Quantum-Secure Aggregate One-time Signatures with Detecting Functionality*

Shingo Sato† Junji Shikata†

February 28, 2022

Abstract

An aggregate signature (ASIG) scheme allows any user to compress multiple signatures into a short signature called an aggregate signature. While a conventional ASIG scheme cannot detect any invalid messages from an aggregate signature, an ASIG scheme with detecting functionality (D-ASIG) has an additional property which can identify invalid messages from aggregate signatures. Hence, D-ASIG is useful to reduce the total amount of signature-sizes on a channel. On the other hand, development of quantum computers has been advanced recently. However, all existing D-ASIG schemes are insecure against attacks using quantum algorithms, which we call quantum attacks. In this paper, we propose a D-ASIG scheme with quantum-security which means security in a quantum setting. Hence, we first introduce quantum-security notions of ASIGs and D-ASIGs because there is no research on such security notions for (D-)ASIGs. Second, we propose a lattice-based aggregate one-time signature scheme with detecting functionality, and prove that this scheme satisfies our quantum-security in the quantum random oracle model and the certified key model. Hence, this scheme is the first quantum-secure D-ASIG.

1 Introduction

Background and Related Work. Digital signature is a fundamental primitive in public key cryptography that ensures integrity of data. The range of applications of this primitive is very wide since publicly verification of data is very useful in many situations. However, when checking validity of multiple messages simultaneously, a total amount of signature-sizes transmitted on a channel (e.g., the internet) is too large, since the total size of signatures is proportional to the number of all the messages. In order to reduce such an amount of signature-sizes, we can use an aggregate signature (ASIG) scheme which compresses multiple signatures into a short signature called an aggregate signature. Boneh et al. introduced the notion of ASIGs and proposed a pairing-based scheme in the random oracle model (ROM) [4]. Under the certified key model in which each signer has to prove knowledge of its secret key in order to certify the corresponding public key, Rückert and Schröder gave a multilinear map-based ASIG scheme without random oracles [27]. Hohenberger, Sahai, and Waters presented (identity-based) ASIG schemes without random oracles by using multilinear maps [15]. Boneh and Kim proposed an aggregate one-time signature (AOTS) and an interactive ASIG based on lattice problems [5]. In addition, other types of aggregate signature schemes have also been researched. Gentry and Ramzan constructed the first (identity-based) synchronized ASIG scheme which aggregates only signatures with the same value [13]. Under this restriction, it is possible to construct ASIG schemes with some properties (e.g., ASIGs without pairing). Thus,

*This paper is the full version of our paper which appears at AINA 2022.

†Yokohama National University, Yokohama, Japan. sato-shingo-zk@ynu.ac.jp, shikata-junji-rb@ynu.ac.jp.

several synchronized ASIG schemes have been proposed in [13, 1, 16]. Lysyanskaya, Micali, Reyzin, and Shacham introduced sequential ASIGs which allows each signer to add his/her signature into the previous aggregate signature, in order [22]. Because there are several useful applications of sequential ASIGs, many schemes have been proposed in [22, 20, 2, 26, 8, 11, 19, 12]. Hartung et al. [14] proposed a fault-tolerant ASIG that has functionality of both aggregating multiple signatures and identifying invalid messages from an aggregate signature. In particular, Sato, Shikata, and Matsumoto introduced the notion of ASIGs with detecting functionality (D-ASIGs) which can detect invalid messages, and proposed D-ASIG schemes by combining ASIGs with group-testing in a comprehensive way [29]. Since the detecting property of D-ASIGs with a total amount of small signature-size is useful, we focus on this topic in public key cryptography.

Furthermore, development of quantum computers has been advanced recently, and many researchers have paid much attention to constructing cryptographic protocols secure against attacks using quantum algorithms, which we call quantum attacks. In particular, we focus on the security model where an adversary is allowed to issue a quantum query (i. e., a quantum superposition of queries) to the signing oracle in a security game [7]. This is because this security model expresses a practical situation where sufficiently large quantum computers are realized. Regarding existing researches, Boneh et al. introduced the security model in which an adversary can issue quantum queries to random oracles (called the quantum random oracle model). Since then, many cryptosystems in security models where issuing quantum queries is allowed have been researched actively (e.g., [33, 32, 7, 6, 31, 28, 18]). Regarding digital signatures, Boneh and Zhandry gave a formalization of security in this model [7], which we call *quantum-security* in this paper, and proposed signature schemes satisfying this formalized quantum-security. As for (D-)ASIGs, however, there is no research on quantum-security. Furthermore, all existing D-ASIG schemes are insecure against quantum attacks by using several quantum algorithms such as Shor's algorithm [30]. Hence, it is important to research quantum-secure D-ASIG schemes.

Contribution. Our goal is to propose a quantum-secure D-ASIG scheme. To this end, we first formalize quantum-security notions of (D-)ASIGs since there is no research on (D-)ASIGs in the security model where an adversary can issue quantum queries to given oracles. Next, we show that a generic construction of quantum-secure D-ASIGs satisfies our formalized security. Then, we present a concrete aggregate one-time signature (AOTS) scheme which can be applied to the generic construction. This implies that the resulting scheme is quantum-secure. Details on our contribution are shown as follows:

- First, we formalize quantum-security notions of ASIGs and D-ASIGs, namely, security notions in the model where an adversary is allowed to issue quantum queries to the signing oracle in a (D-)ASIG's security game. Following a definition of quantum-security for digital signatures [7], we give quantum-security definitions for ASIGs and D-ASIGs.

- Second, we propose a quantum-secure AOTS scheme with detecting functionality (D-AOTS). To this end, we prove that a generic construction starting from a quantum-secure ASIG scheme and a non-adaptive group testing protocol is a quantum-secure D-ASIG. Then, in order to obtain a quantum-secure D-ASIG, we propose a lattice-based AOTS scheme satisfying the formalized quantum-security of ASIGs in the quantum random oracle model [3] and the certified key model [21, 27]. Notice that it is widely believed that lattice problems are computationally hard even if it is possible to utilize quantum algorithms. Hence, the resulting D-AOTS scheme is quantum-secure in the quantum random oracle model and the certified key model. We claim that this proposed scheme is the first quantum-secure D-ASIG, and would be useful like [14, 29] in a quantum era.

Table 1: Comparison of D-ASIG schemes

Scheme	Underlying Primitives	Unforgeability	Identifiability	Certificateless Model ?	Total Aggregate Signature-Size
HKKKR	ASIG [4]	aggUF against cCMA	CMP and wSND against cCMA	✓	$O(d^2 \log \ell)\|\sigma\|$
SSM	ASIG [4] and SNARK [24]	aggUF against cCMA	CMP and SND against cCMA	✓	$O(d^2 \log \ell)(\|\sigma\| + \|\pi\|)$
Our Scheme	AOTS in Section 4	aggUF against qCMA	CMP and wSND against qCMA		$O(d^2 \log \ell)\|\sigma\|$

HKKKR and SSM are concrete D-ASIG schemes which are constructed by applying the schemes described in "Underlying Primitives" to generic constructions proposed in [14] and [29], respectively. SNARK means succinct non-interactive argument of knowledge. The terms "Unforgeability" and "Identifiability" are the security notions of D-ASIGs, which were formalized in [29]. cCMA and qCMA mean "classical chosen message attacks" and "quantum chosen message attacks", respectively. aggUF means "aggregate unforgeability". CMP and SND (resp., wSND) mean completeness and soundness (resp., a weak variant of soundness) of the identifiability of D-ASIGs. Certificateless model means a model where key-registration is unnecessary. ℓ (resp. d) is the total number of messages (resp. the maximum number of invalid messages). $|\sigma|$ (resp. $|\pi|$) is the bit-length of the signature of underlying ASIG (resp. the proof of underlying SNARK).

