}\rangle$
$|0^{\ell_c}\rangle$
$|0^{\ell_s}\rangle$
$|\mathsf{pk}_{\mathsf{R}^*}\rangle$
U_{Enc}
$|\mathsf{pk}_{\mathsf{R}^*}\rangle$
$|\mathsf{sk}_{\mathsf{S}^*}\rangle$
U_{Sign}
$|\mathsf{sk}_{\mathsf{S}^*}\rangle$
$|\mathsf{m}\rangle$
$|r_{\mathsf{enc}}\rangle$
$|\mathsf{c}\rangle$
$|\sigma\rangle$

Figure 16: Quantum circuit implementing unitary U_{SC}, where the unitary bounded by dashed line is handled by the challenger of the underlying signature scheme.

unsigncryption queries. Let $r = (r_{\mathsf{enc}}, r_{\mathsf{sign}})$ denote the randomness of the signcryption algorithm. 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 $\mathsf{IND\text{-}qgCCA}$ 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 $\mathsf{wUF\text{-}qCMA}$ security of the underlying signature scheme PKS. Note that,

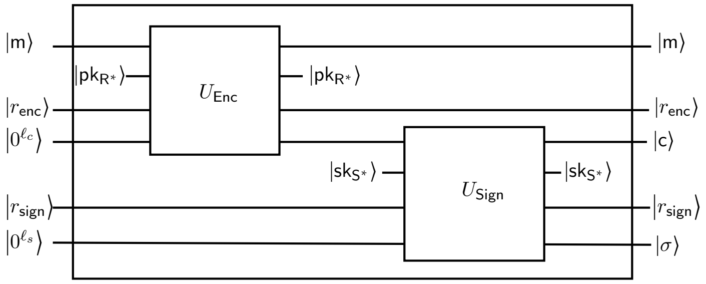
$$\epsilon \leq \Pr[\mathcal{A} \text{ succeeds}] - \frac{1}{2} = \Pr[\mathcal{A} \text{ succeeds} \wedge \mathsf{Forge}] + \Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}] - \frac{1}{2}$$
$$\leq \Pr[\mathsf{Forge}] + \left(\Pr[\mathcal{A} \text{ succeeds} \wedge \overline{\mathsf{Forge}}]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

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 $\mathsf{wUF\text{-}qCMA}$ 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.

$\mathsf{Challenge\ query}$: $\mathcal{A}$ 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 $\mathcal{A}$.

$\mathsf{Signcryption\ queries}$: 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 any signcryption query made by $\mathcal{A}$. This will be answered using $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{enc}}\rangle}$ oracle, where the implementation of $U_{\mathcal{SC}}$ used in $\mathsf{CStO}_{\mathcal{SC}}$ is given in Figure 16. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{enc}}\rangle}$ will be updated with the tuple of the form $(\mathsf{m}, r_{\mathsf{enc}}, \mathsf{u})$ in superposition and adversary's registers will be updated with the desired output.

$\mathsf{Unsigncryption\ queries}$: 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 $\mathcal{A}$. 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 let



$|\mathsf{m}\rangle$
$|\mathsf{pk}_{\mathsf{R}^*}\rangle$
$|r_{\mathsf{enc}}\rangle$
$|0^{\ell_c}\rangle$
U_{Enc}
$|\mathsf{pk}_{\mathsf{R}^*}\rangle$
$|\mathsf{sk}_{\mathsf{S}^*}\rangle$
U_{Sign}
$|\mathsf{sk}_{\mathsf{S}^*}\rangle$
$|r_{\mathsf{sign}}\rangle$
$|0^{\ell_s}\rangle$
$|\mathsf{m}\rangle$
$|r_{\mathsf{enc}}\rangle$
$|\mathsf{c}\rangle$
$|r_{\mathsf{sign}}\rangle$
$|\sigma\rangle$

Figure 17: Quantum circuit implementing unitary U_{SC}, where both the unitary operations U_{Enc} and U_{Sign} are handled by the simulator.

(c,σ) be the outcome. Then $\mathcal{B}_1$ measures each state of the database $\mathcal{D}$ and outputs $\{(\mathsf{c},\sigma)\} \cup \{(\mathsf{c}^*,\sigma^*)\} \cup \{(\mathsf{c}_k,\sigma_k) : k \in [q_s]\}$, where $\mathsf{u}_k = (\mathsf{c}_k,\sigma_k)$ is the k^{th} signcryption text after measuring $\mathcal{D}$ and q_s is the number of signcryption queries till i^{th} unsigncryption query. 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: Based on Lemma 2.1, we can replace $\mathcal{O}_{\mathcal{SC}}$ by $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ (which purifies r). Further, the oracles $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ and $\mathsf{CStO}_{\mathcal{SC}}^{|r_{\mathsf{enc}}\rangle}$ are equivalent thanks to Lemma 2.2. Therefore, all the signcryption queries are answered perfectly from adversary's point of view. By the definition of Forge, $\mathsf{c} \notin \{\mathsf{c}^*\} \cup \{\mathsf{c}_k : k \in [q_s]\}$. Moreover, since each time the ciphertexts in the signcryption queries (including challenge) are answered by sampling fresh randomness, so by assumption the collision probability of any two ciphertexts in $\{\mathsf{c}^*\} \cup \{\mathsf{c}_k : k \in [q_s]\}$ is negligible. Therefore, except with some negligible probability, all the ciphertexts in the output of $\mathcal{B}_1$ are distinct. Hence, $\mathcal{B}_1$ breaks the $\mathsf{wUF\text{-}qCMA}$ security of PKS with probability at least $\epsilon \cdot \mu/(2 \cdot q_u)$.

