PAPER Special Section on Cryptography and Information Security

Decentralized Attribute-Based Encryption and Signatures*

Tatsuaki OKAMOTO[†], ***Fellow and*** **Katsuyuki TAKASHIMA**[††a)], ***Senior Member***

SUMMARY This paper presents decentralized multi-authority attribute-based encryption and signature (DMA-ABE and DMA-ABS) schemes, in which no central authority exists and no global coordination is required except for the setting of a parameter for a prime order bilinear group and a hash function, which can be available from public documents, e.g., ISO and FIPS official documents. In the proposed DMA-ABE and DMA-ABS schemes, every process can be executed in a fully decentralized manner; any party can become an authority and issue a piece for a secret key to a user without interacting with any other party, and each user obtains a piece of his/her secret key from the associated authority without interacting with any other party. While enjoying such fully decentralized processes, the proposed schemes are still secure against collusion attacks, i.e., multiple pieces issued to a user by different authorities can form a collusion resistant secret key, composed of these pieces, of the user. The proposed ABE scheme is the first DMA-ABE for non-monotone relations (and more general relations), which is adaptively secure under the decisional linear (DLIN) assumption in the random oracle model. This paper also proposes the first DMA-ABS scheme for non-monotone relations (and more general relations), which is fully secure, adaptive-predicate unforgeable and perfect private, under the DLIN assumption in the random oracle model. DMA-ABS is a generalized notion of ring signatures. The efficiency of the proposed DMA-ABE and DMA-ABS schemes is comparable to those of the existing practical ABE and ABS schemes with comparable relations and security.

key words: *attribute-based encryption, attribute-based signatures, decentralized multi-authority system, non-monotone predicates*

1. Introduction

1.1 Background

Attribute-based encryption (ABE) [2]–[6] is an advanced (fine-grained) notion of public key encryption that covers identity-based encryption (IBE) [7]–[11] as a special case.

In the notion, a secret key is associated with a parameter, Ψ, and message is encrypted to a ciphertext along with another parameter Υ. Ciphertext can be decrypted by the secret if and only if a relation $R(\Psi, \Upsilon)$ holds.

Similarly, a versatile and privacy-enhanced class of digital signatures have been studied as attribute-based signatures [12]–[21]. A signing key is parameterized by Ψ. A message along with parameter Υ can be signed by signing key associated with Ψ if and only if a relation $R(\Psi, \Upsilon)$ holds. The verification for a signed message associated with parameter Υ is executed using the master public key and parameter Υ. The *privacy* of signers in this class of signatures requires that a signature generated by a secret key with Ψ release no information regarding Ψ except that $R(\Psi, \Upsilon)$ holds.

The notions of ABE and ABS require a trusted party called an *authority*. The authority generates a pair of master public key (system parameter) and master secret key. The master secret key is used to generate user's secret key associated with the user's parameter, Ψ.

In the case of IBE and identity-based signatures (IBS), Ψ is user's identity and relation R is the equality, i.e., $R(\Psi, \Upsilon)$ holds iff $\Psi = \Upsilon$, and more generally in (ciphertext-policy: CP) ABE and ABS for a general access structure, Ψ is a tuple of attributes of a user, and $R(\cdot, \Upsilon)$ is a general access structure.

Although ABE and ABS have many attractive applications, a big problem in the notions is that the security of the whole system depends on a single party, the authority. In other words, if the authority is corrupted, or the master secret key is compromised, the system will be totally broken.

To address this problem, modified notions of ABE and ABS called *multi-authority* (MA) ABE and ABS, have been studied [22]–[26] and [17]–[19], in which multiple authorities are introduced and each authority is responsible for issuing a piece of a user's secret key associated with a category or domain of attributes, i.e., a user obtains a secret key that consists of several pieces, each of which is issued by each corresponding authority.

Chase [22] initiated the notion of the MA-ABE, and introduced an approach of using a global identifier to tie several pieces of a user's secret key issued by different authorities. Her scheme, however, still has a central authority, i.e., if the authority is corrupted, the security of the system will be totally broken. The MA-ABE scheme in [25] and MA-ABS schemes in [17]–[19] also have a central authority and the same problem as [22]. The central authority problem was resolved in [23], however the admissible relation is very limited to an AND policy of a determined set of authorities. Lin et al. [24] also removed the central authority, but the system is only secure up to collusions of m users, where m is a system parameter.

Lewko and Waters [26] presented the first decentral-

Manuscript received March 15, 2019.
Manuscript revised June 18, 2019.

[†]The author is with the NTT Research Inc., California, USA.
[††]The author is with the Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura-shi, 247-8501 Japan.

*An extended abstract of a preliminary version of this paper was presented in [1] at PKC 2013. This provides significant technical contributions over [1], e.g., the full security proofs of DMA-ABS with more general policies than those in [1] and DMA-ABE, whose scheme descriptions are only given in [1] without security proofs. Refer to Sects. 5.4, 6.5, 6.6 and 6.7, and Appendix B.

a) E-mail: Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

DOI: 10.1587/transfun.2019CIP0008

ized multi-authority (DMA) CP-ABE scheme without a central authority whose admissible class of relations are general monotone access structures (or monotone span program). Their result, however, has the following problems: First, their scheme requires a trusted setup of a parameter, composite number $N := p_1p_2p_3$ (p_1, p_2, p_3 are primes) and a generator g_1 of secret subgroup G_{p_1}. That is, there exists a trapdoor, (p_1, p_2, p_3), and the security of the system will not be guaranteed by the security proof, if the trapdoor is compromised. The second problem is the scheme supports only the small universe of attributes, i.e., the number of attributes is bounded in a polynomial of the security parameter (in practice, it should be exponentially large). The third problem is that the security proof is based on four non-standard assumptions over a bilinear group of a composite order.

As for ABS, no DMA-ABS scheme (without a central authority) has been proposed.

1.2 Our Results

This paper addresses the problems with the existing MA-ABE schemes as well as the Lewko-Waters DMA-ABE scheme [26], and presents the first DMA-ABE scheme for non-monotone predicates and the first DMA-ABS scheme.

- The proposed DMA-ABE scheme:
  - This paper proposes the first DMA-ABE scheme for general relations (non-monotone access structures combined with inner-product relations [27]), in which no central authority exists and no global coordination is required except for the setting of a parameter for a prime order bilinear group and a hash function. Note that parameters for a prime order bilinear group on supersingular and some ordinary elliptic curves and specification of hash functions such as the SHA families can be available from public documents, e.g., ISO and FIPS official documents [28], [29] and [30], or can be included in the specification of the scheme.
    The proposed DMA-ABE scheme enjoys fully decentralized processes in the same manner as [26] does; any party can become an authority and issue a piece for a secret key to a user without interacting with any other party, and each user obtains a piece of his/her secret key from the associated authority without interacting with any other party.
    Remark: The general relations (non-monotone access structures combined with inner-product relations [27]) supported by the proposed DMA-ABE scheme are: $\Psi := (\vec{x}_1, \ldots, \vec{x}_d) \in \mathbb{F}_q^{n_1+\cdots+n_d}$ for encryption, and $\Upsilon := (\hat{M}, (\vec{v}_1, \ldots, \vec{v}_d) \in \mathbb{F}_q^{n_1+\cdots+n_d})$ for a secret key (some elements $\vec{x}_i$ or $\vec{v}_j$ can be empty, where $1 \le i, j \le d$). The component-wise inner-product relations for attribute vector components, e.g., $\{\vec{x}_t \cdot \vec{v}_t = 0 \text{ or not }\}_{t\in\{1,\ldots,d\}}$, are input to span program $\hat{M}$, and $R(\Psi, \Upsilon)$ holds iff the truth-value vector of $(\mathsf{T}(\vec{x}_1 \cdot \vec{v}_1 = 0), \ldots, \mathsf{T}(\vec{x}_d \cdot \vec{v}_d = 0))$ is accepted by span program $\hat{M}$.
    If the DMA-ABE for general relations is specialized to DMA-ABE for non-monotone access structures, then $n_t := 2$, i.e., $\vec{x}_t := (1, x_t)$ and $\vec{v}_t := (v_t, -1)$, where $\vec{x}_t \cdot \vec{v}_t = 0$ iff $x_t = v_t$ (x_t and v_t are attributes).
  - The attribute universe is structured in two layers in our DMA-ABE scheme (same as [27]). The upper layer consists of a polynomial number of categories or sub-universes identified by $t = 1, 2, \ldots$, each of which is a subset of the attribute universe. For example, a category (or sub-universe), ID (with some t), is a set of identities of humans. The lower layer consists of an exponential number of elements of each category or sub-universe, e.g., a passport number (or email address) of a person (in general, expressed by a vector form, $\vec{x}_t$) is an element of category (or sub-universe) t for ID.
    The layered structure is very suitable for multi-authority schemes, since each authority can correspond to a category. For example, the government is responsible for category ID or issuing a secret key associated with the identity (e.g., passport number) of a citizen.
    In addition, this layered structure is also suitable for non-monotone predicates as described in [27] (journal version).
  - This paper proves that the proposed DMA-ABE scheme for the general relations is adaptively secure in the DMA security model under the DLIN assumption in the random oracle model. That is, while enjoying such fully decentralized processes, the proposed DMA-ABE scheme is secure against collusion attacks, i.e., multiple pieces issued to a user by different authorities can form a collusion resistant secret key, composed of these pieces, of the user.
    The result herein includes, as a special case, a DMA-ABE scheme for non-monotone access structures adaptively secure under the DLIN assumption (on prime order bilinear groups), i.e., affirmatively solves the above-mentioned problems left by Lewko and Waters in [26].
    If the relation is specialized to the conjunction combined with inner-product relation, our DMA-ABE scheme is adaptively secure and *(weakly-)attribute-hiding* with $\vec{v}_t$ ($t = 1, \ldots, d$) [27].
- The proposed DMA-ABS scheme:
  - This paper proposes the first DMA-ABS scheme for the above-mentioned general relations (which includes non-monotone access structures) with the same DMA properties and other features as our DMA-ABE.
  - This paper proves that the proposed DMA-ABS scheme is fully secure, adaptive-predicate unforgeable and perfectly private, in the DMA secu-

rity model under the DLIN assumption in the random oracle model. Here, the privacy and signing query security are proper requirements for DMA-ABS but not for DMA-ABE.

– Our DMA-ABS scheme is considered to be a natural extension of *ring signatures* [31], [32]. In ring signatures, no central authority and no trusted setup are required and every process is fully distributed. Our DMA-ABS also requires no central authority and no trusted setup and every process is fully distributed. When a user with attributes issued by several authorities signs a message associated with a predicate (satisfied by the user's attributes), many users who have attributes satisfying this predicate are possible signers of this message, but it is concealed which user among these users is the actual signer.
In other words, ring signatures are a very special case of our DMA-ABS where the underlying predicate is just a disjunction and each authority is a user in a ring. For many applications of ring signatures, our DMA-ABS is more suitable. For example, in an application to whistle-blowing, an expose document on a financial scandal to a newspaper company would be better to be endorsed by someone with certain possible positions and qualifications related to the scandal than by someone in a list of real persons.

- The efficiency of the proposed DMA-ABE/ABS schemes is comparable to those of the existing ABE/ABS schemes (e.g., [18], [19], [27]). See Table 3 in Sect. 6.8 for ABS schemes.

1.3 Key Techniques

First we focus on the key techniques of our DMA-ABE and then move to those of our DMA-ABS.

As described in [26], the central technical hurdle to construct a DMA-ABE scheme is to make it collusion resistant. We follow some established key ideas for the target, global identifier gid [22] and (random oracle) hashing of gid [26]. However, the way of employing the hashed value of gid is quite different in the proposed approach compared to the existing schemes (e.g., [26]). The major difference is that we target reducing the security of our DMA-ABE scheme to the DLIN assumption, and that our construction is on the framework of dual pairing vector spaces (DPVS) [27], [33]. For some notations hereafter, see Sect. 1.5.

One of the advantages of DPVS is that it provides us with a rich structure of hierarchical trapdoors. DPVS $\mathbb{V}$ can be constructed on a prime order bilinear group $\mathbb{G}$ as a direct product (tuple) of $\mathbb{G}$, i.e., $(G_1, \ldots, G_n) \in \mathbb{V}$ $(G_i \in \mathbb{G})$, and constitutes a vector space. A pair of dual (or orthonormal) bases of $\mathbb{V}$, $\mathbb{B}$, and $\mathbb{B}^*$, can be randomly generated using random linear transformation X such that $\mathbb{B}$ and $\mathbb{B}^*$ are transformed from the canonical basis $\mathbb{A}$ by transformation X and $(X^{-1})^T$, respectively. In a typical application of DPVS to cryptography, (a part of) $\mathbb{B}$ is used as a public key and (a part of) $\mathbb{B}^*$ is used as a secret key or trapdoor. Here, there is a rich hierarchical structure of trapdoors, the top level X, the second level $\mathbb{B}^*$, and various lower levels $\boldsymbol{t}^* \in \mathsf{span}\langle\mathbb{B}^*\rangle$.

A key trick to securely tie several pieces for a secret key issued by multiple authorities into a single secret key of a user is to share a random scalar value δ among these pieces with the form of $(\delta\vec{x}_t, \ldots)_{\mathbb{B}^*_t}$ $(t = 1, \ldots, d)$, i.e., δ is shared among $(\delta\vec{x}_1, \ldots)_{\mathbb{B}^*_1} \ldots (\delta\vec{x}_d, \ldots)_{\mathbb{B}^*_d}$, where $(\delta\vec{x}_t, \ldots)_{\mathbb{B}^*_t}$ denotes a linear combination over basis $\mathbb{B}^*_t$ by linear coefficient vector $(\delta\vec{x}_t, \ldots)$. Here we employ the (random oracle) hash value of gid, $H(\mathsf{gid})$, as $\delta G \in \mathbb{G}$. It looks, however, difficult to compute $(\delta\vec{x}_t, \ldots)_{\mathbb{B}^*_t}$ from secret key $\mathbb{B}^*_t$ for each authority t, since it is hard to compute discrete logarithm δ of the hashed value, δG. Top level trapdoor X_t now plays an essential role in overcoming the problem, i..e., computing this value without using the discrete logarithm δ. In place of directly computing $(\delta\vec{x}_t, \ldots)_{\mathbb{B}^*_t}$ from $\mathbb{B}^*_t$, we compute $(X_t^{-1})^T((x_{t,1}H(\mathsf{gid}), \ldots, x_{t,n}H(\mathsf{gid}), \ldots))$ $(= (X_t^{-1})^T((\delta\vec{x}_t, \ldots)_{\mathbb{A}}) = (\delta\vec{x}_t, \ldots)_{\mathbb{B}^*_t})$, where $\vec{x}_t := (x_{t,1}, \ldots, x_{t,n})$ and see Sect. 5.2 for the definition of $(X_t^{-1})^T(\cdot)$.

A specific *central* space, $\mathbb{V}_0$ $(t = 0)$, played an essential role in the security proof (based on the dual system encryption technique) of previous ABE scheme in [27]. No such a central space, however, is allowed in our DMA setting, where only spaces, $\mathbb{V}_t$ $(t = 1, \ldots, d)$, generated by decentralized authorities are available. A crucial part of the key techniques in our DMA-ABE scheme is to distribute the dual system encryption trick with the central space $(t = 0)$ to all the spaces with $t = 1, \ldots, d$.

More precisely, the secret-key and ciphertext are of the forms of $(\vec{x}_t, \delta\vec{x}_t, 0^{n_t}, 0^{n_t}, \ldots)_{\mathbb{B}^*_t}$ and $(s_i\vec{v}_i, s'_i\vec{v}_i, 0^{n_t}, 0^{n_t}, \ldots)_{\mathbb{B}_t}$, respectively. Here, s_i and s'_i are shares from an access structure for secret s_0 and 0, respectively. Subspaces with $\{s_i\vec{v}_i\}$ and $\{\vec{x}_t\}$ are used for decryption, and subspaces with $\{s'_i\vec{v}_i\}$ and $\{\delta\vec{x}_t\}$ are for the *distributed* dual system encryption trick without the central space. To execute the trick over the subspaces, $2n_t$-dimensional hidden subspaces are employed for *semi-functional* forms of secret-keys and ciphertexts.

As for the key techniques of the proposed DMA-ABS, there are two major requirements for DMA-ABS, *(collusion resistant) unforgeability* and *privacy* in the decentralized multi-authority model. Our target is to construct a DMA-ABS scheme that is secure (unforgeable and private) in the decentralized multi-authority model.

To realize such a DMA-ABS scheme, the top level strategy is based on Naor's paradigm [9], which is originally a conversion from identity-based encryption (IBE) to (ordinary) digital signatures, but in our case, an encryption counterpart, DMA-ABE, is converted to DMA-ABS, i.e., DMA-ABS can be constructed from DMA-ABE.

Here, a signature associated with policy Υ of DMA-ABS corresponds to an Υ-specified secret key delegated from user's DMA-ABE secret key associated with attribute Ψ, where Ψ should satisfy Υ, and the signature verification is executed by checking whether the signature (or Υ-

specified secret key) can decrypt a DMA-ABE ciphertext associated with Υ made by a verifier. Hence, to convert DMA-ABS from DMA-ABE, one more layer of trick, delegating a secret key, should be added on DMA-ABE. The proposed DMA-ABS scheme is constructed on this strategy from the proposed DMA-ABE.

The (collusion resistant) *unforgeability* of our DMA-ABS can be proven in a manner similar to the (collusion resistant) adaptive security of our DMA-ABE.

A new idea is required to achieve the *privacy* condition for DMA-ABS, since no privacy condition is required for DMA-ABE or included in Naor's paradigm. In this paper, we develop a *new re-randomization* technique to achieve the privacy of DMA-ABS, since the re-randomization technique for privacy in the previous MA-ABS scheme [19] is not effective in the DMA-ABS setting due to the fully distributed structure.

For more details on the techniques in the security proofs of DMA-ABE and DMA-ABS, see the proof outline and construction idea in Sects. 5.4 and 6.3.

1.4 Related Works

1. The proposed DMA-ABE and DMA-ABS schemes are constructed on the same framework as the (single-authority) ABE, ABS and MA-ABS schemes [19], [27], that are based on the DPVS and dual system encryption technique, however, the requirements for DMA-ABE and DMA-ABS are quite different, or much more demanding. Therefore, many key ideas and core techniques of the proposed DMA-ABE and DMA-ABS are novel and essentially different from those in [19], [27] as described in Sect. 1.3.
2. As a subsequent work of [26], Lewko [34] constructed a DMA-ABE scheme over prime order bilinear groups, however, it only allows small-universes for attributes and monotone access structures, i.e., not non-monotone ones. Moreover, another DMA-ABE scheme by Rouselakis and Waters [35] solved some issues of the Lewko-Waters DMA-ABE scheme [26], e.g., its attribute-universe is large and it is constructed over prime order groups. The scheme is, however, not adaptively secure and under a non-standard assumption, q-type assumption. It also supports only monotone access structure relations, same as those in [34].
3. The *mesh signatures* [36] are a variation of ring signatures, where the predicate is an access structure on a list of pairs comprising a message and public key (m_i, pk_i), and a valid mesh signature can be generated by a person who has enough standard signatures σ_i on m_i, each valid under pk_i, to satisfy the given access structure.
   A crucial difference between mesh signatures and DMA-ABS is the security against the collusion of users. In mesh signatures, several users can collude by pooling their signatures together and create signatures that none of them could produce individually. That is, such collusion is considered to be legitimate in mesh signatures. In contrast, the security against collusion attacks is one of the basic requirements in ABS and DMA-ABS.
4. Another related concept is *anonymous credentials (ACs)* [37]–[42]. The notion of ACs also provides a functionality for users to demonstrate anonymously possession of attributes, but the goals of ACs and (DMA-)ABS differ in several points.
   As described in [18], ACs and (DMA-)ABS aim at different goals: ACs target very strong anonymity even in the registration phase, whereas under less demanding anonymity requirements in the registration phase, (DMA-)ABS aims to achieve more expressive functionalities, more efficient constructions and new applications. In addition, (DMA-)ABS is a signature scheme and a simpler primitive compared with ACs.

1.5 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. We denote the finite field of order q by $\mathbb{F}_q$, and $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{v} = (v_1, \ldots, v_n)$, $\vec{x} \cdot \vec{v}$ denotes the inner-product $\sum_{i=1}^n x_i v_i$. The vector $\vec{0}$ is abused as the zero vector in $\mathbb{F}_q^n$ for any n. X^{T} denotes the transpose of matrix X. I_ℓ and 0_ℓ denote the $\ell \times \ell$ identity matrix and the $\ell \times \ell$ zero matrix, respectively. A bold face letter denotes an element of vector space $\mathbb{V}$, e.g., $\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$, $(x_1, \ldots, x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \boldsymbol{b}_i$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} := \sum_{i=1}^N y_i \boldsymbol{b}_i^*$. For a format of attribute vectors $\vec{n} := (d; n_1, \ldots, n_d)$ that indicates dimensions of vector spaces, $\vec{e}_{t,j}$ denotes the canonical basis vector $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n_t - j}) \in \mathbb{F}_q^{n_t}$ for $t = 1, \ldots, d$ and $j = 1, \ldots, n_t$. $GL(n, \mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

2. Dual Pairing Vector Spaces by Direct Product of Symmetric Pairing Groups

For simplicity of description, we will present the proposed schemes on the symmetric version of dual pairing vector spaces (DPVS) [33], [43] constructed using symmetric bilinear pairing groups. For the asymmetric version of DPVS, see Appendix A.2 of the full version of [27].

Definition 1: "Symmetric bilinear pairing groups" $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ are a tuple of a prime q, cyclic additive group $\mathbb{G}$ and multiplicative group $\mathbb{G}_T$ of order q, $G \neq 0 \in \mathbb{G}$, and a polynomial-time computable nondegenerate bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ i.e., $e(sG, tG) = e(G, G)^{st}$ and $e(G, G) \neq 1$.

Let $\mathcal{G}_{\mathsf{bpg}}$ be an algorithm that takes input 1^λ and outputs a description of bilinear pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ with security parameter λ.

Definition 2: "Dual pairing vector spaces (DPVS)" $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ by a direct product of symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ are a tuple of prime q, N-dimensional vector space $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$ over $\mathbb{F}_q$, cyclic group $\mathbb{G}_T$ of order q, canonical basis $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ of $\mathbb{V}$, where $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$, and pairing $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$. (Symbol e is abused as pairing for $\mathbb{G}$ and for $\mathbb{V}$.) The pairing is defined by $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(G_i, H_i) \in \mathbb{G}_T$ where $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ and $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$. This is nondegenerate bilinear i.e., $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ and if $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ for all $\boldsymbol{y} \in \mathbb{V}$, then $\boldsymbol{x} = \boldsymbol{0}$. For all i and j, $e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ where $\delta_{i,j} = 1$ if $i = j$, and 0 otherwise, and $e(G, G) \neq 1 \in \mathbb{G}_T$. DPVS generation algorithm $\mathcal{G}_{\mathsf{dpvs}}$ takes input 1^λ ($\lambda \in \mathbb{N}$) and $N \in \mathbb{N}$, and outputs a description of $\mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ with security parameter λ and N-dimensional $\mathbb{V}$. It can be constructed by using $\mathcal{G}_{\mathsf{bpg}}$.

3. Non-Monotone Access Structures with Inner-Product Relations

3.1 Span Programs and Non-Monotone Access Structures

Definition 3 (Span Programs [44]): Let $\{p_1, \ldots, p_n\}$ be a set of variables. A span program over $\mathbb{F}_q$ is a labeled matrix $\hat{M} := (M, \rho)$ where M is a $(\ell \times r)$ matrix over $\mathbb{F}_q$ and ρ is a labeling of the rows of M by literals from $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ (every row is labeled by one literal), i.e., $\rho : \{1, \ldots, \ell\} \to \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$. A span program accepts or rejects an input by the following criterion. For every input sequence $\delta \in \{0,1\}^n$ define the submatrix M_δ of M consisting of those rows whose labels are set to 1 by the input δ, i.e., either rows labeled by some p_i such that $\delta_i = 1$ or rows labeled by some $\neg p_i$ such that $\delta_i = 0$. (i.e., $\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ is defined by $\gamma(j) = 1$ if $[\rho(j) = p_i] \wedge [\delta_i = 1]$ or $[\rho(j) = \neg p_i] \wedge [\delta_i = 0]$, and $\gamma(j) = 0$ otherwise. $M_\delta := (M_j)_{\gamma(j)=1}$, where M_j is the j-th row of M.)

The span program $\hat{M}$ accepts δ if and only if $\vec{1} \in \mathsf{span}\langle M_\delta \rangle$, i.e., some linear combination of the rows of M_δ gives the all one vector $\vec{1}$. (The row vector has the value 1 in each coordinate.) A span program computes a Boolean function f if it accepts exactly those inputs δ where $f(\delta) = 1$.

A span program is called monotone if the labels of the rows are only the positive literals $\{p_1, \ldots, p_n\}$. Monotone span programs compute monotone functions. (So, a span program in general is "non"-monotone.)

We assume that no row M_i ($i = 1, \ldots, \ell$) of the matrix M is $\vec{0}$. We now introduce a non-monotone access structure with evaluating map γ by using the inner-product of attribute vectors, that is employed in the proposed DMA-ABE and DMA-ABS scheme.

Definition 4: (Inner-Products of Attribute Vectors and Access Structures) $\mathcal{U}_t$ ($t = 1, \ldots, d$ and $\mathcal{U}_t \subset \{0,1\}^*$) is a sub-universe, a set of attributes, each of which is expressed by a pair of sub-universe id and n_t-dimensional vector, i.e., $(t, \vec{v})$, where $t \in \{1, \ldots, d\}$ and $\vec{v} \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$.

We now define such an attribute to be a variable p of a span program $\hat{M} := (M, \rho)$, i.e., $p := (t, \vec{v})$. An access structure $\mathbb{S}$ is a span program $\hat{M} := (M, \rho)$ along with variables $p := (t, \vec{v}), p' := (t', \vec{v}'), \ldots$, i.e., $\mathbb{S} := (M, \rho)$ such that $\rho : \{1, \ldots, \ell\} \to \{(t, \vec{v}), (t', \vec{v}'), \ldots, \neg(t, \vec{v}), \neg(t', \vec{v}'), \ldots\}$. Let Γ be a set of attributes, i.e., $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \leq t \leq d\}$, where t runs through some subset of $\{1, \ldots, d\}$, not necessarily the whole indices.

When Γ is given to access structure $\mathbb{S}$, map $\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ for span program $\hat{M} := (M, \rho)$ is defined as follows: For $i = 1, \ldots, \ell$, set $\gamma(i) = 1$ if $[\rho(i) = (t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t = 0]$ or $[\rho(i) = \neg(t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t \neq 0]$. Set $\gamma(i) = 0$ otherwise.