Furthermore, we compare D-ASIG schemes in order to clarify the difference between existing D-ASIG schemes and our scheme. Table 1 shows a comparison of D-ASIG schemes. Notice that ASIGs with interactive tracing functionality [17] are not included in this comparison because the security model of [17] is different from that of [14, 29]. Regarding the underlying primitives applied to generic constructions of [14, 29], we have selected schemes whose signature/proof-lengths are the shortest of existing schemes. First, the advantage of our scheme is summarized as follows: From the terms "Unforgeability" and "Identifiability" in Table 1, we see that our scheme satisfies the formalized quantum-security while all existing schemes achieve security only in classical security models. As described before, it should be noted that all existing D-ASIGs are insecure against quantum attacks. As another advantage of our scheme, the increment of a total aggregate signature-size of our scheme is not larger than that of any existing one, even though our scheme achieves security in a quantum setting. Second, the disadvantage of our scheme lies in that each signer with a key-pair can generate only one signature, and the security of ours is ensured in the certified key model.

2 Preliminaries

Notation. In this paper, we use the following notation: For a positive integer n, let $[n] := \{1, \ldots, n\}$. For n values $x_1, \ldots, x_n$ and a subset $I \subseteq [n]$ of indexes, let $(x_i)_{i \in I}$ be a sequence of values whose indexes are in I, and let $\{x_i\}_{i \in I}$ be a set of values whose indexes are in I. For a vector $\boldsymbol{x}$ with dimension n, let x_i be the i-th entry ($i \in [n]$). For a $m \times n$ matrix $\boldsymbol{X}$, let $x_{i,j}$ be the entry at the i-th row and the j-th column ($i \in [m]$, $j \in [n]$). For a function $f : \mathbb{N} \to \mathbb{R}$, if $f(\lambda) = o(\lambda^{-c})$ for arbitrary positive c, then f is negligible in λ, and we write $f(\lambda) = \mathsf{negl}(\lambda)$. For $\lambda \in \mathbb{N}$, let $\mathsf{poly}(\lambda)$ be a universal polynomial in λ. A probability is overwhelming if it is $1 - \mathsf{negl}(\lambda)$. In addition, we use the following notation for quantum computation. We write an n-qubit state $|\psi\rangle$ as a linear combination $|\psi\rangle = \sum_{x \in \{0,1\}^n} \psi_x |x\rangle$ with a basis $\{|x\rangle\}_{x \in \{0,1\}^n}$ and amplitudes $\psi_x \in \mathbb{C}$ such that $\sum_{x \in \{0,1\}^n} |\psi_x|^2 = 1$. When $|\psi\rangle$ is measured, a state x is observed with probability $|\psi_x|^2$. Suppose that we have superposition $|\psi\rangle = \sum_{x \in \mathsf{X}, y \in \mathsf{Y}, z \in \mathsf{Z}} \psi_{x,y,z} |x, y, z\rangle$, where $\mathcal{X}$ and $\mathcal{Y}$ are finite sets and $\mathcal{Z}$ is a work space. For an oracle $\mathsf{O} : \mathcal{X} \to \mathcal{Y}$, we write quantum access to O as a mapping $|\psi\rangle \mapsto \sum_{x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}} \psi_{x,y,z} |x, y + \mathsf{O}(x), z\rangle$, where $+ : \mathcal{Y} \times \mathcal{Y} \to \mathcal{Y}$ is a group operation on $\mathcal{Y}$. "Quantum polynomial-time" is abbreviated as QPT.

2.1 Group Testing

Dorfman presented the first group testing protocol in order to effectively detect blood samples contaminated by some disease during the world war II [9]. Group testing (e.g., [10]) is a method to detect positive items among many items with a smaller number of tests than the straightforward individual testing for each item. There are many applications of group testing, such as screening blood samples for detecting a disease, and detecting clones which have a particular DNA sequence.

Canonical non-adaptive group testing is designed by a d-disjunct matrix or a d-cover-free family (e.g., see [10]). A non-adaptive group testing protocol with u tests for ℓ items is represented by a $u \times \ell$ binary matrix, and the (i,j)-th element of the matrix is equal to 1 if and only if the i-th test is executed to the j-th item. The d-disjunct property of binary matrices is defined as follows.

Definition 1 (d-disjunct)**.** *A matrix $\boldsymbol{G} = [\boldsymbol{g}_1, \ldots, \boldsymbol{g}_\ell] \in \{0,1\}^{u \times \ell}$ is d-disjunct if for any d columns $\boldsymbol{g}_{s_1}, \ldots, \boldsymbol{g}_{s_d}$ and any $\bar{\boldsymbol{g}} \in \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_\ell\} \backslash \{\boldsymbol{g}_{s_1}, \ldots, \boldsymbol{g}_{s_d}\}$ ($s_1, \ldots, s_d \in [\ell]$), there exists $z \in [u]$ such that $v_z < \bar{g}_z$, where $\boldsymbol{v} = \bigvee_{i=1}^{d} \boldsymbol{g}_{s_i}$, and $\bigvee$ is the bitwise-OR.*

By using a d-disjunct matrix, a non-adaptive group testing protocol can efficiently detect at most d positive items. We simply describe the process of group testing with a d-disjunct matrix $\boldsymbol{G} \in \{0,1\}^{u \times \ell}$ as follows: Let $S_i(\boldsymbol{G}) = \{j \mid j \in [\ell] \wedge g_{i,j} = 1\}$ for $i \in [u]$ and $\boldsymbol{G} \in \{0,1\}^{u \times \ell}$.

Step 1. Initialize a set $J \leftarrow \{1, 2, \ldots, \ell\}$ of indexes of positive items' candidates.

Step 2. For each $i \in [u]$, compress items whose indexes are in $S_i(\boldsymbol{G})$.

Step 3. For each $i \in [u]$, set $J \leftarrow J \backslash S_i(\boldsymbol{G})$ if the test result of the i-th compressed item is negative. Here, note that the test result of a compressed item shows positive if at least one positive item are included, and shows negative otherwise.

Step 4. Output J.

Then, the output J is a set of indexes of all positive items, due to the d-disjunct property of $\boldsymbol{G}$.

2.2 Aggregate Signatures (with Detecting Functionality)

We first describe the syntax of aggregate signatures and formalize its quantum-security notion.

Definition 2 (Aggregate Signatures)**.** *An aggregate signature (ASIG) scheme* ASig *consists of five polynomial-time algorithms* $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{Agg}, \mathsf{AVrfy})$*: For a security parameter λ, let $\mathcal{M} = \mathcal{M}(\lambda)$ be a message space, and let $\mathcal{S} = \mathcal{S}(\lambda)$ be a signature space.*

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$*: The randomized algorithm* KGen *takes as input a security parameter 1^λ, and it outputs a public key* pk *and a secret key* sk*.*
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$*: The randomized or deterministic algorithm* Sign *takes as input a secret key* sk *and a message $\mathsf{m} \in \mathcal{M}$, and it outputs a signature $\sigma \in \mathcal{S}$.*
- $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma)$*: The deterministic algorithm* Vrfy *takes as input a public key* pk*, a message $\mathsf{m} \in \mathcal{M}$, and a signature $\sigma \in \mathcal{S}$, and it outputs 1 (accept) or 0 (reject).*
- $\widehat{\sigma} \leftarrow \mathsf{Agg}((\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$*: The randomized or deterministic algorithm* Agg *takes as input a tuple $(\mathsf{pk}_1, \mathsf{m}_1, \sigma_1)$, …, $(\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell)$ of public keys, messages and signatures, and it outputs an aggregate signature $\widehat{\sigma} \in \mathcal{S}$.*

- $1/0 \leftarrow \mathsf{AVrfy}((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell), \widehat{\sigma})$*: The deterministic algorithm* AVrfy *takes as input a tuple* $(\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell)$ *of public keys and messages, and an aggregate signature* $\widehat{\sigma} \in \mathcal{S}$*, and it outputs* 1 *(accept) or* 0 *(reject).*

We require that an ASIG scheme satisfies correctness as follows.