Case 2: $\Pr[\mathcal{A}$ **succeeds** $\wedge \overline{\mathsf{Forge}}] - \frac{1}{2} \geq \frac{\epsilon}{2}$**.** Here, the actual oracles $(\mathcal{O}_{\mathcal{SC}},\mathcal{O}_{\mathcal{US}})$ will be replaced by $(\mathsf{CStO}_{\mathcal{SC}},\mathsf{CInvO}_{\mathcal{US}})$ thanks to Lemma 2.3. We construct a quantum PPT algorithm $\mathcal{B}_2$ which breaks the $\mathsf{pqIND\text{-}CPA}$ 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 $\mathsf{u}^* := (\mathsf{c}^*,\sigma^*)$ and returns it to $\mathcal{A}$. $\mathcal{B}_2$ also adds $(\perp,\perp,\mathsf{u}^*)$ to the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$.

Signcryption queries: 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 any signcryption query made by $\mathcal{A}$. This will be answered using $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ oracle, where the implementation of $U_{\mathcal{SC}}$ used in $\mathsf{CStO}_{\mathcal{SC}}$ is given in Figure 17. After each query, the database $\mathcal{D}$ associated with $\mathsf{CStO}_{\mathcal{SC}}^{|r\rangle}$ will be updated with the tuple of the form $(\mathsf{m},r,\mathsf{u})$ in superposition and $\mathcal{A}$'s registers will be updated with the desired output.

$\mathsf{Unsigncryption\ queries}$: Let $\mathsf{u_{quant}} = \sum_{\mathsf{u,m_p}} \psi_{\mathsf{u,m_p}} |\mathsf{u}, \mathsf{m_p}\rangle$ be any unsigncryption query made by $\mathcal{A}$. It will be answered using $\mathsf{CInvO}_{\mathcal{US}}$ oracle as follows. First, define $\mathsf{FindImage}^*$ for searching the database $\mathcal{D}$.

$$\mathsf{FindImage}^*(\mathsf{u}, \mathcal{D}) = \begin{cases} (1, \mathsf{m}) & \text{if there exists } (\mathsf{m}, r, \mathsf{u}') \in \mathcal{D} \text{ s.t } \mathcal{R}'(\mathsf{u}, \mathsf{u}') = \mathsf{True} \\ (0, 0^{\ell_m}) & \text{otherwise.} \end{cases}$$

The oracle $\mathsf{CInvO}_{\mathcal{US}}$ works on $|\mathsf{u}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle$ as follows:

$$\mathsf{CInvO}_{\mathcal{US}} |\mathsf{u}, \mathsf{m_p}\rangle \otimes |\mathcal{D}\rangle = \begin{cases} |\mathsf{u}, \mathsf{m_p} \oplus \mathsf{m}\rangle \otimes |\mathcal{D}\rangle & \text{if } \mathsf{FindImage}^*(\mathsf{u}, \mathcal{D}) = (1, \mathsf{m}) \\ \left|\mathsf{u}, \boxed{\mathsf{m_p} \oplus \bot}\right\rangle \otimes |\mathcal{D}\rangle & \text{if } \mathsf{FindImage}^*(\mathsf{u}, \mathcal{D}) = (0, 0^{\ell_m}). \end{cases}$$

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

$\mathsf{Analysis}$: We show that $\mathcal{B}$ simulates $\mathcal{A}$'s unsigncryption queries properly. Basically, we have to give the justification of the answer (in the box) using $\mathsf{CInvO}_{\mathcal{US}}$. 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 $\mathcal{V}(\mathsf{c}, \sigma, \mathsf{pk_{S^*}}) = 1$ and c was not a result of any previous signcryption oracle or challenge query is 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. □

D.2 Proof of Theorem 6.6

Proof. Here, we only prove the $\mathsf{wUF\text{-}uqCMA}$ security of SC in the outsider model. The proof of $\mathsf{sUF\text{-}ouqCMA}$ follows similarly. Let $\mathcal{R}$ be the equivalence relation w.r.t. which PKE is $\mathsf{IND\text{-}qgCCA}$ 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., $\mathsf{u}_j \longleftarrow \mathcal{E}(0^{\ell_m}; \mathsf{pk_{R^*}})$. 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 $(\mathsf{pk_{R^*}}, \mathsf{sk_{R^*}}) \longleftarrow \mathcal{G}_{\mathcal{E}}(1^\lambda)$ 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.

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).

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 $\mathcal{A}$. $\mathcal{B}_1$ appends an ℓ_m qubit ancilla register, containing the state $|0^{\ell_m}\rangle$, to the query and obtains the state $\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p}, 0^{\ell_m}\rangle$. $\mathcal{B}_1$ then sends a decryption query consisting of 1^{st} and 3^{rd} register to $\mathcal{CH}$. $\mathcal{CH}$ applies the following unitary transformation

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

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

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

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 $\mathcal{A}$'s registers. For perfect simulation, $\mathcal{B}_1$ uncomputes $g(\mathsf{u})$ by making decryption query on $|\mathsf{u}, g(\mathsf{u})\rangle$ to $\mathcal{CH}$ and sends the state $\sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p} \oplus f(\Delta)\rangle$ 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 $\mathsf{u_{quant}} = \sum_{\mathsf{u},\mathsf{m_p}} \psi_{\mathsf{u},\mathsf{m_p}} |\mathsf{u}, \mathsf{m_p}\rangle$ 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

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

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

Forgery: $\mathcal{A}$ outputs a forgery u. $\mathcal{B}_2$ runs $(\mathsf{m}, \sigma) \longleftarrow \mathcal{D}(\mathsf{u}, \mathsf{sk_{R^*}})$ 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. $\square$