Access structure $\mathbb{S} := (M, \rho)$ accepts Γ iff $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$.

Remark 1: The simplest form of the inner-product relations in the above-mentioned access structures, that is for ABS and ABE, is a special case when $n_t = 2$ for all $t \in \{1, \ldots, d\}$, and $\vec{x} := (1, x)$ and $\vec{v} := (v, -1)$. Hence, $(t, \vec{x}_t) := (t, (1, x_t))$ and $(t, \vec{v}_i) := (t, (v_i, -1))$, but we often denote them shortly by (t, x_t) and (t, v_i). Then, $\mathbb{S} := (M, \rho)$ such that $\rho : \{1, \ldots, \ell\} \to \{(t, v), (t', v'), \ldots \neg(t, v), \neg(t', v'), \ldots\}$ $(v, v', \ldots \in \mathbb{F}_q)$, and $\Gamma := \{(t, x_t) \mid x_t \in \mathbb{F}_q, 1 \leq t \leq d\}$.

When Γ is given to access structure $\mathbb{S}$, map $\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ for span program $\hat{M} := (M, \rho)$ is defined as follows: For $i = 1, \ldots, \ell$, set $\gamma(i) = 1$ if $[\rho(i) = (t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i = x_t]$ or $[\rho(i) = \neg(t, v_i)] \wedge [(t, x_t) \in \Gamma] \wedge [v_i \neq x_t]$. Set $\gamma(i) = 0$ otherwise.

Remark 2: When a user has multiple attributes in a sub-universe (category) t, we can employ dimension $n_t > 2$. For instance, a professor (say Alice) in the science faculty of a university is also a professor in the engineering faculty of this university. If the attribute authority of this university manages sub-universe $t :=$ "faculties of this university", Alice obtains a secret key for $(t, \vec{x}_t := (1, -(a+b), ab) \in \mathbb{F}_q^3)$ with $a :=$ "science" and $b :=$ "engineering" from the authority. When a user verifies a signature for an access structure with a single negative attribute $\neg(t,$ "science"$)$, the verification text is encoded as $\neg(t, \vec{v}_i := (a^2, a, 1))$ with $a :=$ "science". Since $\vec{x}_t \cdot \vec{v}_i = 0$, Alice cannot make a valid signature for an access structure with the negative attribute $\neg(t,$ "science"$)$. For such a case with $n_t > 2$, see Sect. 6.4 with our DMA-ABS scheme.

We now construct a secret-sharing scheme for a span program.

Definition 5: A secret-sharing scheme for span program $\hat{M} := (M, \rho)$ is:

1. Let M be $\ell \times r$ matrix. Let column vector $\vec{f}^{\mathrm{T}} := (f_1, \ldots, f_r)^{\mathrm{T}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$. Then, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} = \sum_{k=1}^{r} f_k$ is the secret to be shared, and $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$ is the vector of ℓ shares of the secret s_0 and the share s_i belongs to $\rho(i)$.
2. If span program $\hat{M} := (M, \rho)$ accept δ, or access structure $\mathbb{S} := (M, \rho)$ accepts Γ, i.e., $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$ with $\gamma : \{1, \ldots, \ell\} \to \{0, 1\}$, then there exist constants $\{\alpha_i \in \mathbb{F}_q \mid i \in I\}$ such that $I \subseteq \{i \in \{1, \ldots, \ell\} \mid \gamma(i) = 1\}$ and $\sum_{i \in I} \alpha_i s_i = s_0$. Furthermore, these constants $\{\alpha_i\}$ can be computed in time polynomial in the size of matrix M.

4. Decisional Linear (DLIN) Assumption

Definition 6 (DLIN: Decisional Linear Assumption [45]): The DLIN problem is to guess $\beta \in \{0, 1\}$, given $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$, where

$$\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),$$
$$\kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad Y_0 := (\delta + \sigma)G, \quad Y_1 \xleftarrow{\mathsf{U}} \mathbb{G},$$
$$\text{return } (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta),$$

for $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$. For a probabilistic machine $\mathcal{E}$, we define the advantage of $\mathcal{E}$ for the DLIN problem as: $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left| \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right] \right|$.

The DLIN assumption is: For any probabilistic polynomial-time adversary $\mathcal{E}$, the advantage $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ is negligible in λ.

5. Decentralized Multi-Authority Attribute-Based Encryption (DMA-ABE)

5.1 Definitions of DMA-ABE

Definition 7 (Decentralized Multi-Authority ABE): A decentralized multi-authority (DMA) ABE scheme consists of the following algorithms. These are randomized algorithms except for Dec.

GSetup A party runs the algorithm $\mathsf{GSetup}(1^\lambda)$ which outputs a global parameter gparam. The party publishes gparam.

ASetup An attribute authority t ($1 \le t \le d$) who wishes to issue attributes runs $\mathsf{ASetup}(\mathsf{gparam}, t, n_t)$ which outputs an attribute-authority public key apk_t and an attribute-authority secret key ask_t. The attribute authority t publishes apk_t and stores ask_t.

AttrGen When an attribute authority t issues user gid a secret key associated with an attribute vector $\vec{x}_t$, it runs $\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$ that outputs an attribute secret key $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$. The attribute authority gives $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ to the user.

Enc To encrypt a message $m \in \mathbb{G}_T$ with an access structure $\mathbb{S}$, using a set of public keys for relevant authorities $\{\mathsf{apk}_t\}$, a user runs $\mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S})$ which outputs a ciphertext $\mathsf{ct}_{\mathbb{S}}$.

Dec To decrypt a ciphertext $\mathsf{ct}_{\mathbb{S}}$, using a set of public keys for relevant authorities $\{\mathsf{apk}_t\}$ and secret keys corresponding to user gid and attributes $\{(t, \vec{x}_t)\}$, gid runs $\mathsf{Dec}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, \mathsf{ct}_{\mathbb{S}})$ which outputs a message m or a special symbol $\perp$.

A DMA-ABE scheme should have the following correctness property: for all security parameter λ, all attribute sets $\Gamma := \{(t, \vec{x}_t)\}$, all gid, all messages m and all access structures $\mathbb{S}$, it holds that $m = \mathsf{Dec}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}, \mathsf{ct}_{\mathbb{S}})$ with overwhelming probability, if $\mathbb{S}$ accepts Γ, where $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$, $(\mathsf{apk}_t, \mathsf{ask}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t, n_t)$, $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$ and $\mathsf{ct}_{\mathbb{S}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S})$,

We let S the set of authorities. We assume each attribute is assigned to one authority as in [26], or an attribute is considered to be of the form of $(t, \vec{x}_t)$.

Definition 8 (Adaptive Payload Hiding of DMA-ABE): For an adversary, we define $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABE,PH}}(\lambda)$ to be the success probability in the following experiment for any security parameter λ. An DMA-ABE scheme is adaptively payload-hiding if the success probability of any polynomial-time adversary is negligible:

Setup Given 1^λ, the challenger gives $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$ to adversary $\mathcal{A}$.
$\mathcal{A}$ specifies a set $\mathcal{T}_{\mathsf{bad}} \subset \mathcal{T}$ of corrupt attribute authorities (and good (non-corrupt) authorities $\mathcal{T}_{\mathsf{good}} := \mathcal{T} \setminus \mathcal{T}_{\mathsf{bad}}$). For good authorities $t \in \mathcal{T}_{\mathsf{good}}$, the challenger runs $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t, n_t)$ and gives $\{\mathsf{apk}_t\}_{t\in\mathcal{T}_{\mathsf{good}}}$ to $\mathcal{A}$.

Phase 1 The adversary is allowed to issue a polynomial number of queries, $(\mathsf{gid}, t, \vec{x}_t)$, to the challenger or oracle $\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \cdot, \cdot)$ for attribute secret key $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$.

Challenge Let $\Gamma_{\mathsf{gid}_i} := \{(t, \vec{x})\}$ queried to the AttrGen oracle with the i-th global identifier, gid_i, and $\Gamma_0 := \{(t, *)\}_{t\in\mathcal{T}_{\mathsf{bad}}}$, where $*$ denotes a wild card (an arbitrary value).
The adversary submits two messages $m^{(0)}, m^{(1)}$ and an access structure, $\mathbb{S} := (M, \rho)$, provided that the $\mathbb{S}$ does not accept any $\Gamma_{\mathsf{gid}_i} \cup \Gamma_0$ with any gid_i.
The attacker must also give public keys $\{\mathsf{apk}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$ of corrupt attribute authorities $t \in \mathcal{T}_{\mathsf{bad}}$.
The challenger flips a random coin $b \xleftarrow{\mathsf{U}} \{0, 1\}$, and computes $\mathsf{ct}_{\mathbb{S}}^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m^{(b)}, \mathbb{S})$. It gives $\mathsf{ct}_{\mathbb{S}}^{(b)}$ to the adversary.

Phase 2 The adversary is allowed to issue a polynomial number of queries, $(\mathsf{gid}, t, \vec{x}_t)$, to the challenger or ora-

cle $\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \cdot, \cdot)$ for attribute secret key $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$, provided that $\mathbb{S}$ does not accept $\Gamma_{\mathsf{gid}_i} \cup \Gamma_0$ with any gid_i $(i = 1, \ldots, \nu_H)$.

Guess The adversary outputs a guess b' of b.

The advantage of an adversary $\mathcal{A}$ in the above game is defined as $\mathsf{Adv}^{\mathsf{DMA\text{-}ABE,PH}}_{\mathcal{A}}(\lambda) := \Pr[b' = b] - 1/2$ for any security parameter λ. A DMA-ABE scheme is adaptively payload-hiding secure if all polynomial time adversaries have at most a negligible advantage in the above game.

5.2 Construction

We define function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t, \vec{v})$ or $\rho(i) = \neg(t, \vec{v})$, where ρ is given in access structure $\mathbb{S} := (M, \rho)$. In the proposed scheme, we assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$ with ciphertext $\boldsymbol{c} = \boldsymbol{c}_{\mathbb{S}}$. We showed how to relax the restriction in the full version of [27]. In the description of the scheme, we assume that input vector $\vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$ is normalized such that $x_{t,1} := 1$. (If $\vec{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \vec{x}_t$ assuming that $x_{t,1}$ is non-zero). In addition, we assume that input vector $\vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t})$ satisfies that $v_{i,n_t} \neq 0$. For matrix $X := (\chi_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, $\boldsymbol{g}X$ denotes $(\sum_{i=1}^N G_i\chi_{i,1}, \ldots, \sum_{i=1}^N G_i\chi_{i,N}) = (\sum_{i=1}^N \chi_{i,1}G_i, \ldots, \sum_{i=1}^N \chi_{i,N}G_i)$ by a natural multiplication of a N-dim. row vector and a $N \times N$ matrix. Thus, it holds that $e(\boldsymbol{g}X, \boldsymbol{h}(X^{-1})^{\mathrm{T}}) = e(\boldsymbol{g}, \boldsymbol{h})$ for any $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{V}$.

$\mathsf{GSetup}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,
$H : \{0,1\}^* \to \mathbb{G}$; return $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H)$.

Remark : Given gparam, the following values can be computed by anyone and shared by all parties:
$G_0 := H(0^\lambda) \in \mathbb{G}$, $G_1 := H(0^{\lambda-1}, 1) \in \mathbb{G}$,
$g_T := e(G_0, G_1)$,

$\mathsf{ASetup}(\mathsf{gparam}, t, n_t)$: $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e)$
$:= \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5n_t + 1, \mathsf{param}_{\mathbb{G}})$, $X_t \xleftarrow{\mathsf{U}} GL(5n_t + 1, \mathbb{F}_q)$,
$\boldsymbol{b}_{t,i} := (0^{i-1}, G_0, 0^{5n_t+1-i})X_t$ for $i = 1, \ldots, 5n_t + 1$,
$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t}, \boldsymbol{b}_{t,5n_t+1})$,
$\mathsf{ask}_t := X_t$, $\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t)$, return $(\mathsf{ask}_t, \mathsf{apk}_t)$.

$\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid},$
$\vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ s. t. $x_{t,1} := 1)$:
$G_{\mathsf{gid}} := H(\mathsf{gid}) \in \mathbb{G}$, $\vec{\varphi}_t := (\varphi_{t,1}, \ldots, \varphi_{t,n_t}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$,

$$\boldsymbol{k}^*_t := (\overbrace{x_{t,1}G_1, .., x_{t,n_t}G_1}^{n_t}, \overbrace{x_{t,1}G_{\mathsf{gid}}, .., x_{t,n_t}G_{\mathsf{gid}}}^{n_t}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\varphi_{t,1}G_1, .., \varphi_{t,n_t}G_1}^{n_t}, \overbrace{0}^{1})(X_t^{-1})^{\mathrm{T}},$$

return $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}^*_t)$.

Remark : Let $\boldsymbol{b}^*_{t,i} := (0^{i-1}, G_1, 0^{5n_t+1-i})(X_t^{-1})^{\mathrm{T}}$,
$\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,5n_t+1})$ and $\delta \in \mathbb{F}_q$ s.t. $G_{\mathsf{gid}} = \delta G_1$.
Then $\boldsymbol{k}^*_t$ is represented as

$$\boldsymbol{k}^*_t = (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta\vec{x}_t}^{n_t}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\varphi}_t}^{n_t}, 0)_{\mathbb{B}^*_t}.$$

$\mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S} := (M, \rho))$:
$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,
$\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ s.t. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0$, $\vec{s}'^{\mathrm{T}} := (s'_1, \ldots, s'_\ell)^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$,
for $i = 1, \ldots, \ell$, $\eta_i, \theta_i, \theta'_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,
if $\rho(i) = (t, \vec{v}_i := (v_{i,1}, .., v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ s. t. $v_{i,n_t} \neq 0)$,

$$\boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i}^{n_t}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t, \vec{v}_i)$,

$$\boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{v}_i}^{n_t}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

$c_{d+1} := g_T^{s_0} m$, $\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$, return $\mathsf{ct}_{\mathbb{S}}$.

$\mathsf{Dec}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}^*_t)\},$
$\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1}))$:
If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$,
then compute I and $\{\alpha_i\}_{i \in I}$ such that $\vec{1} = \sum_{i \in I} \alpha_i M_i$,
where M_i is the i-th row of M, and
$I \subseteq \{i \in \{1, .., \ell\} \mid [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$
$\vee \ [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$,

$$K := \prod_{i \in I \wedge \rho(i) = (t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i} \prod_{i \in I \wedge \rho(i) = \neg(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)},$$

return $m' := c_{d+1}/K$.

[Correctness]
If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$,

$$\prod_{i \in I \wedge \rho(i) = (t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i} \cdot \prod_{i \in I \wedge \rho(i) = \neg(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)}$$
$$= \prod_{i \in I \wedge \rho(i) = (t,\vec{v}_i)} g_T^{\alpha_i(s_i + \delta s'_i)} \prod_{i \in I \wedge \rho(i) = \neg(t,\vec{v}_i)} g_T^{\frac{\alpha_i(s_i + \delta s'_i)(\vec{v}_i \cdot \vec{x}_t)}{\vec{v}_i \cdot \vec{x}_t}}$$
$$= g_T^{\sum_{i \in I}(\alpha_i s_i + \delta\alpha_i s'_i)} = g_T^{s_0} \text{ since } \textstyle\sum_{i \in I} \alpha_i s_i = s_0 \text{ and}$$
$\sum_{i \in I} \alpha_i s'_i = 0$.

5.2.1 Comparison with the CP-ABE Scheme in [27]

Okamoto-Takashima [27] gave an adaptively secure CP-ABE scheme on DPVS framework. Ciphertexts (CT) and secret-keys (SK) of the scheme have two components, one for decryption and one for shared secret recovering. Concretely, the first corresponds to $t = 0, d + 1$ component, i.e., $(\boldsymbol{c}_0, c_{d+1})$ and $\boldsymbol{k}^*_0$, and the second corresponds to others, i.e., $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$ and $\{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t) \in \Gamma}$. CT and SK vector components for $t \neq 0$ have dimension $3n_t = n_t + n_t + n_t + 1$, where the first n_t dimension is the real-encoding part (real part, for short) for CT and SK vectors, the second is the hidden part

for semi-functional CT and SK, the third is the SK randomness part, and the fourth is the CT randomness part.

Our DMA-ABE scheme cannot use $\boldsymbol{k}_0^*$ (and then $\boldsymbol{c}_0$) component from the distributed and decentralized key generation. To meet the correctness and (adaptive) security requirements even without $t = 0$ components, both real part and hidden parts are increased to $2n_t$-dimensional, respectively, i.e., with $5n_t = 2n_t + 2n_t + n_t + 1$ inner-structure (see the figure below).

In [27] CP-ABE, a scalar ζ in $\boldsymbol{c}_0$, which is independent of the shared secret s_i in $\boldsymbol{c}_i$ ($i = 1, \ldots, \ell$), is used for ElGamal-like decryption, however in our decentralized situation, we should use s_0 directly for decryption, so in addition to the corresponding shared secret $\{s_i\}$, we add more n_t dimension in the real part to embed another shared secret $\{s_i'\}$ with the share $s_0' = 0$.

Moreover, the dual system security proof in [27] is accomplished using the hidden part in $\boldsymbol{c}_0$ and $\boldsymbol{k}_0^*$. Instead of it, we require more n_t dimension in the hidden part in each vector component $\boldsymbol{c}_t$ and $\boldsymbol{k}_t^*$ with $t \neq 0$ to change each queried key (in the security game) to semi-functional form sequentially i.e., without affecting to the other queried keys.

CT & SK vector ($t \neq 0$) in [27] CP-ABE : ($\overbrace{\text{real}}^{n_t}$ $\overbrace{\text{hidden}}^{n_t}$ $\overbrace{\text{SK ran.}}^{n_t}$ $\overbrace{\text{CT ran.}}^{1}$),

CT & SK vector ($t \neq 0$) in our DMA-ABE : ($\overbrace{\text{real}}^{2n_t}$ $\overbrace{\text{hidden}}^{2n_t}$ $\overbrace{\text{SK ran.}}^{n_t}$ $\overbrace{\text{CT ran.}}^{1}$).

5.3 Security of the Proposed DMA-ABE

Theorem 1: The proposed DMA-ABE scheme is adaptively payload-hiding against chosen plaintext attacks under the DLIN assumption in the random oracle model.

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1, \mathcal{E}_2$ and $\mathcal{E}_3$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABE,PH}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu_H} \left(\mathsf{Adv}_{\mathcal{E}_{2,h}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{3,h}}^{\mathsf{DLIN}}(\lambda)\right) + \epsilon,$$

where $\mathcal{E}_{2,h}(\cdot) := \mathcal{E}_2(h, \cdot)$, $\mathcal{E}_{3,h}(\cdot) := \mathcal{E}_3(h, \cdot)$, ν_H is the maximum number of queries to random oracle H and $\epsilon := ((2d + 10)\nu_H + 2d + 5)/q$.

5.4 Proof Outline of Theorem 1

At the top level strategy of the security proof, an extended form of the dual system encryption by Waters [46] is employed, where ciphertexts and secret keys have three forms, *normal*, *pre-semi-functional* and *semi-functional*. The real system uses only normal ciphertexts and normal secret keys, and pre-semi-functional and semi-functional forms of ciphertexts and keys are used only in a sequence of security games for the security proof. (Additionally, ciphertexts have temporal and non-functional forms. See below.)

We employ Game 0 through Game 3. In Game 1, the challenge ciphertext is changed to temporal 0 form. When at most ν_H random oracle queries are issued by an adversary, there are $4\nu_H$ game changes from Game 1 (Game 2-0-4), Game 2-1-1, Game 2-1-2, Game 2-1-3, Game 2-1-4 through Game 2-ν_H-1, Game 2-ν_H-2, Game 2-ν_H-3, Game 2-ν_H-4.

In Game 2-h-1, the challenge ciphertext is changed to pre-semi-functional form, and keys for the first $h-1$ random oracle queried global identities, gid, are semi-functional form, while the remaining keys are normal. In Game 2-h-2, key for the h-th global identity is changed to pre-semi-functional form while the remaining keys and the challenge ciphertext is the same as in Game 2-h-1. In Game 2-h-3, the challenge ciphertext is changed to semi-functional form while all the queried keys are the same as in Game 2-h-2. In Game 2-h-4, key for the h-th global identity is changed to semi-functional form while the remaining keys and the challenge ciphertext is the same as in Game 2-h-3. At the end of the Game 2 sequence, in Game 2-ν_H-4, all the queried keys are semi-functional forms (and the challenge ciphertext is semi-functional form), which allows the next conceptual change to Game 3. In Game 3, the challenge ciphertext is changed to *non-functional* form (while all the queried keys are semi-functional form). In the final game, advantage of the adversary is zero.

We summarize these changes in Table 1, where shaded parts indicate the challenge ciphertext or queried key(s) which were changed in a game from the previous game.

As usual, we prove that the advantage gaps between neighboring games are negligible.

For $\mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$, we focus on $\vec{\boldsymbol{c}} := (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$, and ignore the other part of $\mathsf{ct}_{\mathbb{S}}$, i.e., $(\mathbb{S}, c_{d+1})$, (and call $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$ ciphertext) in this proof outline. In addition, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \leq B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

A normal secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}$ (with attributes $(t, \vec{x}_t)$), is the correct form of the secret key of the proposed DMA-ABE scheme, and is expressed by Eq. (1). Similarly, a normal ciphertext (with access structure $\mathbb{S}$), $\vec{\boldsymbol{c}}^{\mathsf{norm}}$, is expressed by Eq. (2). A temporal ciphertext is expressed by Eq. (3). A pre-semi-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{pre\text{-}semi}}$, is expressed by Eq. (4) and a pre-semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{pre\text{-}semi}}$, is expressed by Eq. (5). A semi-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{semi}}$, is expressed by Eq. (6) and a semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{semi}}$, is expressed by Eq. (7). An non-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{non\text{-}f}}$, is expressed by Eq. (8).

Below, Problems 1, 2, and 3 and their advantages are used, which are similarly defined as those for DMA-ABS which are given in Definitions 12, 13 and 16, respectively. The differences of the problems for DMA-ABE and DMA-ABS are just additional two dimensions for verifying hash values in DMA-ABS.

To prove that the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0, 1\}$), we construct a simulator of the challenger of

Table 1 Outline of game descriptions for Theorem 1.

	challenge ciphertext	queried keys				
		1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν_H
Game 0	normal	normal				
1	temporal	normal				
2-1-1	pre-semi.	normal				
2-1-2	pre-semi.	pre-semi.	normal			
2-1-3	semi-func.	pre-semi.	normal			
2-1-4	semi-func.	semi-func.	normal			
$\vdots$						
2-h-1	pre-semi.	semi-func.		normal		
2-h-2	pre-semi.	semi-func.		pre-semi.	normal	
2-h-3	semi-func.	semi-func.		pre-semi.	normal	
2-h-4	semi-func.	semi-func.		semi-func.	normal	
$\vdots$						
2-ν_H-4	semi-func.	semi-func.				semi-func.
3	non-func.	semi-func.				

Game 0 (or 1) (against an adversary $\mathcal{A}$) by using an instance with $\beta \xleftarrow{\cup} \{0,1\}$ of Problem 1. We then show that the distribution of the secret keys and challenge ciphertext replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma 1). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 8).

We then show that Game 2-($h-1$)-4 can be conceptually changed to Game 2-h-1 (Lemma 2), by using the fact that parts of bases, $(\boldsymbol{b}_{t,2n_t+1},\ldots,\boldsymbol{b}_{t,4n_t})$ and $(\boldsymbol{b}^*_{t,2n_t+1},\ldots,\boldsymbol{b}^*_{t,4n_t})$, are unknown to the adversary. In particular, when $h = 1$, it means that Game 1 can be conceptually changed to Game 2-1-1. When $h \geq 2$, we notice that normal key and semi-functional challenge ciphertext, $(\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}, \vec{\boldsymbol{c}}^{\,\mathsf{semi}})$, are equivalent to normal key and pre-semi-functional challenge ciphertext, $(\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}, \vec{\boldsymbol{c}}^{\,\mathsf{pre\text{-}semi}})$, except that (0-)shared secret $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 = 0$ is used in $\vec{\boldsymbol{c}}^{\,\mathsf{pre\text{-}semi}}$ instead of ordinary shared secret $\{r''_i\}_{i=1,\ldots,\ell}$ with $r''_0 \xleftarrow{\cup} \mathbb{F}_q$ for some coefficient vector in $\vec{\boldsymbol{c}}^{\,\mathsf{semi}}$. This change of coefficient vectors can be done conceptually since zero vector 0^n is used for the corresponding part in $\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}$.

The advantage gap between Games 2-h-1 and 2-h-2 is shown to be bounded by the advantage of Problem 2 (precisely, a slightly modified Problem 2 with the total dimensions $5n_t + 1$, not $5n_t + 3$ for each t), i.e., advantage of the DLIN assumption (Lemmas 3 and 9).

We then show that Game 2-h-2 can be conceptually changed to Game 2-h-3 (Lemma 4), where we use the fact that all queried keys $\{(t,\vec{x}_t)\}$ do not satisfy the challenge $\mathbb{S}$. Here, we notice that pre-semi-functional key and pre-semi-functional challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{pre\text{-}semi}}, \boldsymbol{c}^{\,\mathsf{pre\text{-}semi}})$, are equivalent to pre-semi-functional key and semi-functional challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{pre\text{-}semi}}, \boldsymbol{c}^{\,\mathsf{semi}})$, except that shared secret $\{r''_i\}_{i=1,\ldots,\ell}$ with $r''_0 \xleftarrow{\cup} \mathbb{F}_q$ is used in $\boldsymbol{c}^{\,\mathsf{semi}}$ instead of $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 = 0$ for some coefficient vector in $\boldsymbol{c}^{\,\mathsf{pre\text{-}semi}}$. Therefore, this conceptual change is proved using Lemma 13.

The advantage gap between Games 2-h-3 and 2-h-4 is similarly shown to be bounded by the advantage of Problem 3, i.e., advantage of the DLIN assumption (Lemmas 5 and 12).

We then show that Game 2-ν_H-4 can be conceptually changed to Game 3 (Lemma 6) by using the fact that parts of bases, $(\boldsymbol{b}_{3n+1},\ldots,\boldsymbol{b}_{4n})$ and $(\boldsymbol{b}^*_1,\ldots,\boldsymbol{b}^*_n)$, are unknown to the adversary.