Definition 3 (Correctness)**.** *An ASIG scheme* $\mathsf{ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{Agg}, \mathsf{AVrfy})$ *satisfies* correctness *if the following conditions hold:*

- *For every* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$ *and every* $\mathsf{m} \in \mathcal{M}$*, it holds that* $\mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma) = 1$ *with overwhelming probability, where* $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$*.*
- *For any* $\ell = \mathsf{poly}(\lambda)$*, every* $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KGen}(1^\lambda), \ldots, (\mathsf{pk}_\ell, \mathsf{sk}_\ell) \leftarrow \mathsf{KGen}(1^\lambda)$*, and every* $\mathsf{m}_1, \ldots, \mathsf{m}_\ell \in \mathcal{M}$*, it holds that* $\mathsf{AVrfy}((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell), \widehat{\sigma}) = 1$ *with overwhelming probability, where* $\widehat{\sigma} \leftarrow \mathsf{Agg}((\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$ *and* $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}_i, \mathsf{m}_i)$ *for every* $i \in [\ell]$*.*

Following definitions of quantum-security of digital signatures [7] and classical security of ASIGs [4], we formalize *aggregate unforgeability against quantum chosen message attacks* (denoted by aggUF-qCMA security) as a quantum-security notion of ASIGs, .

Definition 4 (aggUF-qCMA security)**.** *An ASIG scheme* $\mathsf{ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{Agg}, \mathsf{AVrfy})$ *satisfies* aggUF-qCMA *security if for any QPT adversary* A *against* ASig*, its advantage* $\mathsf{Adv}^{\text{agguf-qcma}}_{\mathsf{ASig},\mathsf{A}}(\lambda) := \Pr[\mathsf{A}\ \textit{wins}]$ *is negligible in* λ*.* $[\mathsf{A}\ \textit{wins}]$ *is the event that* A *wins in the following game:*

Setup. *A challenger generates* $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{KGen}(1^\lambda)$*, and sends* pk^* *to* A*.*

Queries. *Given a quantum signing-query (i.e., a superposition of messages)*

$$\sum_{\mathsf{m} \in \mathcal{M}, s \in \mathcal{S}, z} \psi_{\mathsf{m},s,z} |\mathsf{m}, s, z\rangle,$$

the signing oracle SIGN *chooses randomness* r *used in the* Sign *algorithm, where it does not need to choose randomness* r *if* Sign *is deterministic. Then, it returns*

$$\sum_{\mathsf{m} \in \mathcal{M}, s \in \mathcal{S}, z} \psi_{\mathsf{m},s,z} |\mathsf{m}, s \oplus \mathsf{Sign}(\mathsf{sk}^*, \mathsf{m}; r), z\rangle.$$

Let Q *be the number of queries which* A *submits to the* SIGN *oracle.*

Output. A *outputs* $(PM^{(1)}, \widehat{\sigma}^{(1)}), \ldots, (PM^{(Q+1)}, \widehat{\sigma}^{(Q+1)})$*, where for* $i \in [Q+1]$*,* $PM^{(i)} = ((\mathsf{pk}_1^{(i)}, \mathsf{m}_1^{(i)}), \ldots, (\mathsf{pk}_{\ell^{(i)}}^{(i)}, \mathsf{m}_{\ell^{(i)}}^{(i)}))$*.* A *wins if it holds that* (i) $\mathsf{AVrfy}(PM^{(i)}, \widehat{\sigma}^{(i)}) = 1$ *for every* $i \in [Q+1]$*,* (ii) *there exists* $\mathsf{m}^{*(i)} \in \mathcal{M}$ *such that* $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ *for every* $i \in [Q+1]$*, and* (iii) $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ *are distinct.*

Next, following [29], we describe the syntax of D-ASIGs.

Definition 5 (Aggregate Signatures with Detecting Functionality)**.** *An aggregate signature scheme with detecting functionality (D-ASIG) consists of five polynomial-time algorithms* $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$ *associated with a set* $\mathcal{G}$ *consisting of* d*-disjunct matrices: For a security parameter* λ*, let* $\mathcal{M} = \mathcal{M}(\lambda)$ *be a message space, and let* $\mathcal{S} = \mathcal{S}(\lambda)$ *be a signature space.*

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$*:* *The randomized algorithm* KGen *takes as input a security parameter* 1^λ*, and it outputs a public key* pk *and a secret key* sk*.*

- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$: *The randomized or deterministic algorithm* Sign *takes as input a secret key* sk *and a message* $\mathsf{m} \in \mathcal{M}$*, and it outputs a signature* $\sigma \in \mathcal{S}$*.*

- $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma)$: *The deterministic algorithm* Vrfy *takes as input a public key* pk*, a message* $\mathsf{m} \in \mathcal{M}$*, and a signature* $\sigma \in \mathcal{S}$*, and it outputs* 1 *(accept) or* 0 *(reject).*

- $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u) \leftarrow \mathsf{DAgg}(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$: *The randomized or deterministic algorithm* DAgg *takes as input a* d*-disjunct matrix* $\boldsymbol{G} \in \{0,1\}^{u \times \ell} \cap \mathcal{G}$*, a tuple* $((\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$ *of public keys, messages, and signatures, and it outputs a tuple* $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u)$ *of aggregate signatures.*

- $J \leftarrow \mathsf{DVrfy}(\boldsymbol{G}, ((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell)), (\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u))$: *The deterministic algorithm* DVrfy *takes as input a* d*-disjunct matrix* $\boldsymbol{G} \in \{0,1\}^{u \times \ell} \cap \mathcal{G}$*, a tuple* $((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell))$ *of public keys and messages, and a tuple* $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u)$ *of aggregate signatures, and it outputs a set* J *of public keys and messages.*

We require that D-ASIG scheme satisfies correctness.

Definition 6 (Correctness)**.** *A D-ASIG scheme* $\mathsf{D\text{-}ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$ *satisfies* correctness *if the following conditions hold:*

- *For every* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$ *and every* $\mathsf{m} \in \mathcal{M}$*, it holds that* $\mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma) = 1$ *with overwhelming probability, where* $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$*.*

- *For any* $\ell = \mathsf{poly}(\lambda)$*, every* d*-disjunct matrix* $\boldsymbol{G} \in \{0,1\}^{u \times \ell} \cap \mathcal{G}$*, every* $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KGen}(1^\lambda), \ldots,$ $(\mathsf{pk}_\ell, \mathsf{sk}_\ell) \leftarrow \mathsf{KGen}(1^\lambda)$*, and every* $\mathsf{m}_1, \ldots, \mathsf{m}_\ell \in \mathcal{M}$*, it holds that* $\mathsf{DVrfy}(\boldsymbol{G}, ((\mathsf{pk}_1, \mathsf{m}_1), \ldots,$ $(\mathsf{pk}_\ell, \mathsf{m}_\ell)), (\widehat{\sigma}_1, \ldots, \widehat{\sigma}_\ell)) = \emptyset$ *with overwhelming probability, where* $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_\ell) \leftarrow \mathsf{DAgg}(\boldsymbol{G},$ $(\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$ *and* $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}_i, \mathsf{m}_i)$ *for every* $i \in [\ell]$*.*

Regarding classical security notions of D-ASIGs, unforgeability and identifiability were formalized in [29]. Following the definitions of [29] and [7], we define these notions in the security model where an adversary is allowed to issue quantum queries to given oracles. First, the signing oracle SIGN which an adversary is given quantum access to is defined as follows: Given a quantum signing-query

$$\sum_{\mathsf{m} \in \mathcal{M}, s \in \mathcal{S}, z} \psi_{\mathsf{m},s,z} |\mathsf{m}, s, z\rangle,$$

the signing oracle SIGN chooses randomness r used in the Sign algorithm, where it does not need to choose randomness r if Sign is deterministic. Then, it returns

$$\sum_{\mathsf{m} \in \mathcal{M}, s \in \mathcal{S}, z} \psi_{\mathsf{m},s,z} |\mathsf{m}, s \oplus \mathsf{Sign}(\mathsf{sk}^*, \mathsf{m}; r), z\rangle.$$

Next, we define the two security notions in the quantum security model. Regarding the unforgeability of D-ASIGs in the security model, we define *detectable aggregate unforgeability against quantum chosen message attacks*, denoted by daggUF-qCMA security.