Game 0 : Original security game. That is, the reply to an $\mathsf{AttrGen}$ query $\boldsymbol{k}^{(h)*}_t \in \mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$ to an $\mathsf{AttrGen}$ query for $(\mathsf{gid}_h,(t,\vec{x}_t))$ with $t \in \mathcal{T}_{\mathsf{good}}$, and the challenge ciphertext for $(m^{(0)},m^{(1)},\mathbb{S} := (M,\rho))$ are:

$$\boldsymbol{k}^{(h)*}_t := (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta^{(h)}\vec{x}_t}^{n_t}, \overbrace{\boxed{0^{2n_t}}}^{2n_t}, \overbrace{\vec{\varphi}^{(h)}_t}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t}, \tag{1}$$

$$\left.\begin{array}{l} \text{for } i = 1,\ldots,\ell, \\ \text{if } \rho(i) = (t,\vec{v}_i), \\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{s_i}\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i}^{n_t}, \\ \qquad\qquad \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\ \text{if } \rho(i) = \neg(t,\vec{v}_i), \\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{s_i}\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{v}_i}^{n_t}, \overbrace{\boxed{0^{2n_t}}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\ c_{d+1} := g_T^{\boxed{s_0}} m^{(b)}, \end{array}\right\} \tag{2}$$

where $\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, \vec{f}' \xleftarrow{R} \{\vec{f}' \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, s_i := M_i \cdot \vec{f}^{\mathrm{T}}, s_i' := M_i \cdot \vec{f}'^{\mathrm{T}}, \theta_i, \theta_i', \eta_i, \delta^{(h)} \xleftarrow{\cup} \mathbb{F}_q$ and $\vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.

Game 1 : Same as Game 0 except that the challenge ciphertext, $\boldsymbol{c}_i, c_{d+1}$, are:

$$\left.\begin{array}{l}\text{for } i = 1, \ldots, \ell,\\ \text{if } \rho(i) = (t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\\ \qquad\qquad \overbrace{\boxed{z_i\vec{e}_{t,1}}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{v}_i}^{n_t}, \overbrace{\boxed{z_i\vec{e}_{t,1}}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ c_{d+1} := g_T^{s_0} m^{(b)},\end{array}\right\} \quad (3)$$

where $z_i \xleftarrow{\cup} \mathbb{F}_q$, and the other variables are generated as in Game 0.

Game 2-h-1 ($h = 1, \ldots, \nu_H$) : Game 2-0-4 is Game 1. Game 2-h-1 is the same as Game 2-$(h-1)$-4 except that the challenge ciphertext, $\boldsymbol{c}_i, c_{d+1}$, are:

$$\left.\begin{array}{l}\text{for } i = 1, \ldots, \ell,\\ \text{if } \rho(i) = (t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\\ \qquad \overbrace{\boxed{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t,\ r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{v}_i}^{n_t}, \overbrace{\boxed{r_i\vec{v}_i \cdot Z_t,\ r_i'\vec{v}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ c_{d+1} := g_T^{s_0} m^{(b)},\end{array}\right\} \quad (4)$$

where $\vec{g} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0, M_i \cdot \vec{g}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}, \vec{g}' \xleftarrow{\cup} \{\vec{g}' \in \mathbb{F}_q^r \mid M_i \cdot \vec{g}'^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}, r_i := M_i \cdot \vec{g}^{\mathrm{T}}, r_i' := M_i \cdot \vec{g}'^{\mathrm{T}}, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q), \ \omega_i, \omega_i' \xleftarrow{\cup} \mathbb{F}_q$, and the other variables are generated as in Game 2-$(h-1)$-4.

Game 2-h-2 ($h = 1, \ldots, \nu_H$): Game 2-h-2 is the same as Game 2-h-1 except that the reply $\boldsymbol{k}_t^{(h)*} \in \mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$ to an $\mathsf{AttrGen}$ query for the h-th global identity gid_h and $t \in \mathcal{T}_{\mathsf{good}}$ is:

$$\boldsymbol{k}_t^{(h)*} := (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta^{(h)}\vec{x}_t}^{n_t}, \overbrace{\boxed{\tau^{(h)}\vec{x}_t \cdot U_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*} \quad (5)$$

where $\tau^{(h)} \xleftarrow{\cup} \mathbb{F}_q$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$ used in Eq. (4), and the other variables are generated as in Game 2-h-1.

Game 2-h-3 ($h = 1, \ldots, \nu_H$) : Game 2-h-3 is the same as Game 2-h-2 except that the challenge ciphertext, $\boldsymbol{c}_i, c_{d+1}$, are:

$$\left.\begin{array}{l}\text{for } i = 1, \ldots, \ell,\\ \text{if } \rho(i) = (t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\\ \qquad \overbrace{\boxed{r_i''}\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t,\ r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{v}_i}^{n_t}, \overbrace{\boxed{r_i''}\vec{v}_i \cdot Z_t,\ r_i'\vec{v}_i}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ c_{d+1} := g_T^{s_0} m^{(b)},\end{array}\right\} \quad (6)$$

where $\vec{g} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid M_i \cdot \vec{g}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}, r_i'' := M_i \cdot \vec{g}^{\mathrm{T}}$, and the other variables are generated as in Game 2-h-2.

Game 2-h-4 ($h = 1, \ldots, \nu_H$) : Game 2-h-4 is the same as Game 2-h-3 except that the reply $\boldsymbol{k}_t^{(h)*} \in \mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$ to an $\mathsf{AttrGen}$ query for the h-th global identity gid_h and $t \in \mathcal{T}_{\mathsf{good}}$ is:

$$\boldsymbol{k}_t^{(h)*} = (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta^{(h)}\vec{x}_t}^{n_t}, \overbrace{\boxed{0^{n_t}, \ \tau'^{(h)}\vec{x}_t}}^{2n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*} \quad (7)$$

where $\tau'^{(h)} \xleftarrow{\cup} \mathbb{F}_q$, and the other variables are generated as in Game 2-h-3.

Game 3 : Game 3 is the same as Game 2-ν_H-4 except that the challenge ciphertext, $\boldsymbol{c}_i, c_{d+1}$ are:

$$\left.\begin{array}{l}\text{for } i = 1, \ldots, \ell,\\ \text{if } \rho(i) = (t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{\tilde{s}_i}\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\\ \qquad \overbrace{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t,\ r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = (t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{bad}},\\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{\tilde{s}_i}\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t}, \overbrace{0^{3n_t}}^{3n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{good}},\\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{\tilde{s}_i}\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{v}_i}^{n_t}, \overbrace{r_i\vec{v}_i \cdot Z_t,\ r_i'\vec{v}_i}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge \ t \in \mathcal{T}_{\mathsf{bad}},\\ \quad \boldsymbol{c}_i := (\overbrace{\boxed{\tilde{s}_i}\vec{v}_i}^{n_t}, \overbrace{s_i'\vec{v}_i}^{n_t}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ c_{d+1} := g_T^{\boxed{s_0}} m^{(b)},\end{array}\right\} \quad (8)$$

where $\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, \widetilde{s_i} := M_i \cdot \vec{f}^{\mathrm{T}}$ and $s_0 \xleftarrow{\cup} \mathbb{F}_q$. The other variables are generated as in Game 2-ν_H-4. Here, we note that

s_0 is independent from all the other variables.

Let $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ be $\mathsf{Adv}^{\mathsf{DMA\text{-}ABE,PH}}_{\mathcal{A}}(\lambda)$ in Game 0, and $\mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda), \ldots, \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)$, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game 1, 2-h-1, …, 2-h-4, 3, respectively.

It is obtained that $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$ by Lemma 7. We will show five lemmas (Lemmas 1–6) that evaluate the gaps between pairs of $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda), \ldots, \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)$ for $h = 1, \ldots, \nu_H$, and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$. From these lemmas and Lemmas 8, 9 and 12, we obtain $\mathsf{Adv}^{\mathsf{DMA\text{-}ABE,PH}}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \le \left|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=1}^{\nu_H}\left|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)\right| + \sum_{\iota=1}^{3}\sum_{h=1}^{\nu_H}\left|\mathsf{Adv}^{(2\text{-}h\text{-}\iota)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}(\iota+1))}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(2\text{-}\nu_H\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + \sum_{h=1}^{\nu_H}\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h}}(\lambda) + \sum_{h=1}^{\nu_H}\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3,h}}(\lambda) + (2d\nu_H + 2d)/q \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu_H}\left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2,h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3,h}}(\lambda)\right) + ((2d+10)\nu_H + 2d + 5)/q$. This completes the proof of Theorem 1. □

We will show lemmas for the proof of Theorem 1. Below, advantages $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda), \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h}}(\lambda), \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3,h}}(\lambda)$ of adversaries for Problems 1, 2, and 3 are similarly defined as those for DMA-ABS which are given in Definitions 12, 13 and 16, respectively. The differences of the problems for DMA-ABE and DMA-ABS are just additional two dimensions for verifying hash values in DMA-ABS.

As indicated in Tables 1 and 2, game transformations for DMA-ABE are considered as parts of those for DMA-ABS, namely, Games 0, 1, 2-h-1, …, 2-h-4 (for $h = 1, \ldots, \nu_H$) and 3 for DMA-ABE correspond to Games 0, 1, 3-h-1, …, 3-h-4 (for $h = 1, \ldots, \nu_H$) and 5 for DMA-ABS. Therefore, proofs of lemmas for DMA-ABE are given by proofs of the corresponding lemmas for DMA-ABS.

Lemma 1: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.

Lemma 1 is proven in a similar manner to that of Lemma 14, which is given in Appendix B.2.

Lemma 2: For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \le 2d/q$.

Lemma 2 is proven in a similar manner to that of Lemma 16, which is given in Appendix B.4.

Lemma 3: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h}}(\lambda)$, where $\mathcal{B}_{2,h}(\cdot) := \mathcal{B}_2(h, \cdot)$.

Lemma 3 is proven in a similar manner to that of Lemma 17, which is given in Appendix B.5.

Lemma 4: For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda)$.

Lemma 4 is proven in a similar manner to that of Lemma 18, which is given in Appendix B.6.

Lemma 5: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_3$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3,h}}(\lambda)$, where $\mathcal{B}_{3,h}(\cdot) := \mathcal{B}_3(h, \cdot)$.

Lemma 5 is proven in a similar manner to that of Lemma 19, which is given in Appendix B.7.

Lemma 6: For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(2\text{-}\nu_H\text{-}4)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$.

Lemma 6 is proven in a similar manner to that of Lemma 21, which is given in Appendix B.9.

Lemma 7: For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$.

Proof. Since the value of s_0 in c_{d+1} is independent from all the other variables, the challenge bit b is independent of the advaersary's view in Game 3. Hence, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$. □

6. Decentralized Multi-Authority Attribute-Based Signatures (DMA-ABS)

6.1 Definitions of DMA-ABS

Definition 9 (Decentralized Multi-Authority ABS: DMA-ABS): A decentralized multi-authority ABS scheme consists of the following algorithms/protocols.

GSetup, ASetup, AttrGen are the same as those for DMA-ABE in Definition 7.

Sig This is a randomized algorithm. A user signs message m with claim-predicate (access structure) $\mathbb{S} := (M, \rho)$, only if there is a set of attributes Γ such that $\mathbb{S}$ accepts Γ, the user has obtained a set of keys $\{\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \mid (t, \vec{x}_t) \in \Gamma\}$ from the attribute authorities. Then signature σ can be generated using $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$, where $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$.

Ver To verify signature σ on message m with claim-predicate (access structure) $\mathbb{S}$, using a set of public keys for relevant authorities $\{\mathsf{apk}_t\}$, a user runs $\mathsf{Ver}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S}, \sigma)$ which outputs boolean value accept := 1 or reject := 0.

We let S the set of authorities. We assume each attribute is assigned to one authority.

6.2 Security Definition of DMA-ABS

The definition of perfect privacy for the decentralized multi-authority ABS is essentially the same as that of the ABS given in [19].

Definition 10 (Perfect Privacy of DMA-ABS): A DMA-ABS scheme is perfectly private, if, for all $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$, for all $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t)$ $(1 \le$

$t \le d$), all messages m, all attribute sets Γ_1 associated with gid_1 and Γ_2 associated with gid_2, all signing keys $\{\mathsf{usk}_{t,1} \xleftarrow{R} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_1, \vec{x}_{t,1})\}_{(t,\vec{x}_{t,1})\in\Gamma_1}$ and $\{\mathsf{usk}_{t,2} \xleftarrow{R} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_2, \vec{x}_{t,2})\}_{(t,\vec{x}_{t,2})\in\Gamma_2}$, all access structures $\mathbb{S}$ such that $\mathbb{S}$ accepts Γ_1 and $\mathbb{S}$ accepts Γ_2, the distributions $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{t,1} \mid (t,\vec{x}_{t,1}) \in \Gamma_1\}, m, \mathbb{S})$ and $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{t,2} \mid (t,\vec{x}_{t,2}) \in \Gamma_2\}, m, \mathbb{S})$ are equal.

For a DMA-ABS scheme with perfect privacy, we define algorithm $\mathsf{AltSig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{ask}_t\}, m, \mathbb{S})$ with $\mathbb{S}$ and master key ask_t instead of Γ and $\{\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}$: First, generate $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{R} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$ for arbitrary $\Gamma := \{(t,\vec{x}_t)\}$ which satisfies $\mathbb{S}$, then $\sigma \xleftarrow{R} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$. Return σ.

Definition 11 (Unforgeability of DMA-ABS): For an adversary, we define $\mathsf{Adv}^{\text{DMA-ABS,UF}}_{\mathcal{A}}(\lambda)$ to be the success probability in the following experiment for any security parameter λ. A DMA-ABS scheme is existentially unforgeable if the success probability of any polynomial-time adversary is negligible:

1. The challenger gives $\mathsf{gparam} \xleftarrow{R} \mathsf{GSetup}(1^\lambda)$ to adversary $\mathcal{A}$. Adversary $\mathcal{A}$ specifies a set $\mathcal{T}_{\mathsf{bad}} \subseteq \mathcal{T}$ of corrupt attribute authorities (and good (non-corrupt) authorities $\mathcal{T}_{\mathsf{good}} := \mathcal{T} \setminus \mathcal{T}_{\mathsf{bad}}$). For good authorities $t \in \mathcal{T}_{\mathsf{good}}$, The challenger runs $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{R} \mathsf{ASetup}(\mathsf{gparam}, t, n_t)$ and gives $\{\mathsf{apk}_t\}_{t\in\mathcal{T}_{\mathsf{good}}}$ to $\mathcal{A}$.
2. Adversary $\mathcal{A}$ is allowed to issue a polynomial number of queries, $(\mathsf{gid}, t, \vec{x}_t)$, to the challenger or oracle $\mathsf{AttrGen}(\mathsf{gparam}, \cdot, \mathsf{ask}_t, \cdot, \cdot)$ for attribute secret key $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ for good $t \in \mathcal{T}_{\mathsf{good}}$. $\mathcal{A}$ is also allowed to issue a polynomial number of signing queries, $(\mathsf{gid}, m, \mathbb{S} := (M,\rho), \Gamma)$ where Γ satisfies $\mathbb{S}$, with corrupted authority public keys $\{\mathsf{apk}_t\}$, and attribute secret keys $\{\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$ for corrupt $t \in \mathcal{T}_{\mathsf{bad}} \wedge (t,\vec{x}_t) \in \Gamma$, to the challenger. For good $t \in \mathcal{T}_{\mathsf{good}} \wedge (t,\vec{x}_t) \in \Gamma$, the challenger generates $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{R} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$. Then, he generates $\sigma \xleftarrow{R} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}, m, \mathbb{S})$ and gives it to $\mathcal{A}$.
3. At the end, the adversary outputs $(m', \mathbb{S}', \sigma')$ and corrupted authority public keys $\{\mathsf{apk}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$.

Let $\Gamma_{\mathsf{gid}_i} := \{(t,\vec{x}_t)\}$ queried to the $\mathsf{AttrGen}$ oracle with the i-th global identifier, gid_i, and $\Gamma_0 := \{(t,*)\}_{t\in\mathcal{T}_{\mathsf{bad}}}$, where $*$ denotes a wild card (an arbitrary value). We say the adversary succeeds, if $(m', \mathbb{S}')$ was never queried to Sig oracle, $\mathbb{S}'$ does not accept $\Gamma_{\mathsf{gid}_i} \cup \Gamma_0$ for any gid_i, and $\mathsf{Ver}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m', \mathbb{S}', \sigma') = 1$.

6.3 Construction Idea of the Proposed DMA-ABS Scheme

Here we will show some basic idea to construct the proposed DMA-ABS scheme. Our DMA-ABS scheme is constructed on the DMA- scheme given in Sect. 5.2.

Roughly speaking, a secret signing key sk_Γ with attribute set Γ and a verification text $\vec{c}$ with access structure $\mathbb{S}$ (for signature verification) in our DMA-ABS scheme correspond to a secret decryption key sk_Γ with Γ and a ciphertext $\vec{c}$ with $\mathbb{S}$ in the DMA-ABE scheme, respectively. No counterpart of a signature $\vec{s}^*$ in the DMA-ABS exists in the DMA-ABE, and the privacy property for signature $\vec{s}^*$ is also specific in DMA-ABS. Signature $\vec{s}^*$ in DMA-ABS may be interpreted to be a decryption key specialized to decrypt a ciphertext with access structure $\mathbb{S}$, that is delegated from secret key sk_Γ.

The algorithms of the proposed DMA-ABS scheme can be described in the light of such correspondence to the DMA-ABE scheme:

GSetup Almost the same as that in the DMA-ABE scheme except that a hash function, H_2, is added in gparam. This is used for hashing of message and access structure in the signing and verification algorithms.

ASetup Almost the same as that in the DMA-ABE scheme except that $\widehat{\mathbb{B}}^*_t$ is revealed as a *public* parameter in our DMA-ABS, while it is *secret* in the DMA-ABE scheme. They are published in our DMA-ABS for the signature generation procedure Sig to meet the *privacy* of signers (for randomization). This implies an important gap between DMA-ABE and DMA-ABS.
In [19], since (a part of) $\widehat{\mathbb{B}}^*_0$ is a master secret, other bases $\{\widehat{\mathbb{B}}^*_t\}_{t>0}$ can be public. However, in DMA-ABS, by lack of $\mathbb{V}_0$, public $\{\widehat{\mathbb{B}}^*_t\}_{t>0}$ should include *modified* $(\widetilde{\boldsymbol{b}}^*_{t,\iota})_{\iota=1,2}$ instead of sub-basis $(\boldsymbol{b}^*_{t,\iota})_{\iota=1,\ldots,n_t}$, which requires a new security proof in the dual system encryption.

$\mathsf{AttrGen}$ The same as that in the DMA-ABE scheme.

Sig Specific in DMA-ABS. To meet the privacy condition for $\vec{s}^*$, a novel technique is employed to randomly generate a signature from sk_Γ and $\{\widehat{\mathbb{B}}^*_t\}_{(t,\vec{x}_t)\in\Gamma}$. In [19], attribute vector $\vec{x}_t$ is encoded on n_t-dim. subspace $\mathsf{span}\langle \boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}\rangle$ in a secret key. However, in DMA-ABS, by lack of $\mathbb{V}_0$, the vector is also encoded on another $\mathsf{span}\langle \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,2n_t}\rangle$. To re-randomize both vectors independently using public $(\widetilde{\boldsymbol{b}}^*_{t,\iota}, \boldsymbol{b}^*_{t,n_t+\iota})_{\iota=1,\ldots,n_t}$ is a tricky part of our signature generation.

Ver Signature $\vec{s}^*$ in the DMA-ABS is an endorsement to message m by a signer with attributes accepted by access structure $\mathbb{S}$. The signature verification in our DMA-ABS checks whether a signature (or a specific decryption key) $\vec{s}^*$ works as a decryption key to decrypt a verification text (or a ciphertext) associated with $\mathbb{S}$ and $\mathsf{H}_2(m, \mathbb{S})$.

6.4 Proposed DMA-ABS Scheme

We define function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t,\vec{v})$ or $\rho(i) = \neg(t,\vec{v})$, where ρ is given in access structure $\mathbb{S} := (M,\rho)$. In the proposed scheme, we

assume that $\widetilde{\rho}$ is injective for $\mathbb{S} := (M, \rho)$ with signature $\sigma = \sigma_{\mathbb{S}}$. We showed how to relax the restriction in [47], however, for notational simplicity, we do not include the techniques for removing the restriction here. In the description of the scheme, we assume that input vector $\vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$ is normalized such that $x_{t,1} := 1$. (If $\vec{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \vec{x}_t$ assuming that $x_{t,1}$ is non-zero). In addition, we assume that input vector $\vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t})$ satisfies that $v_{i,n_t} \neq 0$. We refer to Sect. 1.5 for notations on DPVS, e.g., $(x_1, \ldots, x_N)_{\mathbb{B}}, (y_1, \ldots, y_N)_{\mathbb{B}^*}$ for $x_i, y_i \in \mathbb{F}_q$, and $\vec{e}_{t,j}$. For matrix $X := (\chi_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, for notation $\boldsymbol{g}X$, refer to Sect. 5.2.

$\mathsf{GSetup}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,
$H_1 : \{0,1\}^* \to \mathbb{G}$; $H_2 : \{0,1\}^* \to \mathbb{F}_q$;
return $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H_1, H_2)$.

Remark : Given gparam, the following values can be computed by anyone and shared by all parties:
$G_0 := H_1(0^\lambda) \in \mathbb{G}$, $G_1 := H_1(0^{\lambda-1}, 1) \in \mathbb{G}$,
$G_2 := H_1(0^{\lambda-2}, 1, 0) \in \mathbb{G}$, $g_T := e(G_0, G_1)$.

$\mathsf{ASetup}(\mathsf{gparam}, t)$: $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e)$
$:= \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5n_t + 3, \mathsf{param}_{\mathbb{G}})$, $X_t \xleftarrow{\cup} GL(5n_t + 3, \mathbb{F}_q)$,
$\boldsymbol{b}_{t,\iota} := (0^{\iota-1}, G_0, 0^{5n_t+3-\iota})X_t$,
$\boldsymbol{b}^*_{t,\iota} := (0^{\iota-1}, G_1, 0^{5n_t+3-\iota})(X_t^{\mathrm{T}})^{-1}$ for $\iota = 1, \ldots, 5n_t + 3$,
$\widetilde{\boldsymbol{b}}^*_{t,\iota} := (\overbrace{0^{\iota-1}, G_2, 0^{n_t-\iota}}^{n_t}, \overbrace{0^{3n_t+2}}^{3n_t+2}, \overbrace{\widetilde{\varphi}_{t,\iota,1}G_1, .., \widetilde{\varphi}_{t,\iota,n_t}G_1}^{n_t}, 0)(X_t^{\mathrm{T}})^{-1}$,
where $\vec{\widetilde{\varphi}}_{t,\iota} := (\widetilde{\varphi}_{t,\iota,1}, \ldots, \widetilde{\varphi}_{t,\iota,n_t}) \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, for $\iota = 1, \ldots, n_t$,
$\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,5n_t+3})$, $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,5n_t+3})$,
$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,5n_t+3})$,
$\widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1}, .., \widetilde{\boldsymbol{b}}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+1}, .., \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, .., \boldsymbol{b}^*_{t,5n_t+2})$,
return $\mathsf{ask}_t := X_t$, $\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t)$.

Remark : Let $\pi \in \mathbb{F}_q$ s.t. $G_2 = \pi G_1$, then
$\widetilde{\boldsymbol{b}}^*_{t,\iota} = (\overbrace{\pi\vec{e}_{t,\iota}}^{n_t}, \overbrace{0^{3n_t+2}}^{3n_t+2}, \overbrace{\vec{\widetilde{\varphi}}_{t,\iota}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t}$ for $\iota = 1, .., n_t$.

$\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t := (x_{t,1}, .., x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ such that $x_{t,1} := 1)$:
$G_{\mathsf{gid}} := H_1(\mathsf{gid})$, $\vec{\varphi}_t := (\varphi_{t,1}, \ldots, \varphi_{t,n_t}) \xleftarrow{\cup} \mathbb{F}_q^{n_t}$,
$\boldsymbol{k}^*_t := (\overbrace{x_{t,1}G_1, .., x_{t,n_t}G_1}^{n_t}, \overbrace{x_{t,1}G_{\mathsf{gid}}, .., x_{t,n_t}G_{\mathsf{gid}}}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\varphi_{t,1}G_1, .., \varphi_{t,n_t}G_1}^{n_t}, \overbrace{0}^{1})(X_t^{\mathrm{T}})^{-1}$,
return $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}^*_t)$.

Remark : Let $\delta \in \mathbb{F}_q$ s.t. $G_{\mathsf{gid}} = \delta G_1$,
then $\boldsymbol{k}^*_t = (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta\vec{x}_t}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\varphi}_t}^{n_t}, 0)_{\mathbb{B}^*_t}$.

$\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}^*_t)\}, m, \mathbb{S} := (M, \rho))$:
If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$, then compute I and $\{\alpha_i\}_{i \in I}$ such that $\vec{1} = \sum_{i \in I} \alpha_i M_i$, where M_i is the i-th row of M, and
$I \subseteq \{i \in \{1, .., \ell\} | \ [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0]$
$\vee \ [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0] \}$,
$\psi \xleftarrow{\cup} \mathbb{F}_q$, $\psi_i := \psi$ if $i \in I$, $\psi_i := 0$ if $i \notin I$ for $i = 1, \ldots, \ell$,
for $i = 1, \ldots, \ell$, $\zeta_i \xleftarrow{\cup} \mathbb{F}_q$,
$(\beta_{i,0}), (\beta_{i,1}) \xleftarrow{\cup} \{(\beta_1, \ldots, \beta_\ell) \mid \sum_{i=1}^{\ell} \beta_i M_i = \vec{0}\}$,
$\boldsymbol{s}^*_i := \gamma_i \cdot \boldsymbol{k}^*_t + \sum_{\iota=1}^{n_t} \left(y_{i,0,\iota} \widetilde{\boldsymbol{b}}^*_{t,\iota} + (\psi_i x_{t,\iota} + y_{i,1,\iota}) \boldsymbol{b}^*_{t,n_t+\iota} \right)$
$+\zeta_i \left(\boldsymbol{b}^*_{t,2n_t+1} + H_2(m, \mathbb{S}) \boldsymbol{b}^*_{t,2n_t+2} \right) + \boldsymbol{r}^*_i$,
where $\boldsymbol{r}^*_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}^*_{t,4n_t+3}, .., \boldsymbol{b}^*_{t,5n_t+2} \rangle$,
and $\gamma_i, \vec{y}_{i,j} := (y_{i,j,1}, .., y_{i,j,n_t})$ for $j = 0, 1$,
are defined as
if $i \in I \wedge \rho(i) = (t, \vec{v}_i)$,
$\gamma_i := \alpha_i$, $\vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j} \cdot \vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\}$,
if $i \in I \wedge \rho(i) = \neg(t, \vec{v}_i)$,
$\gamma_i := \alpha_i / (\vec{v}_i \cdot \vec{x}_t)$, $\vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j} \cdot \vec{v}_i = \beta_{i,j}\}$,
if $i \notin I \wedge \rho(i) = (t, \vec{v}_i)$,
$\gamma_i := 0$, $\vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j} \cdot \vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\}$,
if $i \notin I \wedge \rho(i) = \neg(t, \vec{v}_i)$,
$\gamma_i := 0$, $\vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j} \cdot \vec{v}_i = \beta_{i,j}\}$,
return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}^*_1, \ldots, \boldsymbol{s}^*_\ell)$.

$\mathsf{Ver}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S} := (M, \rho), \vec{\boldsymbol{s}}^*)$:
$\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,
$\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ s.t. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0$, $\vec{s}'^{\mathrm{T}} := (s'_1, \ldots, s'_\ell)^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$,
for $i = 1, \ldots, \ell$,
if $\rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ s. t. $v_{i,n_t} \neq 0)$,
$\theta_i, \theta'_i, \theta''_i, \eta_i \xleftarrow{\cup} \mathbb{F}_q$,
$\boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i}^{n_t}, \overbrace{\theta''_i(H_2(m, \mathbb{S}), -1)}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}$,
if $\rho(i) = \neg(t, \vec{v}_i)$, $\theta''_i, \eta_i \xleftarrow{\cup} \mathbb{F}_q$,
$\boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{v}_i}^{n_t}, \overbrace{\theta''_i(H_2(m, \mathbb{S}), -1)}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}$,
$c_{d+1} := g_T^{s_0}$,
return 1 if $\prod_{i=1}^{\ell} e(\boldsymbol{c}_i, \boldsymbol{s}^*_i) = c_{d+1}$, return 0 otherwise.

[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$,

$$\prod_{i=1}^{\ell} e(\boldsymbol{c}_i, \boldsymbol{s}_i^*) =$$
$$\prod_{i\in I} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\gamma_i} \prod_{i=1}^{\ell} \prod_{\iota=1}^{n_t} e(\boldsymbol{c}_i, \widetilde{\boldsymbol{b}}_\iota^*)^{y_{i,0,\iota}} e(\boldsymbol{c}_i, \boldsymbol{b}_{n_t+\iota}^*)^{(\psi_i x_{t,\iota} + y_{i,1,\iota})}$$
$$= \prod_{i\in I} g_T^{\alpha_i(s_i+(\delta+\psi)s_i')} \cdot \prod_{i=1}^{\ell} g_T^{\pi\beta_{i,0}s_i+\beta_{i,1}s_i'}$$
$$= g_T^{\sum_{i\in I}\alpha_i(s_i+(\delta+\psi)s_i')} \cdot g_T^{\sum_{i=1}^{\ell}(\pi\beta_{i,0}s_i+\beta_{i,1}s_i')} = g_T^{s_0}, \text{ since}$$
$\sum_{i\in I}\alpha_i s_i = s_0$ and $\sum_{i\in I}\alpha_i s_i' = \sum_{i=1}^{\ell}\beta_{i,0}s_i = \sum_{i=1}^{\ell}\beta_{i,1}s_i' = 0$.

6.5 Security of the Proposed DMA-ABS

Theorem 2: The proposed DMA-ABS scheme is perfectly private.

Proof. Before starting the proof, we first define function AltSig specified in the proposed DMA-ABS scheme as follows:

$$\begin{array}{l}
\mathsf{AltSig}(\mathsf{gparam},\ \{\mathsf{apk_t}, \mathsf{ask}_t\},\ m,\ \mathbb{S}) \\
\quad \widetilde{\delta} \xleftarrow{\cup} \mathbb{F}_q,\ \ (\xi_i), (\xi_i') \xleftarrow{\cup} \{(\xi_1, \ldots, \xi_\ell)\ \mid\ \textstyle\sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\}, \\
\quad \text{for } i = 1, \ldots, \ell, \\
\quad \left.\begin{array}{l}
\text{if } \rho(i) = (t, \vec{v}_i), \text{ then} \\
\quad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0}\cdot\vec{v}_i = \vec{z}_{i,1}\cdot\vec{v}_i = 0, \\
\qquad z_{i,0,1} = \xi_i,\ z_{i,1,1} = \widetilde{\delta}\xi_i'\ \}, \\
\text{if } \rho(i) = \neg(t, \vec{v}_i), \text{ then} \\
\quad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0}\cdot\vec{v}_i = \xi_i, \vec{z}_{i,1}\cdot\vec{v}_i = \widetilde{\delta}\xi_i'\},
\end{array}\right\} \quad (9) \\
\quad \boldsymbol{s}_i^* := (\overbrace{\vec{z}_{i,0}, \vec{z}_{i,1}}^{2n_t}, \overbrace{\zeta_i(1, H_2(m, \mathbb{S}))}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\sigma}_i}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}, \\
\quad \text{where } \zeta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\sigma}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t},\ \text{return } \vec{\boldsymbol{s}}^* := (\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*).
\end{array}$$

Remark: Theorem 2 implies that AltSig defined above is equivalent to AltSig defined just after Definition 10, and this justifies the notations.

We now start the proof. This theorem is true if the following statement is true, where AltSig is defined above:

For all $\mathsf{gparam} \xleftarrow{R} \mathsf{GSetup}(1^\lambda)$, $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{R} \mathsf{ASetup}(\mathsf{gparam}, t)$, all messages m, all attribute sets Γ associated with gid, all signing keys $\{\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{R} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)\}$, all access structures $\mathbb{S}$ such that $\mathbb{S}$ accepts $\Gamma := \{(t, \vec{x}_t)\}$, the distributions of $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$ and $\mathsf{AltSig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{ask}_t\}, m, \mathbb{S})$ are equal.

In the proposed DMA-ABS scheme, $(\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*) \xleftarrow{R} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$ are expressed by

$$\begin{array}{l}
\boldsymbol{s}_i^* := (\vec{z}_{i,0}, \vec{z}_{i,1}, \zeta_i(1, H_2(m, \mathbb{S})), 0^{2n_t}, \vec{\sigma}_i, 0)_{\mathbb{B}_t^*}\ (i = 1, \ldots, \ell+1), \\
\text{where, for } 1 \le i \le \ell, \\
\quad \text{if } i \in I\ \wedge\ \rho(i) = (t, \vec{v}_i), \\
\qquad \vec{z}_{i,0} = \alpha_i\vec{x}_t + \pi\vec{y}_{i,0}\ \ \vec{z}_{i,1} = \alpha_i(\delta+\psi)\vec{x}_t + \vec{y}_{i,1} \\
\qquad \text{where } \vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\} \text{ for } j = 0, 1, \\
\quad \text{if } i \in I\ \wedge\ \rho(i) = \neg(t, \vec{v}_i),\ \ \vec{z}_{i,0} = (\alpha_i/(\vec{v}_i\cdot\vec{x}_t))\vec{x}_t + \pi\vec{y}_{i,0}, \\
\qquad \vec{z}_{i,1} = (\alpha_i/(\vec{v}_i\cdot\vec{x}_t))(\delta+\psi)\vec{x}_t + \vec{y}_{i,1}, \\
\qquad \text{where } \vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j}\ \mid\ \vec{y}_{i,j}\cdot\vec{v}_i = \beta_{i,j}\}\ \text{ for } j = 0, 1, \\
\quad \text{if } i \notin I\ \wedge\ \rho(i) = (t, \vec{v}_i),\ \ \vec{z}_{i,0} = \pi\vec{y}_{i,0},\ \ \vec{z}_{i,1} = \vec{y}_{i,1}, \\
\qquad \text{where } \vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\} \text{ for } j = 0, 1, \\
\quad \text{if } i \notin I\ \wedge\ \rho(i) = \neg(t, \vec{v}_i),\ \ \vec{z}_{i,0} = \pi\vec{y}_{i,0},\ \ \vec{z}_{i,1} = \vec{y}_{i,1}, \\
\qquad \text{where } \vec{y}_{i,j} \xleftarrow{\cup} \{\vec{y}_{i,j}\ \mid\ \vec{y}_{i,j}\cdot\vec{v}_i = \beta_{i,j}\}\ \text{ for } j = 0, 1,
\end{array}$$

Let $\vec{\alpha}' := (\alpha_1', \ldots, \alpha_\ell')$ such that $\alpha_i' := \alpha_i$ if $i \in I$ and $\alpha_i' := 0$ if $i \notin I$, and $\widetilde{\delta} := \delta + \psi$, then it can be rephrased by

$$\begin{array}{l}
\text{for } 1 \le i \le \ell, \\
\quad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1})\ \mid\ \vec{z}_{i,0}\cdot\vec{v}_i = \vec{z}_{i,1}\cdot\vec{v}_i = 0 \\
\qquad \wedge\ z_{i,0,1} = \alpha_i' + \pi\beta_{i,0},\ z_{i,1,1} = \widetilde{\delta}\alpha_i' + \beta_{i,1}\} \text{ if } \rho(i) = (t, \vec{v}_i), \\
\quad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0}\cdot\vec{v}_i = \alpha_i' + \pi\beta_{i,0}, \\
\qquad \vec{z}_{i,1}\cdot\vec{v}_i = \widetilde{\delta}\alpha_i' + \beta_{i,1}\} \text{ if } \rho(i) = \neg(t, \vec{v}_i),
\end{array}$$

where $\widetilde{\delta}$ is uniformly and independently distributed in $\mathbb{F}_q$ for each signature generation.

On the other hand, $(\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*) \xleftarrow{R} \mathsf{AltSig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{ask}_t\}, m, \mathbb{S})$ are expressed by

$$\begin{array}{l}
\boldsymbol{s}_i^* := (\vec{z}_{i,0}, \vec{z}_{i,1}, \zeta_i(1, H_2(m, \mathbb{S})), 0^{2n_t}, \vec{\sigma}_i, 0)_{\mathbb{B}_t^*}, \text{ where} \\
\quad \text{for } i = 1, \ldots, \ell, \\
\qquad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0}\cdot\vec{v}_i = \vec{z}_{i,1}\cdot\vec{v}_i = 0, \\
\qquad\qquad z_{i,0,1} = \xi_i,\ z_{i,1,1} = \widetilde{\delta}\xi_i'\ \},\ \text{if } \rho(i) = (t, \vec{v}_i), \\
\qquad (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1})\ \mid\ \vec{z}_{i,0}\cdot\vec{v}_i = \xi_i,\ \ \vec{z}_{i,1}\cdot\vec{v}_i = \widetilde{\delta}\xi_i'\ \}, \\
\qquad\qquad \text{if } \rho(i) = \neg(t, \vec{v}_i).
\end{array}$$

For any $\{\alpha_i'\}$ such that $\sum_{i=1}^{\ell}\alpha_i' M_i = \vec{1}$ and $\pi \in \mathbb{F}_q^\times$, the distributions of

$$\begin{array}{l}
\Big((\alpha_1' + \pi\beta_{1,0},\ \widetilde{\delta}\alpha_1' + \beta_{1,1}), \ldots, (\alpha_\ell' + \pi\beta_{\ell,0},\ \widetilde{\delta}\alpha_\ell' + \beta_{\ell,1})\Big) \\
\quad \text{s.t. } \widetilde{\delta} \xleftarrow{\cup} \mathbb{F}_q,\ (\beta_{i,0}), (\beta_{i,1}) \xleftarrow{\cup} \{(\beta_i)\ \mid\ \textstyle\sum_{i=1}^{\ell}\beta_i M_i = \vec{0}\} \text{ and} \\
((\xi_1,\ \widetilde{\delta}\xi_1'), \ldots, (\xi_\ell,\ \widetilde{\delta}\xi_\ell')) \\
\quad \text{s.t. } \ \widetilde{\delta} \xleftarrow{\cup} \mathbb{F}_q,\ \ (\xi_i), (\xi_i') \xleftarrow{\cup} \{(\xi_i)\ \mid\ \textstyle\sum_{i=1}^{\ell}\xi_i M_i = \vec{1}\ \},
\end{array}$$

are equivalent. Therefore, distributions $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$ and $\mathsf{AltSig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{ask}_t\}, m, \mathbb{S})$ are equivalent. □

Theorem 3: The proposed DMA-ABS scheme is unforgeable (adaptive-predicate unforgeable) under the DLIN assumption in the random oracle model.

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_{3\text{-}1}, \mathcal{E}_{3\text{-}2}$ and $\mathcal{E}_4$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\begin{array}{l}
\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABS,UF}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu_S}\mathsf{Adv}_{\mathcal{E}_{2\text{-}h}}^{\mathsf{DLIN}}(\lambda) \\
\qquad + \sum_{h=1}^{\nu_H}\Big(\mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda)\Big) + \mathsf{Adv}_{\mathcal{E}_4}^{\mathsf{DLIN}}(\lambda) + \epsilon,
\end{array}$$

where $\mathcal{E}_{2\text{-}h}(\cdot) := \mathcal{E}_2(h, \cdot), \mathcal{E}_{3\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{3\text{-}1}(h, \cdot), \mathcal{E}_{3\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{3\text{-}2}(h, \cdot)$, ν_S (resp. ν_H) is the maximum number of queries

Table 2 Outline of game descriptions for Theorem 3: in the table, norm., temp., pre-s.f., s.f., and non-f. stand for normal, temporal, pre-semi-functional, semi-functional, and non-functional, respectively.

	challenge	queried signatures					queried keys					$\widetilde{\boldsymbol{b}}^*_{t,\iota}$
	CT	1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν_S	1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν_H	
Game 0	norm.	norm.					norm.					norm.
1	temp.	norm.					norm.					norm.
2-1	temp.	s.f.	norm.				norm.					norm.
					$\vdots$							
2-h	temp.	s.f.		s.f.	norm.		norm.					norm.
					$\vdots$							
2-ν_S	temp.	s.f.				s.f.	norm.					norm.
3-1-1	pre-s.f.	s.f.					norm.					norm.
3-1-2	pre-s.f.	s.f.					pre-s.f.	norm.				norm.
3-1-3	s.f.	s.f.					pre-s.f.	norm.				norm.
3-1-4	s.f.	s.f.					s.f.	norm.				norm.
					$\vdots$							
3-h-1	pre-s.f.	s.f.					s.f.		norm.			norm.
3-h-2	pre-s.f.	s.f.					s.f.		pre-s.f.	norm.		norm.
3-h-3	s.f.	s.f.					s.f.		pre-s.f.	norm.		norm.
3-h-4	s.f.	s.f.					s.f.		s.f.	norm.		norm.
					$\vdots$							
3-ν_H-4	s.f.	s.f.					s.f.				s.f.	norm.
4	s.f.	s.f.					s.f.					s.f.
5	non-f.	s.f.					s.f.					s.f.

to signing oracle (resp. random oracle H_1), and $\epsilon := ((d+6)\nu_S + (2d+10)\nu_H + 3d + 11)/q$.

6.5.1 Proof Outline of Theorem 3

As mentioned in Sect. 6.3, secret signing keys and verification texts in our DMA-ABS are the counterparts of secret decryption keys and ciphertexts in DMA-ABE. Based on this correspondence, we follow the dual system encryption methodology proposed by Waters [46], at the top level of strategy of the unforgeability proof. Signatures have two forms, *normal* and *semi-functional*, secret keys have three forms, *normal*, *pre-semi-functional* and *semi-functional*, and verification texts (ciphertexts) have four forms, *normal*, *temporal*, *pre-semi-functional* and *semi-functional* (see Table 2). The real system uses only normal forms, and other forms are used only in a sequence of security games for the security proof. (Additionally, verification texts have *non-functional* form. See below.) In addition to verification texts, secret keys and signatures, a part of public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, has two forms, *normal* and *semi-functional*.

We employ Game 0 through Game 5. In Game 1, the verification text is changed to temporal form. When at most ν_S signature queries are issued by an adversary, there are ν_S game changes from Game 1 (Game 2-0), Game 2-1 through Game 2-ν_S. In Game 2-h, the first h (including the h-th queried) signatures are changed to semi-functional form, while the remaining signatures are normal.

Then, when at most ν_H random oracle queries for H_1 are issued by an adversary, there are $4\nu_H$ game changes from Game 2-ν_S (Game 3-0-4), Game 3-1-1, Game 3-1-2, Game 3-1-3, Game 3-1-4 through Game 3-ν_H-1, Game 3-ν_H-2, Game 3-ν_H-3, Game 3-ν_H-4.

In Game 3-h-1, the verification text is changed to pre-semi-functional form, and keys for the first $h-1$ random-oracle queried global identities, gid, are semi-functional form, while the remaining keys are normal. In Game 3-h-2, key for the h-th global identity is changed to pre-semi-functional form while the remaining keys and the verification text is the same as in Game 3-h-1. In Game 3-h-3, the verification text is changed to semi-functional form while all the queried keys are the same as in Game 3-h-2. In Game 3-h-4, key for the h-th global identity is changed to semi-functional form while the remaining keys and the verification text is the same as in Game 3-h-3. At the end of the Game 3 sequence, in Game 3-ν_H-4, all the queried keys are semi-functional forms (and the verification text is semi-functional form). In Game 4, a part of authority public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, are changed to semi-functional form. In Game 5, the verification text is changed to *non-functional* form since all the queried signatures, keys, and $\widetilde{\boldsymbol{b}}^*_{t,\iota}$ are semi-functional form. In the final game, advantage of the adversary is at most $1/q$.

We summarize these changes in Table 2, where shaded

parts indicate the verification text, keys, signatures, public keys which were changed in a game from the previous game.

As usual, we prove that the advantage gaps between neighboring games are negligible.

We denote verification text by $\vec{c} := (c_1, \ldots, c_\ell)$, and keys by $\vec{k}^* := (k_t^*)_{(t,\vec{x}_t)\in\Gamma}$ in this proof outline. In addition, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \leq B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

A normal secret key, $\vec{k}^{*\,\mathsf{norm}}$ (with attributes $(t, \vec{x}_t)$), is expressed by Eq. (10), and a normal signature, $\vec{s}^{*\,\mathsf{norm}}$ (with access structure $\mathbb{S}$) is expressed by Eq. (12), which are the correct forms of the secret key and signatures of the proposed DMA-ABS scheme, respectively. Similarly, a normal verification text (with $\mathbb{S}$), $\vec{c}^{\,\mathsf{norm}}$, is expressed by Eq. (13), and normal form of (a part of) public key $\widetilde{b}_{t,\iota}^{\mathsf{norm}}$ is given in Eq. (11). A temporal verification text is expressed by Eq. (14). A semi-functional signature, $\vec{s}^{\,\mathsf{semi}}$, is expressed by Eq. (15). A pre-semi-functional verification text, $\vec{c}^{\,\mathsf{pre\text{-}semi}}$, is expressed by Eq. (16) and a pre-semi-functional secret key, $\vec{k}^{*\,\mathsf{pre\text{-}semi}}$, is expressed by Eq. (17). A semi-functional verification text, $\vec{c}^{\,\mathsf{semi}}$, is expressed by Eq. (18) and a semi-functional secret key, $\vec{k}^{*\,\mathsf{semi}}$, is expressed by Eq. (19). A non-functional verification text, $\vec{c}^{\,\mathsf{non\text{-}f}}$, is expressed by Eq. (21).

To prove that the advantage gap between Games 0 and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0, 1\}$), we construct a simulator of the challenger of Game 0 (or 1) (against an adversary $\mathcal{A}$) by using an instance with $\beta \xleftarrow{\cup} \{0, 1\}$ of Problem 1. We then show that the distribution of the secret keys and verification text (in the final step) used by the simulator is equivalent to those of Game 0 when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma 14). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 8).

The advantage gap between Games 2-$(h-1)$ and 2-h is shown to be bounded by the advantage of Problem 2', i.e., advantage of the DLIN assumption (Lemmas 15 and 10).

We then show that Game 3-$(h-1)$-4 can be conceptually changed to Game 3-h-1 (Lemma 16), by using the fact that parts of bases, $(\boldsymbol{b}_{t,2n_t+3}, \ldots, \boldsymbol{b}_{t,4n_t+2})$ and $(\boldsymbol{b}^*_{t,2n_t+3}, \ldots, \boldsymbol{b}^*_{t,4n_t+2})$, are unknown to the adversary. In particular, when $h = 1$, it means that Game 1 can be conceptually changed to Game 3-1-1. When $h \geq 2$, we notice that normal key and semi-functional verification text, $(\vec{k}^{*\,\mathsf{norm}}, \vec{c}^{\,\mathsf{semi}})$, are equivalent to normal key and pre-semi-functional verification text, $(\vec{k}^{*\,\mathsf{norm}}, \vec{c}^{\,\mathsf{pre\text{-}semi}})$, except that (0-)shared secret $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 = 0$ is used in $\vec{c}^{\,\mathsf{pre\text{-}semi}}$ instead of ordinary shared secret $\{r''_i\}_{i=1,\ldots,\ell}$ with $r''_0 \xleftarrow{\cup} \mathbb{F}_q$ for some coefficient vector in $\vec{c}^{\,\mathsf{semi}}$. This change of coefficient vectors can be done conceptually since zero vector 0^{n_t} is used for the corresponding part in $\vec{k}^{*\,\mathsf{norm}}$.

The advantage gap between Games 3-h-1 and 3-h-2 is shown to be bounded by the advantage of Problem 2, i.e., advantage of the DLIN assumption (Lemmas 17 and 9).

We then show that Game 3-h-2 can be conceptually changed to Game 3-h-3 (Lemma 18), where we use the fact that all queried keys $\{(t, \vec{x}_t)\}$ do not satisfy $\mathbb{S}$ that adversary output. Here, we notice that pre-semi-functional key and pre-semi-functional verification text, $(\boldsymbol{k}^{*\,\mathsf{pre\text{-}semi}}, \boldsymbol{c}^{\mathsf{pre\text{-}semi}})$, are equivalent to pre-semi-functional key and semi-functional challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{pre\text{-}semi}}, \boldsymbol{c}^{\mathsf{semi}})$, except that shared secret $\{r''_i\}_{i=1,\ldots,\ell}$ with $r''_0 \xleftarrow{\cup} \mathbb{F}_q$ is used in $\boldsymbol{c}^{\mathsf{semi}}$ instead of $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 = 0$ for some coefficient vector in $\boldsymbol{c}^{\mathsf{pre\text{-}semi}}$. Therefore, this conceptual change is proved using Lemma 13.

The advantage gap between Games 3-h-3 and 3-h-4 is similarly shown to be bounded by the advantage of Problem 3, i.e., advantage of the DLIN assumption (Lemmas 19 and 12).

We then show that the advantage gap between Games 3-ν_H-4 and 4 is bounded by the advantage of Problem 2", i.e., advantage of the DLIN assumption (Lemmas 20 and 11).

We then show that Game 4 can be conceptually changed to Game 5 (Lemma 21) by using the fact that parts of bases, $(\boldsymbol{b}_{t,3n_t+3}, \ldots, \boldsymbol{b}_{t,4n_t+2})$ and $(\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t})$, are unknown to the adversary.

Proof : To prove Theorem 3, we consider the following $(\nu_S + 4\nu_H + 4)$ games. In Game 0, a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0 : Original security game. That is, $\boldsymbol{k}_t^{(h)*} \in \mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$, which is a reply to $\mathsf{AttrGen}$ query for the h-th global identity, $(\mathsf{gid}_h, (t, \vec{x}_t))$ with $t \in S$ for $h = 1, \ldots, \nu_H$ is:

$$\boldsymbol{k}_t^{(h)*} := (\overbrace{\vec{x}_t^{(h)}}^{n_t}, \overbrace{\delta^{(h)}\vec{x}_t^{(h)}}^{n_t}, \overbrace{0^2}^{2}, \overbrace{\boxed{0^{2n_t}}}^{2n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}, \tag{10}$$

where $\delta^{(h)} \xleftarrow{\cup} \mathbb{F}_q, \vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, and $\{\widetilde{\boldsymbol{b}}^*_{t,\iota}\}_{\iota=1,\ldots,n_t}$, which is a part of apk_t is:

$$\widetilde{\boldsymbol{b}}^*_{t,\iota} := (\overbrace{\pi\vec{e}_{t,\iota}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^2}^{2}, \overbrace{0^{n_t}, \boxed{0^{n_t}}}^{2n_t}, \overbrace{\vec{\varphi}_{t,\iota}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*} \tag{11}$$

for $\iota = 1, \ldots, n_t$, where $\pi \xleftarrow{\cup} \mathbb{F}_q, \vec{\varphi}_{t,\iota} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, and $\{\boldsymbol{s}_i^{(h)*}\}_{i=1,\ldots,\ell}$, which is a reply to the h-th AltSig query for $(m^{(h)}, \mathbb{S}^{(h)})$ with $\mathbb{S}^{(h)} := (M, \rho)$ for $h = 1, \ldots, \nu_S$ is:

$$\boldsymbol{s}_i^{(h)*} := (\overbrace{\vec{w}_i^{(h)}}^{n_t}, \overbrace{\vec{w}_i'^{(h)}}^{n_t}, \overbrace{\zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)}))}^{2}, \overbrace{0^{n_t}, \boxed{0^{n_t}}}^{2n_t}, \overbrace{\vec{\sigma}_i}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}, \tag{12}$$

where $\widetilde{\delta}, \zeta_i \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\sigma}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}, (\xi_i), (\xi'_i) \xleftarrow{\cup} \{(\xi_1, \ldots, \xi_\ell) \mid$

$\sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\}$, and for $i = 1, \ldots, \ell$, if $\rho(i) = (t, \vec{v}_i)$, then $(\vec{w}_i^{(h)}, \vec{w}_i'^{(h)}) \xleftarrow{\cup} \{(\vec{w}_i, \vec{w}_i') \mid \vec{w}_i \cdot \vec{v}_i = \vec{w}_i' \cdot \vec{v}_i = 0$, the 1-st coordinate of $\vec{w}_i = \xi_i$, the 1-st coordinate of $\vec{w}_i' = \widetilde{\delta}\xi_i'\}$, if $\rho(i) = \neg(t, \vec{v}_i)$, then $(\vec{w}_i^{(h)}, \vec{w}_i'^{(h)}) \xleftarrow{\cup} \{(\vec{w}_i, \vec{w}_i') \mid \vec{w}_i \cdot \vec{v}_i = \xi_i,\ \vec{w}_i' \cdot \vec{v}_i = \widetilde{\delta}\xi_i'\}$, and the verification text $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1}$, for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$, which is used for verification of the output of the adversary $\mathcal{A}$ at the end of the game is:

$$\left.\begin{array}{l}
\text{if } \rho(i) = (t, \vec{v}_i), \\
\boldsymbol{c}_i := (\overbrace{\boxed{s_i}\vec{e}_{t,1} + \theta_i \vec{v}_i}^{n_t}, \overbrace{s_i' \vec{e}_{t,1} + \theta_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{\boxed{0^{2n_t}}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\
\text{if } \rho(i) = \neg(t, \vec{v}_i), \\
\boldsymbol{c}_i := (\overbrace{\boxed{s_i}\vec{v}_i}^{n_t}, \overbrace{s_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{\boxed{0^{2n_t}}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\
c_{d+1} := g_T^{s_0},
\end{array}\right\} \tag{13}$$

where $\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, \vec{f}' \xleftarrow{\cup} \{\vec{f}' \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, s_i := M_i \cdot \vec{f}^{\mathrm{T}}, s_i' := M_i \cdot \vec{f}'^{\mathrm{T}}, \theta_i, \theta_i', \theta_i'', \eta_i \xleftarrow{\cup} \mathbb{F}_q$.