Definition 7 (daggUF-qCMA security)**.** *A D-ASIG scheme* $\mathsf{D\text{-}ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$ *satisfies* daggUF-qCMA *security if for any QPT adversary* A *against* ASig*, its advantage* $\mathsf{Adv}^{\text{dagguf-qcma}}_{\mathsf{ASig},\mathsf{A}}(\lambda) := \Pr[\mathsf{A}\ \textit{wins}]$ *is negligible in* λ*.* [A *wins*] *is the event that* A *wins in the following game:*

Setup. *A challenger generates* $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{KGen}(1^\lambda)$*, and sends* pk^* *to* A.

Queries. A *is allowed to issue quantum queries to the* SIGN *oracle. Let* Q *be the number of queries which* A *submits to the* SIGN *oracle.*

Output. A *outputs* $(\boldsymbol{G}^{(1)}, PM^{(1)}, \widehat{\Sigma}^{(1)}), \ldots, (\boldsymbol{G}^{(Q+1)}, PM^{(Q+1)}, \widehat{\Sigma}^{(Q+1)})$*, where for every* $i \in [Q+1]$, $\boldsymbol{G}^{(i)} \in \{0,1\}^{u^{(i)} \times \ell^{(i)}} \cap \mathcal{G}$, $PM^{(i)} = ((\mathsf{pk}_1^{(i)}, \mathsf{m}_1^{(i)}), \ldots, (\mathsf{pk}_{\ell^{(i)}}^{(i)}, \mathsf{m}_{\ell^{(i)}}^{(i)}))$ *and* $\widehat{\Sigma}^{(i)} = (\widehat{\sigma}_1^{(i)}, \ldots, \widehat{\sigma}_{u^{(i)}}^{(i)})$. *The challenger computes* $J^{(i)} \leftarrow \mathsf{DVrfy}(\boldsymbol{G}^{(i)}, PM^{(i)}, \widehat{\Sigma}^{(i)})$ *for every* $i \in [Q+1]$. A *wins in this game if the following conditions hold:* (i) $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \notin J^{(i)}$ *for every* $i \in [Q+1]$, (ii) $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ *for every* $i \in [Q+1]$, *and* (iii) $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ *are distinct.*

Definition 8 (Identifiability against Quantum Chosen Message Attacks)**.** *Regarding the* identifiability *of a D-ASIG scheme* $\mathsf{D\text{-}ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$*, we define completeness and soundness, which are denoted by* cmp-qCMA *security and* snd-qCMA *security, respectively. Let* A *be a* d*-dishonest QPT adversary against* D-ASig*, where a QPT adversary* A *against* D-ASig *is* d*-dishonest if it outputs* $(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$ *such that* $|\{(\mathsf{pk}_i, \mathsf{m}_i) \mid i \in [\ell] \wedge \mathsf{Vrfy}(\mathsf{pk}_i, \mathsf{m}_i, \sigma_i) = 0\}| \leq d$*, in the following security game:*

Setup. *A challenger generates* $(\mathsf{pk}^*, \mathsf{sk}^*) \leftarrow \mathsf{KGen}(1^\lambda)$ *and sends* pk^* *to* A.

Queries. A *is allowed to issue quantum queries to the* SIGN *oracle.*

Output. A *outputs* $(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$*. The challenger computes* $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u) \leftarrow \mathsf{DAgg}(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$ *and* $J \leftarrow \mathsf{DVrfy}(\boldsymbol{G}, ((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell)), (\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u))$.

The cmp-qCMA *security and* snd-qCMA *security are defined as follows: For a set* $\{(\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell)\}$*, let* $D = \{(\mathsf{pk}_i, \mathsf{m}_i) \mid i \in [\ell] \wedge \mathsf{Vrfy}(\mathsf{pk}_i, \mathsf{m}_i, \sigma_i) = 0\}$*, and* $\bar{D} = \{(\mathsf{pk}_i, \mathsf{m}_i) \mid i \in [\ell] \wedge \mathsf{Vrfy}(\mathsf{pk}_i, \mathsf{m}_i, \sigma_i) = 1\}$.

- ***Completeness****:* D-ASig *satisfies* cmp-qCMA *security against* d*-dishonest adversaries, if for any* d*-dishonest QPT adversary* A *against* D-ASig*, its advantage*

$$\mathsf{Adv}^{\text{cmp-qcma}}_{\mathsf{D\text{-}ASig},\mathsf{A}}(\lambda) := \Pr\left[\exists \mathsf{m}^* \in \{\mathsf{m}_i\}_{i\in[\ell]}, (\mathsf{pk}^*, \mathsf{m}^*) \in \bar{D} \cap J\right]$$

  is negligible in λ.

- ***Soundness****:* D-ASig *satisfies* snd-qCMA *security against* d*-dishonest adversaries, if for any* d*-dishonest QPT adversary* A *against* D-ASig*, its advantage*

$$\mathsf{Adv}^{\text{snd-qcma}}_{\mathsf{D\text{-}ASig},\mathsf{A}}(\lambda) := \Pr\left[\exists \mathsf{m}^* \in \{\mathsf{m}_i\}_{i\in[\ell]}, (\mathsf{pk}^*, \mathsf{m}^*) \in D \backslash J\right]$$

  is negligible in λ.

In addition, weak-snd-qCMA *security is defined in the same way as* snd-qCMA *security except that the advantage of a* d*-dishonest QPT adversary* A *against* D-ASig *is defined as* $\mathsf{Adv}^{\text{w-snd-qcma}}_{\mathsf{D\text{-}ASig},\mathsf{A}}(\lambda) := \Pr[\exists \textit{distinct}\, \mathsf{m}^*_{k_1}, \ldots, \mathsf{m}^*_{k_t} \in \{\mathsf{m}_i\}_{i\in[\ell]}, t \geq Q+1 \wedge (\mathsf{pk}^*, \mathsf{m}^*_{k_1}), \ldots, (\mathsf{pk}^*, \mathsf{m}^*_{k_t}) \in D \backslash J]$*, where* $k_1, \ldots, k_t \in [\ell]$ *are distinct, and* Q *is the number of queries which* A *submits to the* SIGN *oracle.*

The weak-snd-qCMA security is a weak variant of snd-qCMA security since the winning condition of weak-snd-qCMA security is a special case of that of snd-qCMA security. Furthermore, Proposition 1 shows the relation between daggUF-qCMA security and weak-snd-qCMA security.

Proposition 1. *If a D-ASIG scheme* $\mathsf{D\text{-}ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$ *fulfills* $\mathsf{daggUF\text{-}qCMA}$ *security, then* $\mathsf{D\text{-}ASig}$ *also satisfies* $\mathsf{weak\text{-}snd\text{-}qCMA}$ *security.*

Proof. Let A be a QPT adversary breaking the $\mathsf{weak\text{-}snd\text{-}qCMA}$ security of $\mathsf{D\text{-}ASig}$, and let Q be the number of signing-queries issued by A. By using A, we construct a QPT algorithm F breaking the $\mathsf{daggUF\text{-}qCMA}$ security of $\mathsf{D\text{-}ASig}$, as follows: F takes as input a public key pk^* and sends pk^* to A. When A issues a signing-query, F simulates the signing oracle by using the oracle given in the $\mathsf{daggUF\text{-}qCMA}$ game, in the straightforward way. In **Output** phase, A outputs $(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$. Then, F computes $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u) \leftarrow \mathsf{DAgg}(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$. If there exist distinct $\mathsf{m}^*_{k_1}, \ldots, \mathsf{m}^*_{k_t} \in \{\mathsf{m}_i\}_{i\in[\ell]}$ such that $t \geq Q+1$ and $(\mathsf{pk}^*, \mathsf{m}^*_{k_1}), \ldots, (\mathsf{pk}^*, \mathsf{m}^*_{k_t}) \in D \backslash J$, then F outputs $(\boldsymbol{G}^{(1)}, PM^{(1)}, \widehat{\Sigma}^{(1)}), \ldots, (\boldsymbol{G}^{(Q+1)}, PM^{(Q+1)}, \widehat{\Sigma}^{(Q+1)})$ by setting $\boldsymbol{G}^{(i)} = \boldsymbol{G}$, $PM^{(i)} = ((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell))$, and $\widehat{\Sigma}^{(i)} = (\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u)$ for $i \in [Q+1]$. Otherwise, F aborts.

We analyze the output of F. We assume that the A's output fulfills the winning condition $\exists$distinct $\mathsf{m}^*_{k_1}, \ldots, \mathsf{m}^*_{k_t} \in \{\mathsf{m}_i\}_{i\in[\ell]}$, $t \geq Q+1$ and $(\mathsf{pk}^*, \mathsf{m}^*_{k_1}), \ldots, (\mathsf{pk}^*, \mathsf{m}^*_{k_t}) \in D \backslash J$. The first winning condition of $\mathsf{daggUF\text{-}qCMA}$ security holds since for $i \in [Q+1]$, there exists $(\mathsf{pk}^*, \mathsf{m}^*_{k_i}) \notin J^{(i)} = J$. The second condition also holds since for $i \in [Q+1]$, $(\mathsf{pk}^*, \mathsf{m}^*_{k_i})$ is included in $PM^{(i)}$. The third condition holds clearly since $\mathsf{m}^*_{k_1}, \ldots, \mathsf{m}^*_{k_t}$ are distinct due to the winning condition of A. Hence, the output of F is a valid forgery in the $\mathsf{daggUF\text{-}qCMA}$ security game, and then we obtain the advantage $\mathsf{Adv}^{\text{w-snd-qcma}}_{\mathsf{D\text{-}ASig},\mathsf{A}}(\lambda) \leq \mathsf{Adv}^{\text{dagguf-qcma}}_{\mathsf{D\text{-}ASig},\mathsf{F}}(\lambda)$. □

Quantum Random Oracle Model and Certified Key Model. The quantum random oracle model is a model where a hash function is modeled as an ideal random function, and any party is allowed to issue quantum queries to this function as an oracle called a *quantum random oracle*. See [3] for details on this model. In addition, the certified key model is a model where every signer has to provide a key-pair $(\mathsf{pk}, \mathsf{sk})$ in order to certify pk, and $(\mathsf{pk}, \mathsf{sk})$ is added to the list L of registered key-pairs if sk is a valid secret key corresponding to pk. Following [21, 27], we use this model in order to construct a quantum-secure AOTS scheme.

3 Quantum-Secure D-ASIG from Quantum-Secure ASIG

We consider a D-ASIG generic construction starting from an ASIG scheme and a non-adaptive group testing protocol. This scheme is the same as a generic construction of [29] except that we assume the underlying ASIG satisfies the formalized quantum-security. Then, we prove that this D-ASIG scheme satisfies our quantum-security. The D-ASIG scheme $\mathsf{D\text{-}ASig} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{DAgg}, \mathsf{DVrfy})$ is as follows: Let $\mathsf{ASig} = (\mathsf{KGen}^{asig}, \mathsf{Sign}^{asig}, \mathsf{Vrfy}^{asig}, \mathsf{Agg}^{asig}, \mathsf{AVrfy}^{asig})$ be an ASIG scheme. For a matrix $\boldsymbol{G} \in \{0,1\}^{u\times\ell}$ and $i \in [u]$, let $S_i(\boldsymbol{G}) = \{j \mid j \in [\ell] \wedge g_{i,j} = 1\}$.

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$: Output $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}^{asig}(1^\lambda)$.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$: Output $\sigma \leftarrow \mathsf{Sign}^{asig}(\mathsf{sk}, \mathsf{m})$.
- $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma)$: Output $1/0 \leftarrow \mathsf{Vrfy}^{asig}(\mathsf{pk}, \mathsf{m}, \sigma)$.
- $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u) \leftarrow \mathsf{DAgg}(\boldsymbol{G}, (\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$: For each $i \in [u]$, generate $\widehat{\sigma}_i \leftarrow \mathsf{Agg}^{asig}((\mathsf{pk}_k, \mathsf{m}_k, \sigma_k)_{k\in S_i(\boldsymbol{G})})$. Output $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u)$.
- $J \leftarrow \mathsf{DVrfy}(\boldsymbol{G}, ((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell)), (\widehat{\sigma}_1, \ldots, \widehat{\sigma}_u))$: Set $J \leftarrow \{(\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell)\}$. For each $i \in [u]$, if $\mathsf{AVrfy}^{asig}((\mathsf{pk}_k, \mathsf{m}_k)_{k\in S_i(\boldsymbol{G})}, \widehat{\sigma}_i) = 1$ holds, then set $J \leftarrow J \backslash \{(\mathsf{pk}_k, \mathsf{m}_k)\}_{k\in S_i(\boldsymbol{G})}$. Output J.

Theorems 1 and 2 show the quantum-security of D-ASig.

Theorem 1. *If an ASIG scheme* ASig *fulfills* aggUF-qCMA *security, then the resulting D-ASIG scheme* D-ASig *satisfies* daggUF-qCMA *security.*

Proof. Let A be a QPT adversary breaking the daggUF-qCMA security of D-ASig, and let Q be the number of (quantum) signing-queries issued by A. By using A, we construct a QPT algorithm F breaking the aggUF-qCMA security of ASig, in the following way: F is given a public key pk^* and runs A by sending pk^*. When A issues a (quantum) signing-query, F responds to this query by using the given signing oracle, in the straightforward way. When A outputs $(\boldsymbol{G}^{(1)}, PM^{(1)}, \widehat{\Sigma}^{(1)}), \ldots, (\boldsymbol{G}^{(Q+1)}, PM^{(Q+1)}, \widehat{\Sigma}^{(Q+1)})$ in **Output** phase, F finds distinct $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ such that $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \notin J^{(i)}$ and $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ for $i \in [Q+1]$ by following the procedure of the challenger of the daggUF-qCMA game. Then, for every $i \in [Q+1]$, it finds an index $j_i \in [u^{(i)}]$ such that $\mathsf{AVrfy}^{asig}((\mathsf{pk}_k, \mathsf{m}_k)_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}, \widehat{\sigma}_{j_i}^{(i)}) = 1$ and $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in \{(\mathsf{pk}_k, \mathsf{m}_k)\}_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}$, and outputs the pairs $((\mathsf{pk}_k, \mathsf{m}_k)_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}, \widehat{\sigma}_{j_i}^{(i)})_{i \in [Q+1]}$. If there do not exist distinct $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ satisfying the above conditions, then F aborts.