Game 1 : Same as Game 0 except that (a part of) the verification text, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$, for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$, which is used for verification of the output of $\mathcal{A}$ at the end of the game is:

$$\left.\begin{array}{l}
\text{for } i = 1, \ldots, \ell, \\
\text{if } \rho(i) = (t, \vec{v}_i) \ \wedge\ t \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{c}_i := (\overbrace{s_i \vec{e}_{t,1} + \theta_i \vec{v}_i}^{n_t}, \overbrace{s_i' \vec{e}_{t,1} + \theta_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{0^{n_t}, \boxed{\vec{z}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\
\text{if } \rho(i) = \neg(t, \vec{v}_i) \ \wedge\ t \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{c}_i := (\overbrace{s_i \vec{v}_i}^{n_t}, \overbrace{s_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{0^{n_t}, \boxed{\vec{z}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},
\end{array}\right\} \tag{14}$$

where $\vec{z}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, and the other variables are generated as in Game 0.

Game 2-h ($h = 1, \ldots, \nu_S$): Game 2-0 is Game 1. Game 2-h is the same as Game 2-$(h-1)$ except that the reply $\{\boldsymbol{s}_i^{(h)*}\}_{i=1,\ldots,\ell}$ to the h-th AltSig query for $(m^{(h)}, \mathbb{S}^{(h)} := (M, \rho))$ is:

$$\left.\begin{array}{l}
\text{for } i = 1, \ldots, \ell, \\
\text{if } (\rho(i) = (t, \vec{v}_i) \ \vee\ \rho(i) = \neg(t, \vec{v}_i)) \ \wedge\ t \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{s}_i^{(h)*} := (\overbrace{\vec{w}_i^{(h)}}^{n_t}, \overbrace{\vec{w}_i'^{(h)}}^{n_t}, \overbrace{\zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)}))}^{2}, \\
\qquad \overbrace{0^{n_t}, \boxed{\vec{u}_i^{(h)}}}^{2n_t}, \overbrace{\vec{\sigma}_i}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*},
\end{array}\right\} \tag{15}$$

where $\vec{u}_i^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, and the other variables are generated as in Game 2-$(h-1)$.

Game 3-h-1 ($h = 1, \ldots, \nu_H$) : Game 3-0-4 is Game 2-ν_S. Same as Game 3-$(h-1)$-4 except that (a part of) the verification text, $\boldsymbol{c}_i$, for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$ in the final step:

$$\left.\begin{array}{l}
\text{for } i = 1, \ldots, \ell, \\
\text{If } \rho(i) = (t, \vec{v}_i) \ \wedge\ t \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{c}_i := (\overbrace{s_i \vec{e}_{t,1} + \theta_i \vec{v}_i}^{n_t}, \overbrace{s_i' \vec{e}_{t,1} + \theta_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{\boxed{(r_i \vec{e}_{t,1} + \omega_i \vec{v}_i) \cdot Z_t,\ \ r_i' \vec{e}_{t,1} + \omega_i' \vec{v}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \\
\text{If } \rho(i) = \neg(t, \vec{v}_i) \ \wedge\ t \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{c}_i := (\overbrace{s_i \vec{v}_i}^{n_t}, \overbrace{s_i' \vec{v}_i}^{n_t}, \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2}, \\
\qquad \overbrace{\boxed{r_i \vec{v}_i \cdot Z_t,\ r_i' \vec{v}_i}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},
\end{array}\right\} \tag{16}$$

where $\vec{g} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0,\ M_i \cdot \vec{g}^{\mathrm{T}} = 0$ for $\forall i$ s.t., $\widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}, \vec{g}' \xleftarrow{\cup} \{\vec{g}' \in \mathbb{F}_q^r \mid M_i \cdot \vec{g}'^{\mathrm{T}} = 0$ for $\forall i$ s.t., $\widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}, r_i := M_i \cdot \vec{g}^{\mathrm{T}}, r_i' := M_i \cdot \vec{g}'^{\mathrm{T}}, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q),\ \omega_i, \omega_i' \xleftarrow{\cup} \mathbb{F}_q$, and the other variables are generated as in Game 3-$(h-1)$-4.

Game 3-h-2 ($h = 1, \ldots, \nu_H$): Game 3-h-2 is the same as Game 3-h-1 except that the reply $\boldsymbol{k}_t^{(h)*} \in \mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$ to $\mathsf{AttrGen}$ query for the h-th global identity gid_h with $t \in \mathcal{T}_{\mathsf{good}}$ is:

$$\boldsymbol{k}_t^{(h)*} := (\overbrace{\vec{x}_t^{(h)}}^{n_t}, \overbrace{\delta^{(h)} \vec{x}_t^{(h)}}^{n_t}, \overbrace{0^2}^{2}, \overbrace{\boxed{\tau^{(h)} \vec{x}_t^{(h)} \cdot U_t}, 0^{n_t}}^{2n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*} \tag{17}$$

where $\tau^{(h)} \xleftarrow{\cup} \mathbb{F}_q$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$ used in Eq. (16), and the other variables are generated as in Game 3-h-1.

Game 3-h-3 ($h = 1, \ldots, \nu_H$) : Same as Game 3-h-2 except that (a part of) the verification text, $\boldsymbol{c}_i$, for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$ in the final step:

$$\left.\begin{array}{l}\text{for } i=1,\dots,\ell,\\ \text{If } \rho(i)=(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{good}},\\ \boldsymbol{c}_i:=(\overbrace{s_i\vec{e}_{t,1}+\theta_i\vec{v}_i}^{n_t},\overbrace{s_i'\vec{e}_{t,1}+\theta_i'\vec{v}_i}^{n_t},\overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\\ \overbrace{(\boxed{r_i''}\vec{e}_{t,1}+\omega_i\vec{v}_i)\cdot Z_t,\ r_i'\vec{e}_{t,1}+\omega_i'\vec{v}_i}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{if } \rho(i)=\neg(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{good}},\\ \boldsymbol{c}_i:=(\overbrace{s_i\vec{v}_i}^{n_t},\overbrace{s_i'\vec{v}_i}^{n_t},\overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\\ \overbrace{\boxed{r_i''}\vec{v}_i\cdot Z_t,r_i'\vec{v}_i}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\end{array}\right\}\quad(18)$$

where $\vec{g}\xleftarrow{\cup}\{\vec{g}\in\mathbb{F}_q^r\mid M_i\cdot\vec{g}^{\mathrm{T}}=0 \text{ for } \forall i \text{ s.t., } \widetilde{\rho}(i)\in\mathcal{T}_{\mathsf{bad}}\}$, $r_i'':=M_i\cdot\vec{g}^{\mathrm{T}}$, and the other variables are generated as in Game 3-h-2.

Game 3-h-4 ($h=1,\dots,\nu_H$) : Game 3-h-4 is the same as Game 3-h-3 except that the reply $\boldsymbol{k}_t^{(h)*}\in\mathsf{usk}_{\mathsf{gid}_h,(t,\vec{x}_t)}$ to $\mathsf{AttrGen}$ query for the h-th global identity gid_h with $t\in\mathcal{T}_{\mathsf{good}}$ is:

$$\boldsymbol{k}_t^{(h)*}=(\overbrace{\vec{x}_t^{(h)}}^{n_t},\overbrace{\delta^{(h)}\vec{x}_t^{(h)}}^{n_t},\overbrace{0^2}^{2},\overbrace{\boxed{0^{n_t},\tau'^{(h)}\vec{x}_t^{(h)}}}^{2n_t},\overbrace{\vec{\varphi}_t^{(h)}}^{n_t},\overbrace{0}^{1})_{\mathbb{B}_t^*}\quad(19)$$

where $\tau'^{(h)}\xleftarrow{\cup}\mathbb{F}_q$, and the other variables are generated as in Game 3-h-3.

Game 4: Game 4 is the same as Game 3-ν_H-4 except that a part of apk_t, $\{\widetilde{\boldsymbol{b}}_{t,\iota}^*\}_{\iota=1,\dots,n_t}$, for $t\in\mathcal{T}_{\mathsf{good}}$ is:

$$\widetilde{\boldsymbol{b}}_{t,\iota}^*:=(\overbrace{\pi\vec{e}_{t,\iota}}^{n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{0^2}^{2},\overbrace{0^{n_t},\boxed{\eta\vec{e}_{t,\iota}}}^{2n_t},\overbrace{\vec{\tilde{\varphi}}_{t,\iota}}^{n_t},\overbrace{0}^{1})_{\mathbb{B}_t^*},\quad(20)$$

where $\eta\xleftarrow{\cup}\mathbb{F}_q$, and the other variables are generated as in Game 3-ν_H-4.

Game 5 : Game 5 is the same as Game 4 except that (a part of) the verification text, $\{\boldsymbol{c}_i\}_{i=1,\dots,\ell}, c_{d+1}$, for $(m',\mathbb{S}')$ with $\mathbb{S}':=(M,\rho)$ in the final step is:

$$\left.\begin{array}{l}\text{for } i=1,\dots,\ell,\\ \text{If } \rho(i)=(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{good}},\\ \boldsymbol{c}_i:=(\overbrace{\boxed{\tilde{s}_i}\vec{e}_{t,1}+\theta_i\vec{v}_i}^{n_t},\overbrace{s_i'\vec{e}_{t,1}+\theta_i'\vec{v}_i}^{n_t},\overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\\ \overbrace{(r_i\vec{e}_{t,1}+\omega_i\vec{v}_i)\cdot Z_t,r_i'\vec{e}_{t,1}+\omega_i'\vec{v}_i}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{If } \rho(i)=(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{bad}},\\ \boldsymbol{c}_i:=(\overbrace{\tilde{s}_i\vec{e}_{t,1}+\theta_i\vec{v}_i}^{n_t},\overbrace{s_i'\vec{e}_{t,1}+\theta_i'\vec{v}_i}^{n_t},\\ \overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\overbrace{0^{2n_t}}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{If } \rho(i)=\neg(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{good}},\\ \boldsymbol{c}_i:=(\overbrace{\boxed{\tilde{s}_i}\vec{v}_i}^{n_t},\overbrace{s_i\vec{v}_i}^{n_t},\overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\\ \overbrace{r_i\vec{v}_i\cdot Z_t,r_i'\vec{v}_i}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ \text{If } \rho(i)=\neg(t,\vec{v}_i)\ \wedge\ t\in\mathcal{T}_{\mathsf{bad}},\\ \boldsymbol{c}_i:=(\overbrace{\tilde{s}_i\vec{v}_i}^{n_t},\overbrace{s_i\vec{v}_i}^{n_t},\overbrace{\theta_i''(H_2(m',\mathbb{S}'),-1)}^{2},\\ \overbrace{0^{2n_t}}^{2n_t},\overbrace{0^{n_t}}^{n_t},\overbrace{\eta_i}^{1})_{\mathbb{B}_t},\\ c_{d+1}:=g_T^{\boxed{s_0}},\end{array}\right\}\quad(21)$$

where $\vec{f}\xleftarrow{\cup}\mathbb{F}_q^r$, $\tilde{s}_i:=M_i\cdot\vec{f}^{\mathrm{T}}$ and $s_0\xleftarrow{\cup}\mathbb{F}_q$. The other variables are generated as in Game 4. Here, we note that s_0 is independent from all the other variables.

Let $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)$ be $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABS,UF}}(\lambda)$ in Game 0, and $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda),\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda),\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda),\dots,\ \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}4)}(\lambda)$, $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda),\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game 1, 2-h, 3-h-1, …, 3-h-4, 4, 5, respectively.

It is obtained that $\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)=1/q$ by Lemma 22. We will show eight lemmas (Lemmas 14–21) that evaluate the gaps between pairs of $\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda),\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda),\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)$ for $h=1,\dots,\nu_S$, $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda),\dots,\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}4)}(\lambda)$ for $h=1,\dots,\nu_H$, $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)$. From these lemmas and Lemmas 8, 9 and 12, we obtain $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABS,UF}}(\lambda)=\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)\le\left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right|+\sum_{h=1}^{\nu_S}\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)\right|+\sum_{h=1}^{\nu_H}\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1)\text{-}4)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda)\right|+\sum_{\iota=1}^{3}\sum_{h=1}^{\nu_H}\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}\iota)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}(\iota+1))}(\lambda)\right|+\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}\nu_H\text{-}4)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right|+\left|\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)\right|+\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)\le\mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda)+\sum_{h=1}^{\nu_S}\mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2}}(\lambda)+\sum_{h=1}^{\nu_H}\left(\mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}1}}^{\mathsf{P2}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}1}}^{\mathsf{P3}}(\lambda)\right)+\mathsf{Adv}_{\mathcal{B}_4}^{\mathsf{P2}}(\lambda)+((d+1)\nu_S+2d\nu_H+2d+1)/q\le\mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda)+\sum_{h=1}^{\nu_S}\mathsf{Adv}_{\mathcal{E}_{2\text{-}h}}^{\mathsf{DLIN}}(\lambda)+\sum_{h=1}^{\nu_H}\left(\mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda)+\mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda)\right)+\mathsf{Adv}_{\mathcal{E}_4}^{\mathsf{DLIN}}(\lambda)+((d+6)\nu_S+(2d+10)\nu_H+3d+11)/q$. This completes the proof of Theorem 3. □

6.6 Structure of Reductions for Theorem 3

In Fig. 1, an equality between neighboring games indicates

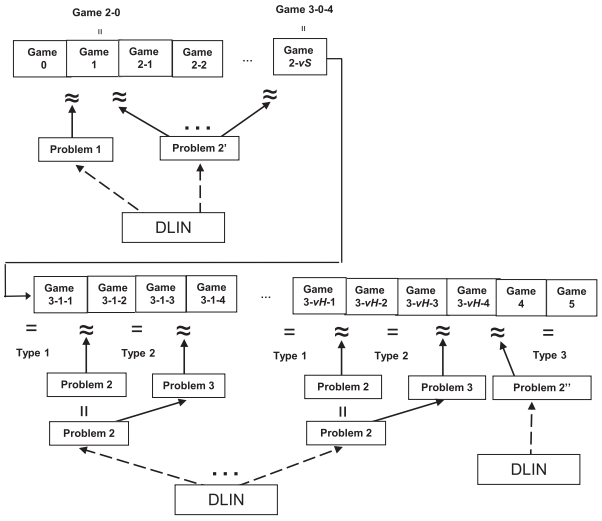


Fig. 1 Structure of reductions.

that the left-hand game can be conceptually (information-theoretically) changed to the right-hand game. An approximate equality between them indicates that the gap between them is upper-bounded by the advantage of the problem indicated. The information-theoretical changes have three types: Type 1 is a (conceptual) linear transformation inside a subspace for a verification text with preserving the secret key and signature coefficients on the subspace, Type 2 is a conceptual coefficients change from the adversary's view through the key query limitation in the security definition (Definition 11), and Type 3 is a (conceptual) linear transformation across subspaces. The DLIN Problem is defined in Definition 6, and Problems 1, 2, 2', 2", 3 are defined in Definitions 12, 13, 14, 15, 16, respectively.

One highlight in the game description is a combination of Type 2 conceptual change and computational one by Problem 3, i.e., the transition from Game 3-h-2 to 3-h-3, and to 3-h-4. The type 2 transformation changes a shared secret $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 = 0$ on the first block of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}_{t,2n_t+3}, \ldots, \boldsymbol{b}_{t,3n_t+2}\rangle$ to a *uniformly generated* shared secret $\{r_i\}_{i=1,\ldots,\ell}$ with $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, which is a *local* target of the h-th part of the Game 3 sequence. Problem 3 then swaps the result on the first block of the hidden part of the h-th gid's secret key to that on the second block of the hidden part, i.e., $\mathsf{span}\langle \boldsymbol{b}^*_{t,3n_t+3}, \ldots, \boldsymbol{b}^*_{t,4n_t+2}\rangle$. This change prepares the next $(h+1)$-st part of the Game 3 sequence, and at the same time, the h-th result remains in the h-th gid's secret key, which makes all queried secret keys semi-functional at the end of the Game 3 sequence i.e., a *global* coordination of the local results.

We have shown that the intractability of (complicated) Problems 1 and 2 (and 2', 2") is reduced to that of the DLIN Problem through several intermediate steps, or intermediate problems, in [27]. They are indicated in Fig. 1 by dotted arrows.

We show that the intractability of Problems 3 is reduced to that of Problem 2 in Lemmas 23 and 24. Problem 1 is used for evaluating the gap between advantages of adversary in Game 0 and 1 (Lemma 14). Problem 2 (resp. 2', 2") is used for evaluating the gap between advantages of adversary in Game 3-h-1 and 3-h-2 (resp. in Game 2-$(h-1)$ and 2-h, in Game 3-ν_H-4 and 4) in Lemma 17 (resp. Lemma 15, Lemma 20). Problem 3 is used for evaluating the gap of those in Game 3-h-3 and 3-h-4 (Lemma 19). They are indicated in Figure 1 by arrows. The rest of gaps between games are evaluated without computational assumptions (Lemmas 16, 18 and 21).

6.7 Lemmas for the Proof of Theorem 3

We will show fifteen lemmas for the proof of Theorem 3. The proofs of Lemmas 9 and 12 are given in Appendix B. Lemma 8 is proven similarly to Lemma 1 in [27], and Lemma 13 is proven in Appendix C in [27]. We describe random dual orthonormal bases generator $\mathcal{G}_{\mathsf{ob}}$ below, which is used as a subroutine in the following problems.

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n} := (d; n_1, \ldots, n_d)) : \\
&\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ \kappa, \xi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, \\
&\text{for } t = 1, \ldots, d, \quad N_t := 5n_t + 3, \\
&\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}), \\
&X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q),\ (\vartheta_{t,i,j})_{i,j} := (X_t^{\mathrm{T}})^{-1}, \\
&\boldsymbol{b}_{t,i} := \kappa(\chi_{t,i,1}, \ldots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \kappa \textstyle\sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}, \\
&\boldsymbol{b}^*_{t,i} := \xi(\vartheta_{t,i,1}, \ldots, \vartheta_{t,i,N_t})_{\mathbb{A}_t} = \xi \textstyle\sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}, \\
&\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),\ \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}), \\
&G_0 := \kappa G,\ \ G_1 := \xi G,\ \ g_T := e(G,G)^{\kappa\xi}, \\
&\mathsf{param}_{\vec{n}} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=1,\ldots,d}, g_T), \\
&\text{return } (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=1,\ldots,d}, G_0, G_1).
\end{aligned}
$$

We note that $g_T = e(\boldsymbol{b}_{t,i}, \boldsymbol{b}^*_{t,i})$ for $t = 1, \ldots, d; i = 1, \ldots, N_t$.

Definition 12 (Problem 1): Problem 1 is to guess β, given $(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,2n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \vec{n})$, where

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=1,\ldots,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n}), \\
&\widehat{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,1}, .., \boldsymbol{b}^*_{t,3n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, .., \boldsymbol{b}^*_{t,5n_t+3}) \ \text{ for } t = 1, .., d, \\
&\omega, \sigma, \gamma_t \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q) \ \text{ for } t = 1, .., d, \\
&\text{for } t = 1, \ldots, d; \\
&\boldsymbol{e}_{0,t,1} := (\overbrace{0^{n_t}}^{n_t}, \overbrace{\omega\vec{e}_{t,1}}^{n_t}, \overbrace{0^{n_t+2}}^{n_t+2}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\gamma_t}^{1})_{\mathbb{B}_t}, \\
&\boldsymbol{e}_{1,t,1} := (\ 0^{n_t}\ , \omega\vec{e}_{t,1}, \ 0^{n_t+2}, \ (\sigma\vec{e}_{t,1}) \cdot Z_t, \ 0^{n_t}, \ \gamma_t\ )_{\mathbb{B}_t}, \\
&\boldsymbol{e}_{t,i} := \omega \boldsymbol{b}_{t,i} \ \text{ for } i = 2, \ldots, n_t, \\
&\text{return } (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}, G_0, G_1),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic machine $\mathcal{B}$, we define the advantage of $\mathcal{B}$ as the quantity $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) := \left|\Pr\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, \vec{n})\right] -\right.$

$$\mathsf{Pr}\left[\mathcal{B}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P1}}(1^\lambda,\vec{n})\right].$$

Lemma 8: For any adversary $\mathcal{B}$, there exist probabilistic machines $\mathcal{E}$, whose running times are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P1}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + (d+5)/q$.

Lemma 8 is proven similarly to Lemma 1 in [27]. □

Definition 13 (Problem 2): Problem 2 is to guess β, given $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1, \delta G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda,\vec{n})$, where

$$\mathcal{G}_\beta^{\mathsf{P2}}(1^\lambda,\vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,..,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,\vec{n}),$$
$$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},..,\boldsymbol{b}_{t,2n_t+2},\boldsymbol{b}_{t,3n_t+3},..,\boldsymbol{b}_{t,5n_t+3}) \quad \text{for } t=1,..,d,$$
$$\delta,\tau,\omega,\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Z_t \xleftarrow{\mathsf{U}} GL(n_t,\mathbb{F}_q), U_t := (Z_t^{-1})^{\mathrm{T}} \text{ for } t=1,..,d,$$
$$\text{for } t=1,\ldots,d;\ i=1,\ldots,n_t; \quad \vec{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$
$$\boldsymbol{h}_{0,t,i}^* := (\overbrace{0^{n_t},\delta\vec{e}_{t,i},0^2}^{2n_t+2}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}$$
$$\boldsymbol{h}_{1,t,i}^* := (0^{n_t},\delta\vec{e}_{t,i},0^2,\ (\tau\vec{e}_{t,i})\cdot U_t,\ 0^{n_t},\ \vec{\delta}_{t,i},\ 0\ )_{\mathbb{B}_t^*}$$
$$\boldsymbol{e}_{t,i} := (0^{n_t},\omega\vec{e}_{t,i},0^2,\ (\sigma\vec{e}_{t,i})\cdot Z_t,\ 0^{n_t},\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},$$
$$\text{return } (\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1, \delta G_1),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda)$, is similarly defined as in Definition 12.

Lemma 9: For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

Lemma 9 is proven similarly to Lemma 2 in [27]. □

We use two variants of Problem 2, i.e., Problem 2' and 2", which have essentially same structure as that of Problem 2, as well as Problem 2. The security of the problems can be reduced to that of Problem 2.

Definition 14 (Problem 2'): Problem 2' is to guess β, given $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,2}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P2'}}(1^\lambda,\vec{n})$, where

$$\mathcal{G}_\beta^{\mathsf{P2'}}(1^\lambda,\vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,..,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,\vec{n}),$$
$$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},..,\boldsymbol{b}_{t,2n_t+2},\boldsymbol{b}_{t,3n_t+3},..,\boldsymbol{b}_{t,5n_t+3}) \quad \text{for } t=1,..,d,$$
$$\delta,\tau,\omega,\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Z_t \xleftarrow{\mathsf{U}} GL(n_t,\mathbb{F}_q), U_t := (Z_t^{-1})^{\mathrm{T}} \text{ for } t=1,..,d,$$
$$\text{for } t=1,\ldots,d;\ i=1,2;\ \vec{e}_1' := (\,1,\,0\,), \vec{e}_2' := (\,0,\,1\,) \in \mathbb{F}_q^2,$$
$$\vec{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$
$$\boldsymbol{h}_{0,t,i}^* := (\overbrace{0^{2n_t},\delta\vec{e}_i'}^{2n_t+2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}$$
$$\boldsymbol{h}_{1,t,i}^* := (0^{2n_t},\delta\vec{e}_i',\ 0^{n_t},(\tau\vec{e}_{t,i})\cdot U_t,\ \vec{\delta}_{t,i},\ 0\ )_{\mathbb{B}_t^*}$$
$$\boldsymbol{e}_{t,i} := (0^{2n_t},\omega\vec{e}_i',\ 0^{n_t},(\sigma\vec{e}_{t,i})\cdot Z_t,\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},$$
$$\text{return } (\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,2}, G_0, G_1),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2', $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2'}}(\lambda)$, is similarly defined as in Definition 12.

Lemma 10: For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2'}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

The proof of Lemma 10 can be reduced to that of Lemma 9. □

Definition 15 (Problem 2"): Problem 2" is to guess β, given $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P2''}}(1^\lambda,\vec{n})$, where

$$\mathcal{G}_\beta^{\mathsf{P2''}}(1^\lambda,\vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,..,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,\vec{n}),$$
$$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},..,\boldsymbol{b}_{t,2n_t+2},\boldsymbol{b}_{t,3n_t+3},..,\boldsymbol{b}_{t,5n_t+3}) \quad \text{for } t=1,..,d,$$
$$\delta,\tau,\omega,\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$
$$\text{for } t=1,\ldots,d;\ i=1,\ldots,n_t; \quad \vec{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$
$$\boldsymbol{h}_{0,t,i}^* := (\overbrace{\delta\vec{e}_{t,i}}^{n_t}, \overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}$$
$$\boldsymbol{h}_{1,t,i}^* := (\delta\vec{e}_{t,i},\ 0^{2n_t+2},\ \tau\vec{e}_{t,i},\ \vec{\delta}_{t,i},\ 0\ )_{\mathbb{B}_t^*}$$
$$\boldsymbol{e}_{t,i} := (\omega\vec{e}_{t,i},\ 0^{2n_t+2},\ \sigma\vec{e}_{t,i},\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},$$
$$\text{return } (\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1),$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2''}}(\lambda)$, is similarly defined as in Definition 12.

Lemma 11: For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P2''}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 5/q$.