F clearly simulates the environment of A. We analyze the output of F. The A's output satisfies the conditions (i) $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \notin J^{(i)}$ for every $i \in [Q+1]$, (ii) $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ for every $i \in [Q+1]$, and (iii) $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ are distinct. Owing to the conditions (ii) and (iii), there exist distinct pairs $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(Q+1)})$ such that $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ for $i \in [Q+1]$. Furthermore, the condition (i) ensures that for $i \in [Q+1]$, there exists an aggregate signature $\widehat{\sigma}_{j_i}^{(i)}$ (where $j_i \in [u^{(i)}]$) such that $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in \{(\mathsf{pk}_k, \mathsf{m}_k)\}_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}$ and $\mathsf{AVrfy}^{asig}((\mathsf{pk}_k, \mathsf{m}_k)_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}, \widehat{\sigma}_{j_i}^{(i)}) = 1$. Therefore, the tuple $((\mathsf{pk}_k, \mathsf{m}_k)_{k \in S_{j_i}(\boldsymbol{G}^{(i)})}, \widehat{\sigma}_{j_i}^{(i)})_{i \in [Q+1]}$ is a valid forgery in the aggUF-qCMA security game. Then, we obtain the advantage $\mathsf{Adv}^{\text{dagguf-qcma}}_{\text{D-ASig,A}}(\lambda) \leq \mathsf{Adv}^{\text{agguf-qcma}}_{\text{ASig,F}}(\lambda)$, and the proof is completed. □

Theorem 2. *The resulting D-ASIG scheme* D-ASig *satisfies the following* identifiability*: Let d be arbitrary positive integer.*

(i) If $\boldsymbol{G}$ is a d-disjunct matrix, and an ASIG scheme ASig *meets* correctness*, then* D-ASig *satisfies* cmp-qCMA *security against d-dishonest adversaries.*

(ii) If an ASIG scheme ASig *meets* aggUF-qCMA *security, then* D-ASig *satisfies* weak-snd-qCMA *security against d-dishonest adversaries.*

Proof. Let A be a QPT adversary against D-ASig. It is shown that D-ASig fulfills cmp-qCMA security, in the same way as the proof of Theorem 2 in [29], because this proof do not have to use any list of quantum queries. Thus, we have $\mathsf{Adv}^{\text{cmp-qcma}}_{\text{D-ASig,A}}(\lambda) \leq \mathsf{negl}(\lambda)$. We can show that D-ASig satisfies weak-snd-qCMA security by combining Proposition 1 and Theorem 1. Thus, we have $\mathsf{Adv}^{\text{w-snd-qcma}}_{\text{D-ASig,A}}(\lambda) \leq \mathsf{Adv}^{\text{agguf-qcma}}_{\text{ASig,F}}(\lambda)$. □

4 Quantum-Secure Aggregate One-Time Signature Scheme from Lattices

In this section, we propose a quantum-secure AOTS scheme which can be applied to the generic construction in Section 3. In order to prove the security of this AOTS, we describe the definition of the short integer solution (SIS) problem which is a computationally hard problem related to lattice problems [25].

Definition 9 ($\mathsf{SIS}_{R,k,q,\beta}$)**.** *For a security parameter λ, let $k = k(\lambda)$, $q = q(\lambda)$, and $\beta = \beta(\lambda)$ be positive integers, and let $R = R_\lambda$ be a ring with a norm function $\|\cdot\| : R \to \mathbb{N}$. The $\mathsf{SIS}_{R,k,q,\beta}$ problem is as follows: Given a vector $\boldsymbol{a} \xleftarrow{\$} R_q^k$, find a non-zero vector $\boldsymbol{x} \in R^k$ such that $\boldsymbol{a}^\top \cdot \boldsymbol{x} = \boldsymbol{0}$ and $\|\boldsymbol{x}\| \leq \beta$. In addition, the $\mathsf{SIS}_{R,k,q,\beta}$ assumption is defined as follows: For any polynomial-time algorithm A, $\Pr_{\boldsymbol{a} \xleftarrow{\$} R_q^k}\left[\boldsymbol{a}^\top \cdot \boldsymbol{x} = \boldsymbol{0} \wedge \|\boldsymbol{x}\| \leq \beta \wedge \boldsymbol{x} \neq \boldsymbol{0} \mid \mathsf{A}(\boldsymbol{a}) \to \boldsymbol{x} \in R^k\right]$ is negligible in λ.*

Then, we present an SIS-based AOTS scheme. This scheme is constructed by combining an existing SIS-based one-time signature scheme of [23] and the generic construction of quantum-secure signatures in the quantum random oracle model [7]. Given one-time signatures $\sigma_1, \ldots, \sigma_\ell$, our AOTS generates an aggregate signature by computing $\sum_{i\in[\ell]} \sigma_i$. However, there is a rogue-key attack against this AOTS. Hence, we assume the certified key model in order to prevent this attack.

Our AOTS scheme $\mathsf{AOTS} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy}, \mathsf{Agg}, \mathsf{AVrfy})$ is constructed as follows: For a security parameter λ, let $\mathcal{M} = \{0,1\}^{\mathsf{poly}(\lambda)}$ be a message space and $\mathcal{U} = \{0,1\}^{\mathsf{poly}(\lambda)}$ be a randomness space. Let $k, q, \beta_s, \beta_{\mathsf{m}}$, and β_{Vrfy} be positive integers, and let R be a ring. For $\beta \in \mathbb{N}$, let $B_\beta = \{r \in R \mid \|r\| \leq \beta\}$. As system parameters of AOTS, choose $\boldsymbol{a} \xleftarrow{\$} R_q^k$ and a cryptographic hash function $H : \mathcal{M} \times \mathcal{U} \to B_{\beta_{\mathsf{m}}}$.

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$: Choose $\boldsymbol{s}_0, \boldsymbol{s}_1 \xleftarrow{\$} B_{\beta_s}^k$ and $r \xleftarrow{\$} \mathcal{U}$, and then compute $v_0 \leftarrow \boldsymbol{a}^\top \boldsymbol{s}_0$ and $v_1 \leftarrow \boldsymbol{a}^\top \boldsymbol{s}_1$. Output $\mathsf{pk} = (v_0, v_1, r)$ and $\mathsf{sk} = (\boldsymbol{s}_0, \boldsymbol{s}_1, r)$.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathsf{m})$: Compute $h \leftarrow H(\mathsf{m}, r)$. Output $\sigma \leftarrow \boldsymbol{s}_0 \cdot h + \boldsymbol{s}_1 \in R^k$.
- $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \mathsf{m}, \sigma)$: Compute $h \leftarrow H(\mathsf{m}, r)$. Output 1 if $\boldsymbol{a}^\top \sigma = v_0 \cdot h + v_1$ and $\|\sigma\| \leq \beta_{\mathsf{Vrfy}}$, and output 0 otherwise.
- $\widehat{\sigma} \leftarrow \mathsf{Agg}((\mathsf{pk}_1, \mathsf{m}_1, \sigma_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell, \sigma_\ell))$: Output $\widehat{\sigma} \leftarrow \sum_{i\in[\ell]} \sigma_i \in R^k$.
- $1/0 \leftarrow \mathsf{AVrfy}((\mathsf{pk}_1, \mathsf{m}_1), \ldots, (\mathsf{pk}_\ell, \mathsf{m}_\ell), \widehat{\sigma})$: Let $\mathsf{pk}_i = (v_{i,0}, v_{i,1}, r_i)$ and $h_i = H(\mathsf{m}_i, r_i)$ for $i \in [\ell]$. Output 1 if $\boldsymbol{a}^\top \cdot \widehat{\sigma} = \sum_{i\in[\ell]}(v_{i,0} \cdot h_i + v_{i,1})$ and $\|\widehat{\sigma}\| \leq \ell \cdot \beta_{\mathsf{Vrfy}}$, and output 0 otherwise.

We assume $R = \mathbb{Z}^{n\times n}$ or $R = \mathbb{Z}[X]/(X^n + 1)$. AOTS satisfies $\mathsf{correctness}$ if it holds that $\beta_{\mathsf{Vrfy}} \geq n \cdot \beta_s(\beta_{\mathsf{m}} + 1)$. Furthermore, Theorem 3 shows the quantum-security of AOTS.