The proof of Lemma 11 can be reduced to that of Lemma 9. □

Definition 16 (Problem 3): Problem 3 is to guess β, given $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i,\iota}\}_{t=1,..,d;i=1,..,n_t;\iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{P3}}(1^\lambda,\vec{n})$, where

$$\mathcal{G}_\beta^{\mathsf{P3}}(1^\lambda,\vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=1,..,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda,\vec{n}),$$
$$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},..,\boldsymbol{b}_{t,2n_t+2},\boldsymbol{b}_{t,4n_t+3},..,\boldsymbol{b}_{t,5n_t+3}) \quad \text{for } t=1,..,d,$$
$$\tau,\tau',\omega_\iota,\omega_\iota' \xleftarrow{\mathsf{U}} \mathbb{F}_q \quad \text{for } \iota=1,2,$$
$$Z_t \xleftarrow{\mathsf{U}} GL(n_t,\mathbb{F}_q), U_t := (Z_t^{-1})^{\mathrm{T}} \text{ for } t=1,..,d,$$
$$\text{for } t=1,\ldots,d;\ i=1,\ldots,n_t;\ \iota=1,2;\ \vec{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$
$$\boldsymbol{h}_{0,t,i}^* := (\overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{(\tau\vec{e}_{t,i})\cdot U_t,\ 0^{n_t}}^{2n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*}$$
$$\boldsymbol{h}_{1,t,i}^* := (0^{2n_t+2},\ 0^{n_t},\ \tau'\vec{e}_{t,i},\ \vec{\delta}_{t,i},\ 0\ )_{\mathbb{B}_t^*}$$
$$\boldsymbol{e}_{t,i,\iota} := (0^{2n_t+2},\ (\omega_\iota\vec{e}_{t,i})\cdot Z_t, \omega_\iota'\vec{e}_{t,i},\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},$$

Table 3 Comparison with the existing MA-ABS schemes.

	MPR10 [18] Instantiation 3	MPR10 [18] Instantiation 2	OT11 [19]	Proposed
Signature size (# of group elts)	$\ell + r + 2$	$36\ell + 2r + 9\lambda + 12$	$7\ell + 11$	13ℓ
Decentralized	×	×	×	✓
Model	generic group model	standard model	standard model	random oracle model
Security	full	full	full	full
Assumptions	CR hash	DLIN	DLIN and CR hash	DLIN
Predicates	monotone	monotone	non-monotone	non-monotone
Sig. size example 1 ($\ell = 10, r = 5, \lambda = 128$)	17	1534	81	130
Sig. size example 2 ($\ell = 100, r = 50, \lambda = 128$)	152	4864	711	1300

return $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i,t}\}_{t=1,..,d;i=1,..,n_t;t=1,2}, G_0, G_1)$,

for $\beta \xleftarrow{\cup} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 3, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 12.

Lemma 12: For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

Lemma 13 (Lemma 3 in [27]): For $p \in \mathbb{F}_q$, let $C_p := \{(\vec{x}, \vec{v}) | \vec{x} \cdot \vec{v} = p\} \subset V \times V^*$ where V is n-dimensional vector space $\mathbb{F}_q^n$, and V^* its dual. For all $(\vec{x}, \vec{v}) \in C_p$, for all $(\vec{r}, \vec{w}) \in C_p$, $\Pr[\vec{x}U = \vec{r} \wedge \vec{v}Z = \vec{w}] = \Pr[\vec{x}Z = \vec{r} \wedge \vec{v}U = \vec{w}] = 1/\sharp C_p$, where $Z \xleftarrow{\cup} GL(n, \mathbb{F}_q)$, $U := (Z^{-1})^{\mathrm{T}}$.

Lemma 14: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.

Lemma 15: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}'}_{\mathcal{B}_{2\text{-}h}}(\lambda) + 4/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.

Lemma 16: For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \le 2d/q$.

Lemma 17: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{3\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{3\text{-}h\text{-}1}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{3\text{-}1}(h, \cdot)$.

Lemma 18: For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(3\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(3\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda)$.

Lemma 19: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{3\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3\text{-}h\text{-}2}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{3\text{-}2}(h, \cdot)$.

Lemma 20: For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_4$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}\nu_H\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2}''}_{\mathcal{B}_4}(\lambda)$.

Lemma 21: For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)$.

Lemma 22: For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda) = 1/q$.

Proof. Since the value of s_0 in c_{d+1} is independent from all the other variables, the verification equation, $\prod_{i=1}^{\ell} e(\boldsymbol{c}_i, \boldsymbol{s}^*_i) = c_{d+1}$, holds with probability $1/q$ in Game 5. Hence, $\mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda) = 1/q$. □

The proofs of Lemma 12 and Lemmas 14–21 are given in Appendix B.

6.8 Performance (When $\vec{n} := (d; 2, \ldots, 2)$)

In this section, we compare the efficiency and security of the proposed DMA-ABS scheme with parameter $\vec{n} := (d; 2, \ldots, 2)$ to those of the existing MA-ABS schemes in the standard model (instantiation 2 in [18] and MA-ABS in [19]) as well as the ABS scheme in the generic group model (instantiation 3 in [18]) as a benchmark. Since all of these schemes can be implemented over a *prime order* pairing group, the size of a group element can be around the size of $\mathbb{F}_q$ (e.g., 256 bits). In Table 3, ℓ and r represent the size of the underlying access structure matrix M for a predicate, i.e., $M \in \mathbb{F}_q^{\ell \times r}$.

For example, some predicate with 4 AND and 5 OR gates as well as 10 variables may be expressed by a 10×5 matrix, and a predicate with 49 AND and 50 OR gates as well as 100 variables may be expressed by a 100×50 matrix (see the appendix of [26]). λ is the security parameter (e.g., 128).

References

[1] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," PKC 2013, K. Kurosawa and G. Hanaoka, eds., Lecture Notes in Computer Science, vol.7778, pp.125–142, Springer, 2013.
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," IEEE Symposium on Security and Privacy, pp.321–334, IEEE Computer Society, 2007.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Juels et al. [50], pp.89–98, 2006.
[4] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," ACM CCS 2007, P. Ning, S.D.C. di Vimercati, and P.F. Syverson, eds., pp.195–203, ACM, 2007.
[5] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in Juels et al. [50], pp.99–112, 2006.
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," EUROCRYPT 2005, R. Cramer, ed., LNCS, vol.3494, pp.457–473, Springer, 2005.
[7] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," EUROCRYPT 2004, C. Cachin and J. Camenisch, eds., LNCS, vol.3027, pp.223–238, Springer, 2004.
[8] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Franklin [49], pp.443–459, 2004.
[9] D. Boneh and M.K. Franklin, "Identity-based encryption from the Weil pairing," CRYPTO 2001, J. Kilian, ed., LNCS, vol.2139, pp.213–229, Springer, 2001.
[10] C. Cocks, "An identity based encryption scheme based on quadratic residues," IMA Int. Conf. 2001, B. Honary, ed., LNCS, vol.2260, pp.360–363, Springer, 2001.
[11] C. Gentry, "Practical identity-based encryption without random oracles," EUROCRYPT 2006, S. Vaudenay, ed., LNCS, vol.4004, pp.445–464, Springer, 2006.
[12] S. Guo and Y. Zeng, "Attribute-based signature scheme," ISA, pp.509–511, IEEE, 2008.
[13] D. Khader, "Attribute based group signatures," IACR Cryptology ePrint Archive, vol.2007, p.159, 2007.
[14] D. Khader, "Attribute based group signature with revocation," IACR Cryptology ePrint Archive, vol.2007, p.241, 2007.
[15] J. Li, M.H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," ASIACCS, D. Feng, D.A. Basin, and P. Liu, eds., pp.60–69, ACM, 2010.
[16] J. Li and K. Kim, "Attribute-based ring signatures," IACR Cryptology ePrint Archive, vol.2008, p.394, 2008.
[17] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, vol.2008, p.328, 2008.
[18] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," CT-RSA, A. Kiayias, ed., Lecture Notes in Computer Science, vol.6558, pp.376–392, Springer, 2011.
[19] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds., LNCS, vol.6571, pp.35–52, Springer, 2011. This is an extended abstract of a preliminary version of [47].
[20] S.F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," AFRICACRYPT, B. Preneel, eds., Lecture Notes in Computer Science, vol.5580, pp.198–216, Springer, 2009.
[21] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature," IACR Cryptology ePrint Archive, vol.2008, p.2, 2008.
[22] M. Chase, "Multi-authority attribute based encryption," TCC, S.P. Vadhan, ed., LNCS, vol.4392, pp.515–534, Springer, 2007.
[23] M. Chase and S.S.M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp.121–130, ACM, 2009.
[24] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol.180, no.13, pp.2618–2632, 2010.
[25] S. Mueller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Fraunhofer SIT, vol.46, 07 2009.
[26] A.B. Lewko and B. Waters, "Decentralizing attribute-based encryption," EUROCRYPT 2011, K.G. Paterson, ed., LNCS, vol.6632, pp.568–588, Springer, 2011.
[27] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," CRYPTO 2010, T. Rabin, ed., LNCS, vol.6223, pp.191–208, Springer, 2010. The full version is available as an online first article in Journal of Cryptology.
[28] ISO/IEC 15946-5, "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation," ISO/IEC, 2009.
[29] FIPS PUB 180-1, 180-2, "Secure hash standard," NIST, 1995, 2002.
[30] N. Estibals, "Compact hardware for computing the tate pairing over 128-bit-security supersingular curves," Pairing, M. Joye, A. Miyaji, and A. Otsuka, eds., Lecture Notes in Computer Science, vol.6487, pp.397–416, Springer, 2010.
[31] R.L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," ASIACRYPT, C. Boyd, ed., Lecture Notes in Computer Science, vol.2248, pp.552–565, Springer, 2001.
[32] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," Public Key Cryptography, T. Okamoto and X. Wang, eds., Lecture Notes in Computer Science, vol.4450, pp.166–180, Springer, 2007.
[33] T. Okamoto and K. Takashima, "Dual pairing vector spaces and their applications," IEICE Trans. Fundamentals, vol.E98-A, no.1, pp.3–15, Jan. 2015.
[34] A.B. Lewko, Functional Encryption: New Proof Techniques and Advancing Capabilities, Ph.D. thesis, The University of Texas at Austin, 2012.
[35] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," Financial Cryptography and Data Security - 19th International Conference, FC 2015, Revised Selected Papers, pp.315–332, San Juan, Puerto Rico, Jan. 2015.
[36] X. Boyen, "Mesh signatures," EUROCRYPT, M. Naor, ed., Lecture Notes in Computer Science, vol.4515, pp.210–227, Springer, 2007.
[37] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in Halevi [48], pp.108–125, 2009.
[38] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," TCC, R. Canetti, ed., Lecture Notes in Computer Science, vol.4948, pp.356–374, Springer, 2008.
[39] J. Camenisch and T. Groß, "Efficient attributes for anonymous credentials," ACM Conference on Computer and Communications Security, P. Ning, P.F. Syverson, and S. Jha, eds., pp.345–356, ACM, 2008.
[40] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," EUROCRYPT, B. Pfitzmann, ed., Lecture Notes in Computer Science, vol.2045, pp.93–118, Springer, 2001.
[41] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in Franklin [49], pp.56–72, 2004.
[42] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," Commun. ACM, vol.28, no.10, pp.1030–1044, 1985.
[43] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," ASIACRYPT 2009, M. Matsui, ed., LNCS, vol.5912, pp.214–231, Springer, 2009.
[44] A. Beimel, Secure Schemes for Secret Sharing and Key Distribution, Ph.D. thesis, Israel Institute of Technology, Technion, Haifa, 1996.
[45] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Franklin [49], pp.41–55, 2004.
[46] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in Halevi [48], pp.619–636, 2009.
[47] T. Okamoto and K. Takashima, "Efficient attribute-based signatures

for non-monotone predicates in the standard model," IEEE Trans. Cloud Comput., vol.2, no.4, pp.409–421, 2014. Full version is available at http://eprint.iacr.org/2011/700.
[48] S. Halevi, ed., Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Proceedings, LNCS, vol.5677, Springer, Santa Barbara, CA, USA, Aug. 2009.
[49] M.K. Franklin, ed., Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Proceedings, LNCS, vol.3152, Springer, Santa Barbara, California, USA, Aug. 2004.
[50] A. Juels, R.N. Wright, and S.D.C. di Vimercati, eds., Proc. 13th ACM Conference on Computer and Communications Security, CCS 2006, ACM, Alexandria, VA, USA, Oct.–Nov. 2006.

Appendix A: Security of MA-ABS Schemes When Central Authority Is Corrupted

Three MA-ABS schemes, which are based on single-authority ABS schemes, Schemes 1, 2 and 3, have been presented in Appendix F.1 of [18]. Here, we call them Schemes 1-MA, 2-MA and 3-MA. In this appendix, we will show that the three MA-ABS schemes are totally broken if the central authority (called "the signature trustee" in [18]) is corrupted.

In Schemes 1-MA and 2-MA, the role of the central authority is to issue its own signature verification key (public key) and a CRS for the NIWI protocol. Their attribute-based signature scheme is based on the OR-proof on attribute authorities' signatures for attributes or the central authority's signature for pseudo-attributes. Therefore, if the central authority is corrupted, or an attacker can get the signing key (secret key) of the central authority, then the attacker can forge a signature for any policy and message, as the simulator for the security proof can do.

In Scheme 3-MA, the role of the central authority is to issue a public key including (A_0, h_0) and signature verification key $TVer$, where a_0 with $A_0 = h_0^{a_0}$ is a secret key of the central authority, and to issue user uid a token $\tau := (\mathsf{uid}, K_{\mathsf{base}}, K_0, \rho)$, where ρ is the authority's signature on $\mathsf{uid}||K_{\mathsf{base}}$ that is verified by $TVer$.

In the last paragraph of Appendix F.1, a modification based on the random oracle model (ROM) is described such that K_{base} can be a hash value of uid, i.e., $K_{\mathsf{base}} := R(\mathsf{uid})$ for some hash function R or the random oracle. By this modification, the token can be simper under ROM such that $\tau := (\mathsf{uid}, K_0)$. Note that, however, even in this modification, the central authority still has a secret key a_0, and the secret key plays an essential role for the security.

If the central authority is corrupted, or an attacker can get the secret key, a_0, then for any policy Υ and message m, the attacker can compute $S_i := (Cg^{\mu})^{r_i}$ $(\forall i \in [\ell])$, $Y := (Cg^{\mu})^{w}$ $(w \xleftarrow{\mathsf{U}} \mathbb{Z}_p)$, $P_1 := h_1^{-w} \cdot \prod_{i=1}^{\ell} (A_1 B_1^{u(i)})^{\mathbf{M}_{i1} \cdot r_i}$, $W := Y^{1/a_0}$, and P_j for $j = 2, \ldots, t$ are the same as the original ones. Here, all the notations follow those in the description of ABS.Sign in page 12 of [18]. The obtained (forged) signature, $\sigma := (Y, W, S_1, \ldots, S_\ell, P_1, \ldots, P_t)$, for (Υ, m) is verified validly. That is, by getting the secret key of the central authority, the attacker can forge a signature for any policy and message (even using ROM additionally).

Appendix B: Proofs of Lemmas 12 and 14–21

B.1 Proof of Lemma 12

Lemma 12. *For any adversary $\mathcal{B}$, there exists a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Problem 3 is the hybrid of the following Experiment 3-0, 3-1 and 3-2, i.e., $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{3\text{-}0}_{\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 23, 24 and 9, there exist probabilistic machines C and $\mathcal{E}$, whose running time are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{3\text{-}0}_{\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right| \\
&\le \left|\Pr\left[\mathsf{Exp}^{3\text{-}0}_{\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}(\lambda) \to 1\right]\right| \\
&\quad + \left|\Pr\left[\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}(\lambda) \to 1\right] - \Pr\left[\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right| \\
&\le \mathsf{Adv}^{\mathsf{P2}}_{C}(\lambda) \le \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q.
\end{aligned}$$

This completes the proof of Lemma 12. □

Definition 17 (Experiment 3-α ($\alpha = 0, 1, 2$)): We define Exp-3-α instance generator, $\mathcal{G}^{\mathsf{Exp\text{-}3}}_{\alpha}(1^\lambda, \vec{n})$, where

$$\begin{aligned}
&\mathcal{G}^{\mathsf{Exp\text{-}3}}_{\alpha}(1^\lambda, \vec{n}) : (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=1,\ldots,d}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n}), \\
&\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,4n_t+3}, .., \boldsymbol{b}_{t,5n_t+3}) \text{ for } t = 1, .., d, \\
&\tau, \tau', \omega_\iota, \omega'_\iota \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } \iota = 1, 2, \\
&Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q),\ U_t := (Z_t^{-1})^{\mathrm{T}} \text{ for } t = 1, \ldots, d, \\
&\text{for } t = 1, \ldots, d; i = 1, \ldots, n_t; \iota = 1, 2; \quad \vec{\delta}_{t,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}, \\
&\boldsymbol{h}^*_{0,t,i} := (\overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\tau\vec{e}_{t,i} \cdot U_t,\ 0^{n_t}}^{2n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t} \\
&\boldsymbol{h}^*_{1,t,i} := (0^{2n_t+2}, \tau\vec{e}_{t,i} \cdot U_t, \tau'\vec{e}_{t,i}, \vec{\delta}_{t,i}, 0)_{\mathbb{B}^*_t} \\
&\boldsymbol{h}^*_{2,t,i} := (0^{2n_t+2}, 0^{n_t}, \tau'\vec{e}_{t,i}, \vec{\delta}_{t,i}, 0)_{\mathbb{B}^*_t} \\
&\boldsymbol{e}_{t,i,\iota} := (0^{2n_t+2}, \omega_\iota\vec{e}_{t,i} \cdot Z_t, \omega'_\iota\vec{e}_{t,i}, 0^{n_t}, 0)_{\mathbb{B}_t}, \\
&\text{return } (\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t, \{\boldsymbol{h}^*_{\alpha,t,i}, \boldsymbol{e}_{t,i,\iota}\}_{t=1,\ldots,d;i=1,\ldots,n_t;\iota=1,2}, \\
&\qquad G_0, G_1).
\end{aligned}$$

For a probabilistic adversary $\mathcal{B}$, we define 3 experiments $\mathsf{Exp}^{3\text{-}\alpha}_{\mathcal{B}}$ ($\alpha = 0, 1, 2$) as follows:

1. $\mathcal{B}$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{Exp\text{-}3}}_{\alpha}(1^\lambda, \vec{n})$.
2. Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{B}(1^\lambda, \varrho)$.

Lemma 23: For any adversary $\mathcal{B}$, for any security parameter λ, $\Pr\left[\mathsf{Exp}^{3\text{-}0}_{\mathcal{B}}(\lambda) \to 1\right] = \Pr\left[\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}(\lambda) \to 1\right]$.

Proof. Let $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$. If we set, for $i = 1, \ldots, n_t$,

$$\begin{aligned}
\boldsymbol{d}_{t,3n_t+2+i} &:= (0^{2n_t+2}, -\theta\vec{e}_{t,i} \cdot Z_t, \vec{e}_{t,i}, 0^{n_t+1})_{\mathbb{B}_t}, \\
\boldsymbol{d}^*_{t,2n_t+2+i} &:= (0^{2n_t+2}, \vec{e}_{t,i}, \theta\vec{e}_{t,i} \cdot Z_t, 0^{n_t+1})_{\mathbb{B}^*_t}.
\end{aligned}$$

Then, $\mathbb{D}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,3n_t+2}, \boldsymbol{d}_{t,3n_t+3}, \ldots, \boldsymbol{d}_{4n_t+2}, \boldsymbol{b}_{4n_t+3}, \ldots, \boldsymbol{b}_{5n_t+3})$ and $\mathbb{D}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{d}^*_{t,2n_t+3}, \ldots, \boldsymbol{d}^*_{t,3n_t+2}, \boldsymbol{b}^*_{t,3n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+3})$ are dual orthonormal bases. Moreover, $(\mathbb{D}_t, \mathbb{D}^*_t)$ are consistent with $\widehat{\mathbb{B}}_t$. Then,

$$\begin{aligned}
\boldsymbol{h}^*_{0,t,i} :=& (\overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\tau\vec{\boldsymbol{e}}_{t,i}\cdot U_t,\ 0^{n_t}}^{2n_t}, \overbrace{\delta_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t}\\
=& (0^{2n_t+2}, \tau\vec{\boldsymbol{e}}_{t,i}\cdot U_t, \tau'\vec{\boldsymbol{e}}_{t,i}, \delta_{t,i}, 0)_{\mathbb{D}^*_t}\\
\boldsymbol{e}_{t,i,\iota} :=& (0^{2n_t+2}, \omega_\iota\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, \omega'_\iota\vec{\boldsymbol{e}}_{t,i}, 0^{n_t}, 0)_{\mathbb{B}_t},\\
=& (0^{2n_t+2}, \widetilde{\omega}_\iota\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, \omega'_\iota\vec{\boldsymbol{e}}_{t,i}, 0^{n_t}, 0)_{\mathbb{D}_t},
\end{aligned}$$

where $\tau' := -\theta\tau$ and $\widetilde{\omega}_\iota := \omega_\iota + \theta\omega'_\iota$, which are independently and uniformly distributed since $\theta, \omega_\iota \xleftarrow{\cup} \mathbb{F}_q$. That is, the joint distribution for Exp-3-0 and that for Exp-3-1 are equivalent. □

Lemma 24: For any adversary $\mathcal{B}$, there is a probabilistic machine C, whose running time is essentially the same as that of $\mathcal{B}$, for any security parameter λ, $\left|\mathsf{Pr}\left[\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right| = \mathsf{Adv}^{\mathsf{P2}}_{C}(\lambda)$.

Proof. In order to prove Lemma 24, we construct a probabilistic machine C against Problem 2 using a machine $\mathcal{B}$ distinguishing the experiment $\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}$ from $\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}$ as a black box as follows: C is given a Problem 2 instance, $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n}, G_0, G_1, \delta G_1)$. C sets, for $i = 1, \ldots, n_t$,

$$\begin{aligned}
&\boldsymbol{e}_{t,i,1} := \boldsymbol{e}_{t,i},\ \boldsymbol{e}_{t,i,2} := \eta_1\boldsymbol{b}_{t,n_t+i} + \eta_2\boldsymbol{e}_{t,i} \text{ where } \eta_1, \eta_2 \xleftarrow{\cup} \mathbb{F}_q,\\
&\mathbb{D}_t := (\boldsymbol{d}_{t,i})_{i=1,\ldots,5n_t+3} := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+3}, \ldots, \boldsymbol{b}_{t,4n_t+2},\\
&\quad \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,3n_t+2}, \boldsymbol{b}_{t,n_t+1}, \ldots, \boldsymbol{b}_{t,2n_t}, \boldsymbol{b}_{t,4n_t+3}, \ldots, \boldsymbol{b}_{t,5n_t+3}),\\
&\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,i})_{i=1,\ldots,5n_t+3} := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,3n_t+3}, \ldots, \boldsymbol{b}^*_{t,4n_t+2},\\
&\quad \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,3n_t+2}, \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,2n_t}, \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+3}),\\
&\widehat{\mathbb{D}}_t := (\boldsymbol{d}_{t,1}, \ldots, \boldsymbol{d}_{t,2n_t+2}, \boldsymbol{d}_{t,4n_t+3}, \ldots, \boldsymbol{d}_{t,5n_t+3})\\
&\quad = (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,3n_t+3}, \ldots, \boldsymbol{b}_{t,4n_t+2}, \boldsymbol{b}_{t,2n_t+1}, \boldsymbol{b}_{t,2n_t+2},\\
&\qquad \boldsymbol{b}_{t,4n_t+3}, \ldots, \boldsymbol{b}_{t,5n_t+3}),
\end{aligned}$$

where C can calculate $\widehat{\mathbb{D}}_t$ and $\mathbb{D}^*$ from a part of the Problem 2 instance, i.e., $(\widehat{\mathbb{B}}_t, \mathbb{B}^*_t)$, while C cannot calculate a part of basis $\mathbb{D}_t$, i.e., $(\boldsymbol{d}_{t,2n_t+3}, \ldots, \boldsymbol{d}_{t,3n_t+2})$, from the Problem 2 instance. C gives $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{D}}_t, \mathbb{D}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i,\iota}\}_{t=1,\ldots,d;i=1,\ldots,n_t;\iota=1,2}, G_0, G_1)$ to $\mathcal{B}$, and receives $\beta' \in \{0, 1\}$. C then outputs $1 - \beta'$.