Theorem 3. *If the SIS assumption $\mathsf{SIS}_{R,k,q,2\beta_{\mathsf{Vrfy}}}$ holds, then the AOTS scheme AOTS satisfies $\mathsf{aggUF\text{-}qCMA}$ security in the quantum random oracle model and the certified key model.*

Proof. Let A be a QPT adversary against AOTS. Let Q_h be the number of queries which A submits to the random oracle H. In order to prove Theorem 3, we consider security games $\mathsf{Game}_0, \ldots, \mathsf{Game}_4$.

$\underline{\mathsf{Game}_0}$: This game is the ordinary $\mathsf{aggUF\text{-}qCMA}$ security game. Then, the probability that A wins in Game_0 is $\epsilon = \mathsf{Adv}^{\mathsf{agguf\text{-}qcma}}_{\mathsf{AOTS},\mathsf{A}}(\lambda)$. Assuming ϵ is non-negligible, there exists a polynomial $p = \mathsf{poly}(\lambda)$ such that $\mathsf{poly}(\lambda) > 1/\epsilon$ for sufficiently large λ.

$\underline{\mathsf{Game}_1}$: This game is the same as Game_0 except that the random oracle H is defined as $H(\mathsf{m}, r) = W(V(\mathsf{m}, r))$, where $V : \mathcal{M} \times \mathcal{U} \to [\kappa]$ and $W : [\kappa] \to B_{\beta_{\mathsf{m}}}$ are random oracles, and we define $\kappa = 2C \cdot p \cdot Q_h^3$ for some constant C. Due to Lemma 2.4 in [7] (given by [32]), A wins Game_1 with at least probability $(\epsilon - 1/(2p))$.

$\underline{\mathsf{Game}_2}$: This game is the same as Game_1 except that, at the beginning of the game, κ hash values $h_1, \ldots, h_\kappa \in B_{\beta_{\mathsf{m}}}$ are chosen uniformly at random, and H is defined as $H(\mathsf{m}, r) = h_{V(\mathsf{m},r)}$. Then, it is possible to simulate V by using a $2Q_h$-wise independent hash function, due to Lemma 2.2 in

[7] (given by [32]). The hash values $h_1, \ldots, h_\kappa$ are chosen uniformly at random and independent of queries (m, r). Thus, A cannot distinguish between Game_1 and Game_2.

Game_3: This game is the same as Game_2 except for measuring the value of $V(\mathsf{m}, r^*)$. Due to Lemma 2.1 in [7], the probability that A wins in this game is at least $(\epsilon - 1/(2p))/\kappa$.

Game_4: This game is the same as Game_3 except that, at the beginning of the game, the challenger chooses $i^* \xleftarrow{\$} [\kappa]$ and checks whether i^* is equal to the result of measuring the value of $V(\mathsf{m}, r^*)$, at the end of the game. The result of this measurement is equal to i^* with at least probability $1/\kappa$. Thus, A wins this game with at least probability $(\epsilon - 1/(2p))/\kappa^2$

By using the adversary which wins in Game_4, we construct a PPT algorithm S solving $\mathsf{SIS}_{R,k,q,2\beta_{\mathsf{Vrfy}}}$ as follows: Given an $\mathsf{SIS}_{R,k,q,2\beta_{\mathsf{Vrfy}}}$ instance $\boldsymbol{a} \in R_q^k$, S generates $\mathsf{pk}^* = (v_0^*, v_1^*, r^*)$ and $\mathsf{sk}^* = (s_0^*, s_1^*, r^*)$ following the KGen algorithm, and chooses $h_1, \ldots, h_\kappa \xleftarrow{\$} B_{\beta_\mathsf{m}}$, $i^* \xleftarrow{\$} [\kappa]$, and a $2Q_h$-wise independent hash function. Then S sets a list $\mathsf{L} \leftarrow \emptyset$ and gives pk^* to A.

When A submits a key-pair $(\mathsf{pk}, \mathsf{sk})$ to certify pk, S sets $\mathsf{L} \leftarrow \mathsf{L} \cup \{(\mathsf{pk}, \mathsf{sk})\}$ if sk is the secret key corresponding to pk. S responds to a quantum query to the SIGN oracle by using $\mathsf{sk}^* = (\boldsymbol{s}_0^*, \boldsymbol{s}_1^*, r^*)$, and responds to quantum queries to the H oracle by using the values $h_1, \ldots, h_\kappa$ and a $2Q_h$-wise independent hash function.

In **Output** phase, A outputs $(PM^{(1)}, \widehat{\sigma}^{(1)})$ and $(PM^{(2)}, \widehat{\sigma}^{(2)})$. Then S checks whether it holds that $\mathsf{AVrfy}(PM^{(i)}, \widehat{\sigma}^{(i)}) = 1$ for $i \in \{1, 2\}$, there exists $\mathsf{m}^{*(i)} \in \mathcal{M}$ such that $(\mathsf{pk}^*, \mathsf{m}^{*(i)}) \in PM^{(i)}$ for $i \in \{1, 2\}$, and $(\mathsf{pk}^*, \mathsf{m}^{*(1)}), \ldots, (\mathsf{pk}^*, \mathsf{m}^{*(2)})$ are distinct. Furthermore, it checks whether all public keys $\mathsf{pk}_1^{(i)}, \ldots, \mathsf{pk}_{\ell^{(i)}}^{(i)} \in PM^{(i)}$ (except for pk^*) are registered in L for $i \in \{1, 2\}$, and $i^* = V(\mathsf{m}^{*(i)}, r^*)$ holds for some $i \in \{1, 2\}$. If the output of A does not satisfy these conditions, S aborts. If the A's output satisfies these ones, S checks whether $\mathsf{Vrfy}(\mathsf{pk}^*, \mathsf{m}^{*(i)}, \sigma^{*(i)}) = 1$ for $i \in \{1, 2\}$, where let $\sigma^{*(i)} = \widehat{\sigma}^{(i)} - \sum_{j \in [\ell^{(i)}] \text{ s.t. } (\mathsf{pk}_j^{(i)}, \mathsf{m}_j^{(i)}) \neq (\mathsf{pk}^*, \mathsf{m}^{*(i)})} \left(\boldsymbol{s}_{j,0}^{(i)} \cdot h_j^{(i)} + \boldsymbol{s}_{j,1}^{(i)} \right)$ for $i \in \{1, 2\}$, let $\mathsf{sk}_j^{(i)} = (\boldsymbol{s}_{j,0}^{(i)}, \boldsymbol{s}_{j,1}^{(i)}, r_j^{(i)})$, and let $h_j^{(i)} = H(\mathsf{m}_j^{(i)}, r_j^{(i)})$ for $i \in \{1, 2\}$ and $j \in [\ell^{(i)}]$. Let $h^{*(i)} = H(\mathsf{m}^{*(i)}, r^*)$. If $\mathsf{Vrfy}(\mathsf{pk}^*, \mathsf{m}^{*(i)}, \sigma^{*(i)}) = 1$ holds, it is proved that $(\boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*, \sigma^{*(i)})$ is a collision of $\boldsymbol{a}$ for some $i \in \{1, 2\}$ (such that $i^* \neq V(\mathsf{m}^{*(i)}, r^*)$), by combining the proofs of Theorem 3.2 and Lemma 4.7 in [23]. Namely, $\boldsymbol{a}^\top \sigma^{*(i)} = \boldsymbol{a}^\top (\boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*)$ and $\sigma^{*(i)} \neq \boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*$ hold with at least probability $O((\epsilon - 1/(2p))/\kappa^2)$. Hence, the non-zero vector $\sigma^{*(i)} - (\boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*)$ is a solution to $\mathsf{SIS}_{R,k,q,2\beta_{\mathsf{Vrfy}}}$, such that $\|\sigma^{*(i)} - (\boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*)\| \leq 2\beta_{\mathsf{Vrfy}}$ and $\boldsymbol{a}^\top (\sigma^{*(i)} - (\boldsymbol{s}_0^* h^{*(i)} + \boldsymbol{s}_1^*)) = \boldsymbol{0}$. If the $\mathsf{SIS}_{R,k,q,2\beta_{\mathsf{Vrfy}}}$ assumption holds, we have $O((\epsilon - 1/(2p))/\kappa^2) \leq \mathsf{negl}(\lambda)$, namely, $\epsilon - 1/(2p) \leq \mathsf{negl}(\lambda)$ holds. Since $\epsilon > 1/p$, $1/(2p) < \mathsf{negl}(\lambda)$ holds, but this contradicts the fact $p = \mathsf{poly}(\lambda)$. Therefore, ϵ is negligible in λ. □

5 Conclusion Remarks

In this paper, we proposed a quantum-secure D-ASIG scheme. To this end, we did the following: First, we formalized quantum-security notions of ASIGs and D-ASIGs. Concretely, we formalized aggUF-qCMA security for ASIGs, and formalized aggUF-qCMA security, cmp-qCMA security, and (weak-)snd-qCMA security for D-ASIGs. Second, we showed a D-ASIG generic construction starting from any aggUF-qCMA secure ASIG scheme and any non-adaptive group testing protocol with d-disjunct matrices, and then we proved that this scheme satisfies our quantum-security notions daggUF-qCMA security, cmp-qCMA security, and weak-snd-qCMA security. Finally, we proposed a lattice-based AOTS scheme with aggUF-qCMA security. To obtain a quantum-secure D-AOTS scheme, it is possible to apply this AOTS to the D-ASIG generic construction. Therefore, the resulting D-AOTS scheme is the first quantum-secure D-ASIG scheme.

We should remark that it is possible to construct a D-AOTS with snd-qCMA security, by combining our AOTS with a proof of knowledge system in the security model where an adversary utilizes quantum computations by itself, but issues only classical queries. This construction is the same as the D-ASIG generic construction with the soundness of the identifiability of D-ASIGs [29].

Acknowledgments. This research was conducted under a contract of "research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[1] J. H. Ahn, M. Green, and S. Hohenberger. Synchronized aggregate signatures: new definitions, constructions and applications. In *ACM Conference on Computer and Communications Security*, pages 473–484. ACM, 2010.

[2] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. In *ACM Conference on Computer and Communications Security*, pages 276–285. ACM, 2007.

[3] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *ASIACRYPT*, volume 7073 of *LNCS*, pages 41–69. Springer, 2011.

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *EUROCRYPT*, volume 2656 of *LNCS*, pages 416–432. Springer, 2003.

[5] D. Boneh and S. Kim. One-time and interactive aggregate signatures from lattices, 2020. `https://crypto.stanford.edu/~skim13/agg_ots.pdf`.

[6] D. Boneh and M. Zhandry. Quantum-secure message authentication codes. In *EUROCRYPT*, volume 7881 of *LNCS*, pages 592–608. Springer, 2013.

[7] D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *CRYPTO (2)*, volume 8043 of *LNCS*, pages 361–379. Springer, 2013.

[8] K. Brogle, S. Goldberg, and L. Reyzin. Sequential aggregate signatures with lazy verification from trapdoor permutations - (extended abstract). In *ASIACRYPT*, volume 7658 of *LNCS*, pages 644–662. Springer, 2012.

[9] R. Dorfman. The detection of defective members of large populations. *The Annals of Mathematical Statistics*, Vol. 14, No. 4:436–440, 1943.

[10] D.-Z. Du and F. K. Hwang. *Combinatorial Group Testing and Its Applications (2nd Edition)*, volume 12 of *Series on Applied Mathematics*. World Scientific, 2000.

[11] M. Fischlin, A. Lehmann, and D. Schröder. History-free sequential aggregate signatures. In *SCN*, volume 7485 of *LNCS*, pages 113–130. Springer, 2012.

[12] C. Gentry, A. O'Neill, and L. Reyzin. A unified framework for trapdoor-permutation-based sequential aggregate signatures. In *Public Key Cryptography (2)*, volume 10770 of *LNCS*, pages 34–57. Springer, 2018.

[13] C. Gentry and Z. Ramzan. Identity-based aggregate signatures. In *Public Key Cryptography*, volume 3958 of *LNCS*, pages 257–273. Springer, 2006.

[14] G. Hartung, B. Kaidel, A. Koch, J. Koch, and A. Rupp. Fault-tolerant aggregate signatures. In *Public Key Cryptography (1)*, volume 9614 of *LNCS*, pages 331–356. Springer, 2016.

[15] S. Hohenberger, A. Sahai, and B. Waters. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. In *CRYPTO (1)*, volume 8042 of *LNCS*, pages 494–512. Springer, 2013.

[16] S. Hohenberger and B. Waters. Synchronized aggregate signatures from the RSA assumption. In *EUROCRYPT (2)*, volume 10821 of *LNCS*, pages 197–229. Springer, 2018.

[17] R. Ishii, K. Yamashita, Y. Sakai, T. Matsuda, T. Teruya, G. Hanaoka, K. Matsuura, and T. Matsumoto. Aggregate signature with traceability of devices dynamically generating invalid signatures. In *ACNS Workshops*, volume 12809 of *LNCS*, pages 378–396. Springer, 2021.

[18] H. Jiang, Z. Zhang, L. Chen, H. Wang, and Z. Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In *CRYPTO (3)*, volume 10993 of *LNCS*, pages 96–125. Springer, 2018.

[19] K. Lee, D. H. Lee, and M. Yung. Sequential aggregate signatures made shorter. In *ACNS*, volume 7954 of *LNCS*, pages 202–217. Springer, 2013.

[20] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In *EUROCRYPT*, volume 4004 of *LNCS*, pages 465–485. Springer, 2006.

[21] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles. *J. Cryptology*, 26(2):340–373, 2013.

[22] A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. Sequential aggregate signatures from trapdoor permutations. In *EUROCRYPT*, volume 3027 of *LNCS*, pages 74–90. Springer, 2004.

[23] V. Lyubashevsky and D. Micciancio. Asymptotically efficient lattice-based digital signatures. *J. Cryptol.*, 31(3):774–797, 2018.

[24] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejohn. Sonic: Zero-knowledge snarks from linear-size universal and updatable structured reference strings. In *ACM Conference on Computer and Communications Security*, pages 2111–2128. ACM, 2019.

[25] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007.

[26] G. Neven. Efficient sequential aggregate signed data. In *EUROCRYPT*, volume 4965 of *LNCS*, pages 52–69. Springer, 2008.

[27] M. Rückert and D. Schröder. Aggregate and verifiably encrypted signatures from multilinear maps without random oracles. In *ISA*, volume 5576 of *LNCS*, pages 750–759. Springer, 2009.

[28] T. Saito, K. Xagawa, and T. Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In *EUROCRYPT (3)*, volume 10822 of *LNCS*, pages 520–551. Springer, 2018.

[29] S. Sato, J. Shikata, and T. Matsumoto. Aggregate signature with detecting functionality from group testing. *IACR Cryptol. ePrint Arch.*, page 1219, 2020.

[30] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[31] E. E. Targhi and D. Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In *TCC (B2)*, volume 9986 of *LNCS*, pages 192–216, 2016.

[32] M. Zhandry. How to construct quantum random functions. In *FOCS*, pages 679–687. IEEE Computer Society, 2012.

[33] M. Zhandry. Secure identity-based encryption in the quantum random oracle model. In *CRYPTO*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012.