Then,

$$\begin{aligned}
\boldsymbol{h}^*_{0,t,i} :=& (\overbrace{0^{n_t}, \delta\vec{\boldsymbol{e}}_{t,i}, 0^2}^{2n_t+2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\delta}_{t,i}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t}\\
=& (0^{2n_t+2}, 0^{n_t}, \delta\vec{\boldsymbol{e}}_{t,i}, \vec{\delta}_{t,i}, 0)_{\mathbb{D}^*_t},\\
\boldsymbol{h}^*_{1,t,i} :=& (0^{n_t}, \delta\vec{\boldsymbol{e}}_{t,i}, 0^2, \tau\vec{\boldsymbol{e}}_{t,i}\cdot U_t, 0^{n_t}, \vec{\delta}_{t,i}, 0)_{\mathbb{B}^*_t}\\
=& (0^{2n_t+2}, \tau\vec{\boldsymbol{e}}_{t,i}\cdot U_t, \delta\vec{\boldsymbol{e}}_{t,i}, \vec{\delta}_{t,i}, 0)_{\mathbb{D}^*_t},\\
\boldsymbol{e}_{t,i,1} :=& (0^{n_t}, \omega\vec{\boldsymbol{e}}_{t,i}, 0^2, \sigma\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, 0^{n_t}, 0^{n_t}, 0)_{\mathbb{B}_t}\\
=& (0^{2n_t+2}, \sigma\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, \omega\vec{\boldsymbol{e}}_{t,i}, 0^{n_t}, 0)_{\mathbb{D}_t},
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{e}_{t,i,2} :=& (\overbrace{0^{n_t}, (\eta_1+\eta_2\omega)\vec{\boldsymbol{e}}_{t,i}, 0^2}^{2n_t+2}, \overbrace{\eta_2\sigma\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, 0^{n_t}}^{2n_t}, \overbrace{0^{n_t+1}}^{n_t+1})_{\mathbb{B}_t}\\
=& (\overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\eta_2\sigma\vec{\boldsymbol{e}}_{t,i}\cdot Z_t, (\eta_1+\eta_2\omega)\vec{\boldsymbol{e}}_{t,i}}^{2n_t}, \overbrace{0^{n_t+1}}^{n_t+1})_{\mathbb{D}_t},
\end{aligned}$$

where $\delta, \tau, \omega, \sigma, \eta_1 + \eta_2\omega$ and $\eta_2\sigma$ are independently and uniformly distributed in $\mathbb{F}_q$ (except with negligible probability) since $\delta, \tau, \omega, \sigma, \eta_1, \eta_2 \xleftarrow{\cup} \mathbb{F}_q$. That is, the above $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{D}}_t, \mathbb{D}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i,\iota}\}_{t=1,\ldots,d;i=1,\ldots,n_t;\iota=1,2}, G_0, G_1)$ has the same distribution as the output of the generator $\mathcal{G}^{\mathsf{Exp\text{-}3}}_1(1^\lambda, \vec{n})$ (resp. $\mathcal{G}^{\mathsf{Exp\text{-}3}}_2(1^\lambda, \vec{n})$) when $\beta = 1$ (resp. $\beta = 0$). This completes the proof of Lemma 24. □

B.2 Proof of Lemma 14

Lemma 14. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.*

Proof. In order to prove Lemma 14, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1 by using any adversary $\mathcal{A}$ in a security game (Game 0 or 1) as a black box as follows:

1. $\mathcal{B}_1$ is given Problem 1 instance $(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=2,\ldots,n_t}, G_0, G_1)$.
2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, for each authority $t \in \mathcal{T}_{\mathsf{good}}$, $\mathcal{B}_1$ sets

$$\begin{aligned}
&\mathbb{D}_t := (\boldsymbol{d}_{t,j})_{j=1,\ldots,5n_t+3} := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,n_t+2}, \ldots,\\
&\quad \boldsymbol{b}_{t,2n_t}, \boldsymbol{b}_{t,n_t+1}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,5n_t+3}),\\
&\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,j})_{j=1,\ldots,5n_t+3} := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+2}, \ldots,\\
&\quad \boldsymbol{b}^*_{t,2n_t}, \boldsymbol{b}^*_{t,n_t+1}, \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,5n_t+3}),\\
&\widehat{\mathbb{D}}_t := (\boldsymbol{d}_{t,1}, \ldots, \boldsymbol{d}_{t,2n_t+2}, \boldsymbol{d}_{t,5n_t+3}),\\
&\widehat{\mathbb{D}}^*_t := (\widetilde{\boldsymbol{d}}^*_{t,1}, \ldots, \widetilde{\boldsymbol{d}}^*_{t,n_t}, \boldsymbol{d}^*_{t,n_t+1}, \ldots, \boldsymbol{d}^*_{t,2n_t+2},\\
&\quad \boldsymbol{d}^*_{t,4n_t+3}, \ldots, \boldsymbol{d}^*_{t,5n_t+2}),
\end{aligned}$$

where $\pi \xleftarrow{\cup} \mathbb{F}_q$, $\boldsymbol{r}_{t,\iota} \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2}\rangle$, $\widetilde{\boldsymbol{d}}^*_{t,\iota} := \pi\boldsymbol{d}^*_{t,\iota} + \boldsymbol{r}_{t,\iota}$ for $\iota = 1, \ldots, n_t$. $\mathcal{B}_1$ does not actually calculate $\mathbb{D}^*_t$ since $\boldsymbol{b}^*_{t,3n_t+3}, \ldots, \boldsymbol{b}^*_{t,4n_t+2}$ are not available in the Problem 1 instance, but obtains $\widehat{\mathbb{D}}_t$ and $\widehat{\mathbb{D}}^*_t$ from $\mathbb{B}_t$ and $\widehat{\mathbb{B}}^*_t$ in the instance. $\mathcal{B}_1$ sets $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H_1, H_2)$ using $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e)$ underlying $\mathsf{param}_{\vec{n}}$, and G_0, G_1, g_T contained in the Problem 1 instance, where H_1, H_2 is modeled as random oracles. $\mathcal{B}_1$ then returns gparam and $\{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{D}}_t, \widehat{\mathbb{D}}^*_t)\}_{t\in\mathcal{T}_{\mathsf{good}}}$ to $\mathcal{A}$. $\mathcal{B}_1$ prepares a list (H-list) for answers of the random oracle queries, which has data $(0^\lambda, \perp, G_0)$ and $((0^{\lambda-1}, 1), \perp, G_1)$ at the beginning.
4. When a random oracle query for H_1 is issued for a global identity gid, if gid is not queried before, then a fresh $\delta_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q$ is generated and $\mathcal{B}_1$ answers $\delta_{\mathsf{gid}}G_1$ and records data $(\mathsf{gid}, \delta_{\mathsf{gid}}, \delta_{\mathsf{gid}}G_1)$ to the H list. Otherwise, $\mathcal{B}_1$ obtains $\delta_{\mathsf{gid}}G_1$ from the H-list, and answers it to $\mathcal{A}$.

5. When an AttrGen query is issued for a pair of a global identity and an attribute $(\mathsf{gid}, (t, \vec{x}_t))$ for $t \in \mathcal{T}_{\mathsf{good}}$, $\mathcal{B}_1$ first asks a random oracle H_1 query for gid, then obtains the scalar δ_{gid} from the H-list. $\mathcal{B}_1$ calculates

$$\boldsymbol{k}_t^* = (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta_{\mathsf{gid}}\vec{x}_t}^{n_t}, \overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\vec{\varphi}_{\mathsf{gid},t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{D}_t^*}, \qquad (\mathrm{A}\cdot 1)$$

using $\vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ and $\widehat{\mathbb{D}}_t^*$. $\mathcal{B}_1$ answers $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}_t^*)$ to $\mathcal{A}$.

6. When a Sig query, $(\mathsf{gid}, m, \mathbb{S} := (M, \rho), \Gamma, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{t\in\mathcal{T}_{\mathsf{bad}} \wedge (t,\vec{x}_t)\in\Gamma})$, is issued by $\mathcal{A}$, $\mathcal{B}_1$ generates $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ for $t \in \mathcal{T}_{\mathsf{good}} \wedge (t, \vec{x}_t) \in \Gamma$ as in Eq. (A·1). Then, $\mathcal{B}_1$ answers $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}, m, \mathbb{S})$ to $\mathcal{A}$.
7. When $\mathcal{B}_1$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ and $\{\mathsf{apt}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$ from $\mathcal{A}$ (where $\mathbb{S}' := (M, \rho)$), $\mathcal{B}_1$ calculates the verification text $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ as follows: for $i = 1, \ldots, \ell$,

$$\begin{aligned}
&\boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} c_{i,j}\boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t-1} c_{i,n_t+j}\boldsymbol{e}_{t,j+1} + c_{i,2n_t}\boldsymbol{e}_{\beta,t,1} \\
&\quad + \textstyle\sum_{j=1}^{2} c_{i,2n_t+j}\boldsymbol{b}_{t,2n_t+j} \text{ if } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{good}}, \\
&\boldsymbol{c}_i := \textstyle\sum_{j=1}^{2n_t+2} c_{i,j}\boldsymbol{b}_{t,j} + \eta_i\boldsymbol{b}_{t,5n_t+3} \quad \text{if } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}, \\
&c_{d+1} := g_T^{s_0},
\end{aligned}$$

where $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1}\cdot\vec{f}^{\mathrm{T}}$, $\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ s.t. $\vec{1}\cdot\vec{f}'^{\mathrm{T}} = 0$, $\vec{s}'^{\mathrm{T}} := (s'_1, \ldots, s'_\ell)^{\mathrm{T}} := M\cdot\vec{f}'^{\mathrm{T}}$, $\theta_i, \theta'_i, \theta''_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, and if $\rho(i) = (t, \vec{v}_i)$, then $\vec{c}_i := (s_i\vec{e}_{t,1} + \theta_i\vec{v}_i, s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i, \theta''_i(H_2(m, \mathbb{S}), -1))$, if $\rho(i) = \neg(t, \vec{v}_i)$, then $\vec{c}_i := (s_i\vec{v}_i, s'_i\vec{v}_i, \theta''_i(H_2(m, \mathbb{S}), -1))$ for $i = 1, \ldots, \ell$, and $\boldsymbol{e}_{\beta,t,1}, \{\boldsymbol{e}_{t,j}\}_{j=2,\ldots,n_t}$ are from the Problem 1 instance, $\{\mathbb{B}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$ from $\{\mathsf{apt}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$. $\mathcal{B}_1$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ using Ver with the above $(\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1})$, and outputs $\beta' := 1$, if the verification succeeds, $\beta' := 0$ otherwise.

When $\beta = 0$, it is straightforward that the distribution by $\mathcal{B}_1$'s simulation is equivalent to that in Game 0. When $\beta = 1$, the distribution by $\mathcal{B}_1$'s simulation is equivalent to that in Game 1 except for the case that there exists an $i \in \{1, \ldots, \ell\}$ such that $c_{i,2n_t} = v_{i,n_t}\theta'_i = 0$, or there exists an $t \in \{1, \ldots, d\}$ such that $(z_{t,1}, \ldots, z_{t,3n_t}) = \vec{0}$, i.e., except with probability $(\ell + d)/q \le 2d/q$ since $\ell \le d$. □

B.3 Proof of Lemma 15

Lemma 15. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_2$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2}'}(\lambda) + (d+1)/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Proof. In order to prove Lemma 15, we construct a probabilistic machine $\mathcal{B}_2$ against Problem 2' by using an adversary $\mathcal{A}$ in a security game (Game 2-$(h-1)$ or 2-h) as a black box as follows:

1. $\mathcal{B}_2$ is given an integer h and a Problem 2' instance, $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,2}, G_0, G_1)$.
2. $\mathcal{B}_2$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_2$ provides $\mathcal{A}$ public keys gparam as in the proof of Lemma 14 and $\{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}'_t, \widehat{\mathbb{B}}_t^*)\}_{t=S}$ of Game 2-$(h-1)$ (and 2-h), where $\pi \xleftarrow{\mathsf{U}} \mathbb{F}_q, \widetilde{\boldsymbol{b}}_{t,\iota}^* := \pi\boldsymbol{b}_{t,\iota}^* + \boldsymbol{r}_{t,\iota}^*$ with $\boldsymbol{r}_{t,\iota}^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle\boldsymbol{b}_{t,4n_t+3}^*, \ldots, \boldsymbol{b}_{t,5n_t+2}^*\rangle$, $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,5n_t+3})$ and $\widehat{\mathbb{B}}_t^* := (\widetilde{\boldsymbol{b}}_{t,1}^*, \ldots, \widetilde{\boldsymbol{b}}_{t,n_t}^*, \boldsymbol{b}_{t,n_t+1}^*, \ldots, \boldsymbol{b}_{t,2n_t+2}^*, \boldsymbol{b}_{t,4n_t+3}^*, \ldots, \boldsymbol{b}_{t,5n_t+2}^*)$ for each authority $t \in \mathcal{T}_{\mathsf{good}}$, that are obtained from the Problem 2' instance. The H-list is initialized as in the proof of Lemma 14.
4. When a random oracle query for H_1 is issued for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$, $\mathcal{B}_2$ answers as follows: When gid is not queried before, then a fresh $\delta_{\mathsf{gid}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ is generated and $\mathcal{B}_2$ answers $\delta_{\mathsf{gid}}G_1$ to $\mathcal{A}$ and records data $(\mathsf{gid}, \delta_{\mathsf{gid}}, \delta_{\mathsf{gid}}G_1)$ to the H list. When gid is already queried, $\mathcal{B}_{3\text{-}1}$ obtains $\delta_{\mathsf{gid}}G_1$ from the H-list, and answers it to $\mathcal{A}$.
5. When an AttrGen query for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$ is issued for a pair of a global identity and an attribute $(\mathsf{gid}, (t, \vec{x}_t))$ for $t \in \mathcal{T}_{\mathsf{good}}$, $\mathcal{B}_2$ calculates normal key $\boldsymbol{k}_t^*$ with Eq. (10), that is computed using $\mathbb{B}_t^*$ of the Problem 2 instance and δ_{gid} as

$$\boldsymbol{k}_t^* := (\overbrace{\vec{x}_t}^{n_t}, \overbrace{\delta_{\mathsf{gid}}\vec{x}_t}^{n_t}, \overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\vec{\varphi}_{\mathsf{gid},t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_t^*},$$

where $\vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$.
6. When a Sig query, $(\mathsf{gid}, m, \mathbb{S} := (M, \rho), \Gamma, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{t\in\mathcal{T}_{\mathsf{bad}} \wedge (t,\vec{x}_t)\in\Gamma})$, is issued by $\mathcal{A}$, $\mathcal{B}_{3\text{-}1}$ generates $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ for $t \in \mathcal{T}_{\mathsf{good}} \wedge (t, \vec{x}_t) \in \Gamma$ as in Eq. (A·1). Then, $\mathcal{B}_{3\text{-}1}$ answers $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}, m, \mathbb{S})$ to $\mathcal{A}$.
7. When the ι-th Sig query, Sig query, $(\mathsf{gid}, m, \mathbb{S} := (M, \rho), \Gamma, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{t\in\mathcal{T}_{\mathsf{bad}} \wedge (t,\vec{x}_t)\in\Gamma})$, is issued by $\mathcal{A}$, $\mathcal{B}_{3\text{-}1}$ computes the replied signatures as follows:
   a. When $\iota < h$, $\mathcal{B}_2$ computes a semi-functional signature $(\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*)$ for $(m, \mathbb{S})$ as in Eq. (15) using $\{\mathbb{B}_t^*\}_{t=1,\ldots,d}$ in the Problem 2' instance.
   b. When $\iota = h$, $\mathcal{B}_2$ computes signature $(\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*)$ for $(m, \mathbb{S})$ as follows:

$$\begin{aligned}
\boldsymbol{s}_i^* := &(\overbrace{\vec{z}_{i,0}, \vec{z}_{i,1}}^{2n_t}, \overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\vec{\sigma}_i}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_i^*} \\
&+(\chi_{i,1}\boldsymbol{b}_{t,2n_t+1}^* + \chi_{i,2}\boldsymbol{h}_{\beta,t,1}^*) \\
&+H_2(m, \mathbb{S})(\chi_{i,1}\boldsymbol{b}_{t,2n_t+2}^* + \chi_{i,2}\boldsymbol{h}_{\beta,t,2}^*),
\end{aligned}$$

where $\widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\vec{\sigma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}, (\xi_i), (\xi'_i) \xleftarrow{\mathsf{U}} \{(\xi_1, \ldots, \xi_\ell) \mid \sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\}$, and for $i = 1, \ldots, \ell$, if $\rho(i) = (t, \vec{v}_i)$, then $(\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\mathsf{U}} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid$

$\vec{z}_{i,0} \cdot \vec{v}_i = \vec{z}_{i,1} \cdot \vec{v}_i = 0$, $z_{i,0,1} = \xi_i$, $z_{i,1,1} = \widetilde{\delta}\xi'_i$ }, if $\rho(i) = \neg(t, \vec{v}_i)$, then $(\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0} \cdot \vec{v}_i = \xi_i, \ \vec{z}_{i,1} \cdot \vec{v}_i = \widetilde{\delta}\xi'_i \}$, $\chi_{i,j} \xleftarrow{\cup} \mathbb{F}_q$ for $i = 1, \ldots, \ell$; $j = 1, 2$.

c. When $\iota > h$, $\mathcal{B}_2$ computes a normal signature $(\boldsymbol{s}^*_1, \ldots, \boldsymbol{s}^*_\ell)$ for $(m, \mathbb{S})$ as in Eq. (12) using $\{\mathbb{B}^*_t\}_{t=1,\ldots,d}$ in the Problem 2' instance.

8. When $\mathcal{B}_2$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ and from $\mathcal{A}$ (where $\mathbb{S}' := (M, \rho)$), $\mathcal{B}_2$ calculates the verification text $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ as follows: for $i = 1, \ldots, \ell$,

$$\begin{aligned}
\boldsymbol{c}_i &:= \textstyle\sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j} + H_2(m', \mathbb{S}')(\widetilde{\chi}_{i,1}\boldsymbol{b}_{t,2n_t+1} + \widetilde{\chi}_{i,2}\boldsymbol{e}_{t,1}) \\
&\quad -(\widetilde{\chi}_{i,1}\boldsymbol{b}_{t,2n_t+2} + \widetilde{\chi}_{i,2}\boldsymbol{e}_{t,2}) + \eta_i\boldsymbol{b}_{t,5n_t+3} \ \text{ for } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{good}}, \\
\boldsymbol{c}_i &:= \textstyle\sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j} + \widetilde{\chi}_{i,1}(H_2(m', \mathbb{S}')\boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}) \\
&\quad +\eta_i\boldsymbol{b}_{t,5n_t+3} \ \text{ for } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}, \\
c_{d+1} &:= g_T^{s_0},
\end{aligned}$$

where $\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ s.t. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0$, $\vec{s}'^{\mathrm{T}} := (s'_1, \ldots, s'_\ell)^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$, $\eta_i, \theta_i, \theta'_i \xleftarrow{\cup} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, and if $\rho(i) = (t, \vec{v}_i)$, then $\vec{c}_i := (s_i\vec{e}_{t,1} + \theta_i\vec{v}_i, s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i) \in \mathbb{F}_q^{2n_t}$, if $\rho(i) = \neg(t, \vec{v}_i)$, then $\vec{c}_i := (s_i\vec{v}_i, s'_i\vec{v}_i) \in \mathbb{F}_q^{2n_t}$ for $i = 1, \ldots, \ell$, $\widetilde{\chi}_{i,j} \xleftarrow{\cup} \mathbb{F}_q$ for $i = 1, \ldots, \ell$; $j = 1, 2$, and $\{\boldsymbol{e}_{t,j}\}_{j=1,2}$ are from the Problem 2' instance. $\mathcal{B}_2$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ using Ver with the above $(\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1})$, and outputs $\beta' := 1$, if the verification succeeds, $\beta' := 0$ otherwise.

Claim 1: The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_2$ given a Problem 2' instance with $\beta \in \{0, 1\}$ is the same as that in Game 2-$(h-1)$ (resp. Game 2-h) if $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$ (resp. d/q).

Proof. We consider the joint distribution of $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ generated in step 8 and $\{\boldsymbol{s}^*_i := \boldsymbol{s}^{(h)*}_i\}_{i=1,\ldots,\ell}$ generated in case (b) of step 7.

$\boldsymbol{c}_i$ for $i = 1, \ldots, \ell$ calculated in step 8 in the above simulation are expressed as:

$$\boldsymbol{c}_i = (\overbrace{\vec{c}_i,}^{2n_t} \overbrace{\omega_i(H_2(m', \mathbb{S}'), -1),}^{2} \overbrace{0^{n_t},}^{n_t} \overbrace{\sigma_i(H_2(m', \mathbb{S}'), -1, 0^{n_t-2}) \cdot Z_t,}^{n_t} \overbrace{0^{n_t},}^{n_t} \overbrace{\eta_i}^{1})_{\mathbb{B}_t}, \quad (\mathrm{A}\cdot 2)$$

where $\omega_i := \widetilde{\chi}_{i,1} + \widetilde{\chi}_{i,2}\omega, \sigma_i := \widetilde{\chi}_{i,2}\sigma$, and $\omega, \sigma, \{Z_t\}_{t=1,\ldots,d}$ are defined in Problem 2' and $\vec{c}_i \in \mathbb{F}_q^{2n_t}$ are defined in step 8 above. Note that ω_i, σ_i are uniformly and independently distributed.

When $\beta = 0$, replied signature $\boldsymbol{s}^*_i$ generated in case (b) of step 7 is

$$\boldsymbol{s}^*_i := (\overbrace{\vec{z}_{i,0}, \vec{z}_{i,1},}^{2n_t} \overbrace{\delta_i(1, H_2(m, \mathbb{S})),}^{2} \overbrace{0^{2n_t},}^{2n_t} \overbrace{\vec{\varphi}_i,}^{n_t} \overbrace{0}^{1})_{\mathbb{B}^*_t},$$

where $\delta_i := \chi_{i,1} + \chi_{i,2}\delta$, and δ is defined in Problem 2', $(\vec{z}_{i,0}, \vec{z}_{i,1}) \in \mathbb{F}_q^{2n_t}$ are defined in case (b) of step 7 above, and $\vec{\varphi}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}$. When $\beta = 1$, replied signature $\boldsymbol{s}^*_i$ generated in case (b) of step 7 is

$$\boldsymbol{s}^*_i := (\overbrace{\vec{z}_{i,0}, \vec{z}_{i,1},}^{2n_t} \overbrace{\delta_i(1, H_2(m, \mathbb{S})),}^{2} \overbrace{0^{n_t},}^{n_t} \overbrace{\tau_i(1, H_2(m, \mathbb{S}), 0^{n_t-2}) \cdot U_t,}^{n_t} \overbrace{\vec{\varphi}_i,}^{n_t} \overbrace{0}^{1})_{\mathbb{B}^*_t}, \quad (\mathrm{A}\cdot 3)$$

where $\delta_i := \chi_{i,1} + \chi_{i,2}\delta, \tau_i := \chi_{i,2}\tau$, and $\delta, \tau, \{U_t\}_{t=1,\ldots,d}$ are defined in Problem 2', $(\vec{z}_{i,0}, \vec{z}_{i,1}) \in \mathbb{F}_q^{2n_t}$ are defined in case (b) of step 7 above, and $\vec{\varphi}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}$. Note that δ_i, τ_i are uniformly and independently distributed.

Therefore, when $\beta = 0$, the distribution by $\mathcal{B}_2$'s simulation is equivalent to that in Game 2-$(h-1)$ except that σ defined in Problem 2' is zero, i.e., except with probability $1/q$. When $\beta = 1$, since $(m', \mathbb{S}')$ in Eq. (A·2) is not equal to $(m, \mathbb{S})$ in Eq. (A·3), the pair $(\tau_i(1, H_2(m, \mathbb{S}), 0^{n_t-2}) \cdot U_t, \sigma_i(H_2(m', \mathbb{S}'), -1, 0^{n_t-2}) \cdot Z_t) \in \mathbb{F}_q^{n_t} \times \mathbb{F}_q^{n_t}$ is distributed uniformly in $\mathbb{F}_q^{n_t} \times \mathbb{F}_q^{n_t}$ for each t except with probability d/q by Lemma 13, since $\widetilde{\rho}(\cdot)$ is injective. Hence, the distribution by $\mathcal{B}_2$'s simulation is equivalent to that in Game 2-h except that with probability d/q. □

From Claim 1, when $\beta = 0$, except in the event that occurs with probability $\frac{1}{q}$, the above game is the same as Game 2-$(h-1)$, and when $\beta = 1$, except in the event that occurs with probability $\frac{d}{q}$, the above game is the same as Game 2-h. Hence, when $\beta = 0$ (resp. $\beta = 1$), since the advantage of $\mathcal{A}$ in the above game is equal to $\mathsf{Pr}_0 := \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P2}'}(1^\lambda, n)\right]$ $\left(\text{resp. } \mathsf{Pr}_1 := \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P2}'}(1^\lambda, n)\right]\right)$, $\mathsf{Adv}^{(2\text{-}(h-1))}_{\mathcal{A}}(\lambda) \le \mathsf{Pr}_0 + \frac{1}{q}$ $\left(\text{resp. } \mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda) \le \mathsf{Pr}_1 + \frac{d}{q}\right)$ from Shoup's difference lemma. Therefore, $|\mathsf{Adv}^{(2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda)| \le |\mathsf{Pr}_0 - \mathsf{Pr}_1| + \frac{4}{q} = \mathsf{Adv}^{\mathsf{P2}'}_{\mathcal{B}_{2\text{-}h}}(\lambda) + \frac{d+1}{q}$. This completes the proof of Lemma 15. □

B.4 Proof of Lemma 16

Lemma 16. *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \le 2d/q$.*

Proof. Case that $h = 1$, i.e., proof for $|\mathsf{Adv}^{(2\text{-}\nu_S)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}1\text{-}1)}_{\mathcal{A}}(\lambda)| \le 2d/q$:

We consider the joint distribution of $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ and $\{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t=1,\ldots,d}$. In order to prove Lemma 16 in this case, we define new (dual orthonormal) bases $(\mathbb{D}_t, \mathbb{D}^*_t)$ of $\mathbb{V}_t$ as follows:

Since $\vec{z}_i \in \mathbb{F}_q^{n_t}$ is uniformly distribued and no $\vec{z}_i$ are $\vec{0}$ except for negligible probability, i.e., d/q, vector $\vec{\chi}_i := (0^{n_t}, \vec{z}_i) \cdot F_t$ is uniformly distributed in $\mathbb{F}_q^{2n_t}$ for $F_t \xleftarrow{\cup} GL(2n_t, \mathbb{F}_q)$ except for negligible probability $1/q$. Let $\vec{f}_{t,i}$ (resp. $\vec{f}^*_{t,i}$) be

the i-th row of matrix F_t (resp. $\left(F_t^{-1}\right)^{\mathrm{T}}$) for $i = 1, \ldots, 2n_t$, i.e., $F_t = \begin{pmatrix} \vec{f}_{t,1} \\ \vdots \\ \vec{f}_{t,2n} \end{pmatrix}$ and $\left(F_t^{-1}\right)^{\mathrm{T}} = \begin{pmatrix} \vec{f}^*_{t,1} \\ \vdots \\ \vec{f}^*_{t,2n} \end{pmatrix}$, $\boldsymbol{d}_{t,2n_t+2+i} := (0^{2n_t+2}, \vec{f}^*_{t,i}, 0^{n_t+1})_{\mathbb{B}_t}$ and $\boldsymbol{d}^*_{t,2n_t+2+i} := (0^{2n_t+2}, \vec{f}_{t,i}, 0^{n_t+1})_{\mathbb{B}^*_t}$ for $i = 1, \ldots, 2n_t$. Then, $\mathbb{D}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{d}_{t,2n_t+3}, \ldots, \boldsymbol{d}_{t,4n_t+2}, \boldsymbol{b}_{t,4n_t+3}, \ldots, \boldsymbol{b}_{t,5n_t+3})$ and $\mathbb{D}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{d}^*_{t,2n_t+3}, \ldots, \boldsymbol{d}^*_{t,4n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+3})$ are dual orthonormal bases.

In Game 2-ν_S, verification text $\boldsymbol{c}_i$ ($i = 1, \ldots, \ell$) are

$$\boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{0^{n_t}, \vec{z}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{D}_t}, \quad (\mathrm{A}\cdot 4)$$

for $i = 1, \ldots, \ell$, where the coefficients $\vec{\chi}_i$ on $\mathbb{D}_t$ are obtained from the definitions of $\vec{\chi}_i$ and $\mathbb{D}_t$, and $\vec{\chi}_i \in \mathbb{F}_q^{2n_t}$ are uniformly distributed and independent from all the other variables.

And, since no coefficient vectors $\vec{z}_i := ((r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t, r'_i\vec{e}_{t,1} + \omega'_i\vec{v}_i)$ if $\rho(i) = (t, \vec{v}_i)$ and $\vec{z}_i := (r_i\vec{v}_i \cdot Z_t, r'_i\vec{v}_i)$ if $\rho(i) = \neg(t, \vec{v}_i)$, where $\omega_i, \omega'_i \xleftarrow{\cup} \mathbb{F}_q, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q), \vec{g} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0\}, \vec{g}' \xleftarrow{\cup} \mathbb{F}_q^r, r_i := M_i \cdot \vec{g}^{\mathrm{T}}, r'_i := M_i \cdot (\vec{g}')^{\mathrm{T}}$ are zero except for negligible probability d/q, $\vec{\chi}_i := \vec{z}_i \cdot F_t$ are uniformly distributed in $\mathbb{F}_q^{2n_t}$ except for negligible probability d/q. Therefore, in Game 3-1-1, for the similarly defined dual orthonormal bases $(\widetilde{\mathbb{D}}_t, \widetilde{\mathbb{D}}^*_t)$, verification text $\boldsymbol{c}_i$ ($i = 1, \ldots, \ell$) are

$$\boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{z}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{D}_t}, \quad (\mathrm{A}\cdot 5)$$

for $i = 1, \ldots, \ell$, where the coefficients $\vec{\chi}_i$ on $\mathbb{D}_t$ are obtained from the definitions of $\vec{\chi}_i$ and $\mathbb{D}_t$, and $\vec{\chi}_i \in \mathbb{F}_q^{2n_t}$ are uniformly distributed and independent from all the other variables.

In the light of the adversary's view, $(\mathbb{D}_t, \mathbb{D}^*_t)$ and $(\widetilde{\mathbb{D}}_t, \widetilde{\mathbb{D}}^*_t)$ are consistent with authority public keys $\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t)$. Moreover, since the RHS of Eq. (A·4) and that of Eq. (A·5) are the same form, the challenge ciphertext $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ and $c_{d+1} := g_T^{s_0}$ in Game 2-ν_S can be conceptually changed to that in Game 3-1-1.

Case that $h \geq 2$, i.e., proof for $\left|\mathsf{Adv}^{(3\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)\right| \leq 2d/q$ for $h \geq 2$:

To prove Lemma 16 in this case, we will show distribution $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t\in S}, \{\boldsymbol{k}^{(j)*}_t\}_{j=1,\ldots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(j)}}, \{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1})$ in Game 3-$(h-1)$-4 and that in Game 3-h-1 are equivalent. For that purpose, we define new (dual orthonormal) bases $(\mathbb{D}_t, \mathbb{D}^*_t)$ of $\mathbb{V}_t$ as follows:

Since no r''_i, ω_i are zero except with negligible probability d/q, vectors $\vec{\chi}_i := ((r''_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t) \cdot F_t$ if $\rho(i) = (t, \vec{v}_i)$ and $\vec{\chi}_i := (r''_i\vec{v}_i \cdot Z_t) \cdot F_t$ if $\rho(i) = \neg(t, \vec{v}_i)$ are uniformly distributed in $\mathbb{F}_q^{n_t}$ for $F_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$ except with negligible probability d/q, where $\omega_i \xleftarrow{\cup} \mathbb{F}_q, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q), \vec{g}'' \xleftarrow{\cup} \mathbb{F}_q^r, r''_i := M_i(\vec{g}'')^{\mathrm{T}}$. Let $\vec{f}_{t,i}$ (resp. $\vec{f}^*_{t,i}$) be the i-th row of matrix F_t (resp. $\left(F_t^{-1}\right)^{\mathrm{T}}$) for $i = 1, \ldots, n$, i.e., $F_t = \begin{pmatrix} \vec{f}_{t,1} \\ \vdots \\ \vec{f}_{t,n} \end{pmatrix}$ and $\left(F_t^{-1}\right)^{\mathrm{T}} = \begin{pmatrix} \vec{f}^*_{t,1} \\ \vdots \\ \vec{f}^*_{t,n} \end{pmatrix}$, $\boldsymbol{d}_{t,2n_t+2+i} := (0^{2n_t+2}, \vec{f}^*_{t,i}, 0^{2n_t+1})_{\mathbb{B}_t}$ and $\boldsymbol{d}^*_{t,2n_t+2+i} := (0^{2n_t+2}, \vec{f}_{t,i}, 0^{2n_t+1})_{\mathbb{B}^*_t}$ for $i = 1, \ldots, n$. Then, $\mathbb{D}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{d}_{t,2n_t+3}, \ldots, \boldsymbol{d}_{t,3n_t+2}, \boldsymbol{b}_{t,3n_t+3}, \ldots, \boldsymbol{b}_{t,5n_t+3})$ and $\mathbb{D}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{d}^*_{t,2n_t+3}, \ldots, \boldsymbol{d}^*_{t,3n_t+2}, \boldsymbol{b}^*_{t,3n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+3})$ are dual orthonormal bases.

Verification text $\boldsymbol{c}_i$ ($i = 1, \ldots, \ell$) in Game 3-$(h-1)$-4 is

$$\begin{aligned}
&\text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r''_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} \\
&\qquad = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t}, \\
&\text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r''_i\vec{v}_i) \cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} \\
&\qquad = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t}, \qquad (\mathrm{A}\cdot 6)
\end{aligned}$$

where the coefficients $\vec{\chi}_i$ on $\mathbb{D}_t$ are obtained from the definitions of $\vec{\chi}_i$ and $\mathbb{D}_t$, and $\vec{\chi}_i \in \mathbb{F}_q^{n_t}$ are uniformly distributed and independent from all the other variables.

When $1 \leq j \leq \nu_H$, all the coefficients on $\mathsf{span}\langle \boldsymbol{b}^*_{t,2n_t+3}, \ldots, \boldsymbol{b}^*_{t,3n_t+2}\rangle$ of queried key $\{\boldsymbol{k}^{(j)*}_t\}_{(t,\vec{x}_t)\in\Gamma^{(j)}}$ for the j-th gid_j in Game 3-$(h-1)$-4 are zero. Therefore, the keys have the same coefficients on $\mathbb{D}^*_t$ as on $\mathbb{B}^*_t$. The same holds for queried signatures $\{\boldsymbol{s}^{(j)*}_i\}_{i=1,\ldots,\ell}$ for $j = 1, \ldots, \nu_S$.

And, no r_i, ω_i are zero except with negligible probability d/q, vectors $\vec{\chi}_i := ((r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t) \cdot F_i$ if $\rho(i) = (t, \vec{v}_i)$ and $\vec{\chi}_i := (r_i\vec{v}_i \cdot Z_t) \cdot F_t$ if $\rho(i) = \neg(t, \vec{v}_i)$ are uniformly distributed in $\mathbb{F}_q^{n_t}$ for $F_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$ except with negligible probability d/q, where $\omega_i \xleftarrow{\cup} \mathbb{F}_q, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q), \vec{g} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0\}, r_i := M_i \cdot \vec{g}^{\mathrm{T}}$. Therefore, in Game 3-$h$-1, for the similarly defined dual orthonormal bases $(\widetilde{\mathbb{D}}_t, \widetilde{\mathbb{D}}^*_t)$, verification text $\boldsymbol{c}_i$ ($i = 1, \ldots, \ell$) in Game 3-$(h-1)$-4 is

$$\begin{aligned}
&\text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} \\
&\qquad = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t}, \\
&\text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i\vec{v}_i) \cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} \\
&\qquad = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t}, \qquad (\mathrm{A}\cdot 7)
\end{aligned}$$

where the coefficients $\vec{\chi}_i$ on $\mathbb{D}_t$ are obtained from the definitions of $\vec{\chi}_i$ and $\mathbb{D}_t$, and $\vec{\chi}_i \in \mathbb{F}_q^{n_t}$ are uniformly distributed and independent from all the other variables.

In the light of the adversary's view, both $(\mathbb{D}_t, \mathbb{D}^*_t)$ and $(\widetilde{\mathbb{D}}_t, \widetilde{\mathbb{D}}^*_t)$ are consistent with public key $\mathsf{apk} := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t)$. Moreover, since the RHS of Eq. (A·6)

and that of Eq. (A·7) are the same form. Therefore, $\{\boldsymbol{k}_t^{(j)*}\}_{j=1,\ldots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(j)}}$, $\{\boldsymbol{s}_i^{(j)*}\}_{j=1,\ldots,\nu_S;i=1,\ldots,\ell}$ and $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ above can be expressed as keys, signatures, and verification text in two ways, in Game 3-$(h-1)$-4 and in Game 3-h-1. Thus, Game 3-$(h-1)$-4 can be conceptually changed to Game 3-h-1. □

B.5 Proof of Lemma 17

Lemma 17. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{3\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{3\text{-}h\text{-}1}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{3\text{-}1}(h,\cdot)$.*

Proof. In order to prove Lemma 17, we construct a probabilistic machine $\mathcal{B}_{3\text{-}1}$ against Problem 2 by using an adversary $\mathcal{A}$ in a security game (Game 3-h-1 or 3-h-2) as a black box as follows:

1. $\mathcal{B}_{3\text{-}1}$ is given an integer h and a Problem 2 instance, $(\mathsf{param}_{\vec{\imath}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n_t}, G_0, G_1, \delta G_1)$.
2. $\mathcal{B}_{3\text{-}1}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{3\text{-}1}$ provides $\mathcal{A}$ public keys gparam as in the proof of Lemma 14 and $\{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}'_t, \widehat{\mathbb{B}}^*_t)\}_{t\in\mathcal{T}_{\mathsf{good}}}$ of Game 3-h-1 (and 3-h-2), where $\pi \xleftarrow{\cup} \mathbb{F}_q, \widetilde{\boldsymbol{b}}^*_{t,\iota} := \pi\boldsymbol{b}^*_{t,\iota} + \boldsymbol{r}^*_{t,\iota}$ with $\boldsymbol{r}^*_{t,\iota} \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2}\rangle$, $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,5n_t+3})$ and $\widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1}, \ldots, \widetilde{\boldsymbol{b}}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2})$ for each authority $t \in \mathcal{T}_{\mathsf{good}}$, that are obtained from the Problem 2 instance. The H-list is initialized as in the proof of Lemma 14.
4. When a random oracle query for H_1 is issued for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$, $\mathcal{B}_{3\text{-}1}$ answers as follows:
   a. When $\iota \neq h$ and gid is not queried before, then a fresh $\delta_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q$ is generated and $\mathcal{B}_{3\text{-}1}$ answers $\delta_{\mathsf{gid}}G_1$ to $\mathcal{A}$ and records data $(\mathsf{gid}, \delta_{\mathsf{gid}}, \delta_{\mathsf{gid}}G_1)$ to the H list. When $\iota \neq h$ and gid is already queried, $\mathcal{B}_{3\text{-}1}$ obtains $\delta_{\mathsf{gid}}G_1$ from the H-list, and answers it to $\mathcal{A}$.
   b. When $\iota = h$, $\mathcal{B}_{3\text{-}1}$ answers δG_1 in the Problem 2 instance to $\mathcal{A}$ and records data $(\mathsf{gid}, \perp, \delta G_1)$ to the H list.
5. When an $\mathsf{AttrGen}$ query for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$ is issued for a pair of a global identity and an attribute $(\mathsf{gid}, (t, \vec{x}_t))$ for $t \in \mathcal{T}_{\mathsf{good}}$, $\mathcal{B}_{3\text{-}1}$ calculates $\boldsymbol{k}^*_t$ $(\in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)})$ as follows and then answers $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ to $\mathcal{A}$:
   a. When $1 \leq \iota \leq h-1$, $\mathcal{B}_{3\text{-}1}$ calculates semi-functional key $\boldsymbol{k}^*_t$ with Eq. (19) to $\mathcal{A}$, that is computed using $\mathbb{B}^*_t$ of the Problem 2 instance and δ_{gid} as

$$\boldsymbol{k}^*_t := (\overbrace{\vec{x}_t, \delta_{\mathsf{gid}}\vec{x}_t, 0^2}^{2n_t+2}, \overbrace{0^{n_t}, \tau'_{\mathsf{gid}}\vec{x}_t}^{2n_t}, \overbrace{\vec{\varphi}_{\mathsf{gid},t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t},$$

   where $\tau'_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q, \vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.
   b. When $\iota = h$, $\mathcal{B}_{3\text{-}1}$ calculates $\boldsymbol{k}^{(h)*}_t$ using $\mathbb{B}^*_t$ and $\{\boldsymbol{h}^*_{\beta,t,j}\}_{j=1,..,n_t}$ of the Problem 2 instance as follows:

$$\boldsymbol{k}^{(h)*}_t := \textstyle\sum_{j=1}^{n_t} x^{(h)}_{t,j}(\boldsymbol{b}^*_{t,j} + \boldsymbol{h}^*_{\beta,t,j}).$$

   c. When $\iota \geq h+1$, $\mathcal{B}_{3\text{-}1}$ calculates normal key $\boldsymbol{k}^*_t$ with Eq. (10), that is computed using $\mathbb{B}^*_t$ of the Problem 2 instance and δ_{gid} as

$$\boldsymbol{k}^*_t := (\overbrace{\vec{x}_t, \delta_{\mathsf{gid}}\vec{x}_t, 0^2}^{2n_t+2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\varphi}_{\mathsf{gid},t}}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}^*_t},$$

   where $\vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.
6. When a Sig query, $(\mathsf{gid}, m, \mathbb{S} := (M,\rho), \Gamma, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{t\in\mathcal{T}_{\mathsf{bad}}\wedge(t,\vec{x}_t)\in\Gamma})$, is issued by $\mathcal{A}$, $\mathcal{B}_{3\text{-}1}$ generates $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$ for $t \in \mathcal{T}_{\mathsf{good}} \wedge (t,\vec{x}_t) \in \Gamma$ as in Eq. (A·1). Then, $\mathcal{B}_{3\text{-}1}$ answers $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apt}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}_{(t,\vec{x}_t)\in\Gamma}, m, \mathbb{S})$ to $\mathcal{A}$.
7. When $\mathcal{B}_{3\text{-}1}$ receives an output $(m', \mathbb{S}', \vec{s}'^*)$ from $\mathcal{A}$ and $\{\mathsf{apt}_t\}_{t\in\mathcal{T}_{\mathsf{bad}}}$ (where $\mathbb{S}' := (M,\rho)$), $\mathcal{B}_{3\text{-}1}$ computes (pre-semi-functional) verification text $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ given as Eq. (16) as follows: Let

$$\begin{aligned}
&F^{<0>} := \{\vec{f} \in \mathbb{F}_q^r | \vec{1}\cdot\vec{f}^{\mathrm{T}} = 0\},\\
&F^{<1>} := \{\vec{f} \in \mathbb{F}_q^r | M_i\cdot\vec{f}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\},\\
&F^{<2>} := F^{<0>} \cap F^{<1>}\\
&= \{\vec{f} \in \mathbb{F}_q^r | \vec{1}\cdot\vec{f}^{\mathrm{T}} = 0, M_i\cdot\vec{f}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}.
\end{aligned}$$

   Then, $\mathcal{B}_{3\text{-}1}$ generates

$$\begin{aligned}
&\pi'_t, \mu_t \xleftarrow{\cup} \mathbb{F}_q \text{ for } t = 1, \ldots, d; (M_{i,k})_{i=1,..,\ell;k=1,..,r} := M,\\
&\vec{g}' := (g'_k)_{k=1,\ldots,r}, \vec{\mu}' := (\mu'_k)_{k=1,\ldots,r} \xleftarrow{\cup} F^{<2>};\\
&\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, s_0 := \vec{1}\cdot\vec{f}^{\mathrm{T}}, s_i := M_i\cdot\vec{f}^{\mathrm{T}},\\
&\vec{f}^{<0>} \xleftarrow{\cup} F^{<0>}, s_i^{<0>} := M_i\cdot(\vec{f}^{<0>})^{\mathrm{T}},\\
&\vec{g}^{<1>} \xleftarrow{\cup} F^{<1>}, r_i^{<1>} := M_i\cdot\left(\vec{g}^{<1>}\right)^{\mathrm{T}},\\
&\text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t;\\
&\boldsymbol{f}_{t,j} := \pi'_t\boldsymbol{e}_{t,j} + \mu_t\boldsymbol{b}_{t,n_t+j},\ \widetilde{\boldsymbol{f}}_{t,k,j} := g'_k\boldsymbol{e}_{t,j} + \mu'_k\boldsymbol{b}_{t,n_t+j},\\
&\text{for } i = 1 \ldots, \ell,\ \theta_i, \theta'_i, \theta''_i, \omega'_i \xleftarrow{\cup} \mathbb{F}_q,\ \boldsymbol{q}_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,5n_t+3}\rangle,\\
&\text{if } \rho(i) = (t, \vec{v}_i) \wedge t \in \mathcal{T}_{\mathsf{good}},\\
&(c_{i,1}, \ldots, c_{i,3n_t})\\
&:= (s_i\vec{e}_{t,1} + \theta_i\vec{v}_i,\ s_i^{<0>}\vec{e}_{t,1} + \theta'_i\vec{v}_i,\ r_i^{<1>}\vec{e}_{t,1} + \omega'_i\vec{v}_i),\\
&\boldsymbol{c}_i := \textstyle\sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j}\boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k}\widetilde{\boldsymbol{f}}_{t,k,1}\\
&\qquad + \theta''_i\left(H_2(m', \mathbb{S}')\boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}\right)\\
&\qquad + \textstyle\sum_{j=1}^{n_t} c_{i,n_t+j}\boldsymbol{b}_{t,3n_t+2+j} + \boldsymbol{q}_i,\\
&\text{if } \rho(i) = (t, \vec{v}_i) \wedge t \in \mathcal{T}_{\mathsf{bad}},
\end{aligned}$$

$(c_{i,1},\ldots,c_{i,2n_t}) := (s_i\vec{e}_{t,1} + \theta_i\vec{v}_i,\ s_i^{<0>}\vec{e}_{t,1} + \theta_i'\vec{v}_i)$,
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j}$
$+\theta_i''\,(H_2(m',\mathbb{S}')\boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}) + \boldsymbol{q}_i$,
if $\rho(i) = \neg(t,\vec{v}_i)\ \wedge\ t \in \mathcal{T}_{\mathsf{good}}$,
$(c_{i,1},\ldots,c_{i,3n_t}) := (s_i\vec{v}_i,\ s_i^{<0>}\vec{v}_i,\ r_i^{<1>}\vec{v}_i)$,
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j}\sum_{k=1}^{r} M_{i,k}\widetilde{\boldsymbol{f}}_{t,k,j}$
$+\theta_i''\,(H_2(m',\mathbb{S}')\boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2})$
$+\sum_{j=1}^{n_t} c_{i,n_t+j}\boldsymbol{b}_{t,3n_t+2+j} + \boldsymbol{q}_i$,
if $\rho(i) = \neg(t,\vec{v}_i)\ \wedge\ t \in \mathcal{T}_{\mathsf{bad}}$,
$(c_{i,1},\ldots,c_{i,2n_t}) := (s_i\vec{v}_i,\ s_i^{<0>}\vec{v}_i)$,
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j}$
$+\theta_i''\,(H_2(m',\mathbb{S}')\boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}) + \boldsymbol{q}_i$,
$c_{d+1} := g_T^{s_0}$,

where $\{\boldsymbol{b}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,2n_t+2,3n_t+3,\ldots,4n_t+2}$ and $\{\boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t}$ are obtained from the Problem 2 instance. $\mathcal{B}_{3\text{-}1}$ verifies the signature $(m',\mathbb{S}',\vec{s}'^{*})$ using Ver with the above $(\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell},\ c_{d+1})$, and $\beta' := 1$ if the verification succeeds, $\beta' := 0$ otherwise.

Claim 2: The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{3\text{-}1}$ given a Problem 2 instance with $\beta \in \{0,1\}$ is the same as that in Game 3-h-1 (resp. Game 3-h-2) if $\beta = 0$ (resp. $\beta = 1$).

Proof. We consider the joint distribution of $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ generated in step 7 and $\boldsymbol{k}_t^{(h)*}$ generated in case (b) of step 5.

$\boldsymbol{f}_{t,j},\ \widetilde{\boldsymbol{f}}_{t,k,j}$ for $t = 1,\ldots,d; k = 1,\ldots,r; j = 1,\ldots,n_t$ calculated in step 7 in the above simulation are expressed as:

$$\pi_t := \pi_t'\sigma,\ \ \theta_t := \pi_t'\omega + \mu_t,\ \ g_k := g_k'\sigma,\ \ f_k := g_k'\omega + \mu_k',$$
$$\boldsymbol{f}_{t,j} = (\overbrace{0^{n_t}}^{n_t},\ \overbrace{\theta_t\vec{e}_{t,j}}^{n_t},\ \overbrace{0^2}^{2},\ \overbrace{(\pi_t\vec{e}_{t,j})Z_t}^{n_t},\ \overbrace{0^{2n_t+1}}^{2n_t+1})_{\mathbb{B}_t},$$
$$\widetilde{\boldsymbol{f}}_{t,k,j} = (0^{n_t},\ f_k\vec{e}_{t,j},\ 0^2,\ (g_k\vec{e}_{t,j})Z_t,\ 0^{2n_t+1})_{\mathbb{B}_t},$$

where $\omega,\sigma,\{Z_t\}_{t=1,\ldots,d}$ are defined in Problem 2. Note that variables $\{\theta_t,\pi_t\}_{t=1,\ldots,d}$ are independently and uniformly distributed, and $\vec{f} := (f_k)_{k=1,\ldots,r}, \vec{g} := (g_k)_{k=1,\ldots,r} \in \mathbb{F}_q^r$ are independently and uniformly distributed with only relations $\vec{1}\cdot\vec{f} = \vec{1}\cdot\vec{g} = 0$ and $M_i\cdot\vec{f} = M_i\cdot\vec{g} = 0$ for $\widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}$. Therefore, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ are distributed as in Eq. (16).

When $\beta = 0$, secret key $\boldsymbol{k}_t^{(h)*}$ for $t \in \mathcal{T}_{\mathsf{good}}$ generated in case (b) of step 5 is

$$\boldsymbol{k}_t^{(h)*} = \sum_{j=1}^{n_t} x_{t,j}^{(h)}(\boldsymbol{b}_{t,j}^* + \boldsymbol{h}_{\beta,t,j}^*)$$
$$= (\overbrace{\vec{x}_t^{(h)},\ \delta\vec{x}_t^{(h)}}^{2n_t},\ \overbrace{0^2}^{2},\ \overbrace{0^{2n_t}}^{2n_t},\ \overbrace{\vec{\varphi}_t^{(h)}}^{n_t},\ 0)_{\mathbb{B}_t^*} \text{ with } \vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

When $\beta = 1$, secret key $\boldsymbol{k}_t^{(h)*}$ generated in case (b) of step 5 is

$$\boldsymbol{k}_t^{(h)*} = \sum_{j=1}^{n_t} x_{t,j}^{(h)}(\boldsymbol{b}_{t,j}^* + \boldsymbol{h}_{\beta,t,j}^*)$$
$$= (\overbrace{\vec{x}_t^{(h)},\ \delta\vec{x}_t^{(h)},\ 0^2}^{2n_t+2},\ \overbrace{\tau\vec{x}_t^{(h)}U_t,\ 0^{n_t}}^{2n_t},\ \overbrace{\vec{\varphi}_t^{(h)},\ 0}^{n_t})_{\mathbb{B}_t^*} \text{ with } \vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

Therefore, when $\beta = 0$, the distribution by $\mathcal{B}_{3\text{-}1}$'s simulation is equivalent to that in Game 3-h-1. When $\beta = 1$, the distribution by $\mathcal{B}_{3\text{-}1}$'s simulation is equivalent to that in Game 3-h-2. □

From Claim 2, we obtain Lemma 17 in the same manner as in the proof of Lemma 15. □

B.6 Proof of Lemma 18

Lemma 18. *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}2)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}3)}(\lambda)$.*

Proof.

Let $\vec{w}_i^{+,<b>} := (r_i^{<b>}\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t,\ \vec{w}_i^{-,<b>} := r_i^{<b>}\vec{v}_i\cdot Z_t,\ \vec{y}_t := \tau\vec{x}_t\cdot U_t$, where $b = 2,3$, $\tau := \tau^{(h)}$, $\vec{x}_t := \vec{x}_t^{(h)}$ and $r_i^{<2>}$ is a share of 0, $r_i^{<3>}$ is a share of a secret $r_0 \xleftarrow{\cup} \mathbb{F}_q$, i.e., $\vec{g}^{<2>} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1}\cdot\vec{g}^{\mathrm{T}} = 0,\ M_i\cdot\vec{f}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}$, $\vec{g}^{<3>} \xleftarrow{\cup} \{\vec{g} \in \mathbb{F}_q^r \mid M_i\cdot\vec{f}^{\mathrm{T}} = 0 \text{ for } \forall i \text{ s.t. } \widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{bad}}\}$, $r_i^{<b>} := M_i\cdot(\vec{g}^{<b>})^{\mathrm{T}}$ for $b = 2,3$; $\widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{good}}$.

For Game 3-h-2, we will consider the joint distribution of $(\vec{w}_i^{+,<2>},\vec{y}_t)$ with $\rho(i) = (t,\vec{v}_i)$ and that of $(\vec{w}_i^{-,<2>},\vec{y}_t)$ with $\rho(i) = \neg(t,\vec{v}_i)$. For Game 3-$h$-3, we will consider the joint distribution of $(\vec{w}_i^{+,<3>},\vec{y}_t)$ with $\rho(i) = (t,\vec{v}_i)$ and that of $(\vec{w}_i^{-,<3>},\vec{y}_t)$ with $\rho(i) = \neg(t,\vec{v}_i)$.

With respect to the joint distribution of these variables, there are five cases for each $i \in \{1,\ldots,\ell\}$. Note that for any $i \in \{1,\ldots,\ell\}$, (Z_t,U_t) with $t := \widetilde{\rho}(i)$ is independent from the other variables since $\widetilde{\rho}$ is injective, and that random vectors $\vec{g}^{<2>}$ and $\vec{g}^{<3>}$ are independent from the other variables. $\gamma(i)$ for $\widetilde{\rho}(i) \in \mathcal{T}_{\mathsf{good}}$ is defined in Definition 3.

1. $\gamma(i) = 1$ and $[\rho(i) = (t,\vec{v}_i)\ \wedge\ (t,\vec{x}_t) \in \Gamma\ \wedge\ \vec{v}_i\cdot\vec{x}_t = 0]$.
   Then, from Lemma 13, the joint distribution of $(\vec{w}_i^{+,<b>},\vec{y}_t)$ is uniformly and independently distributed on $C_{\tau r_i^{<b>}} := \{(\vec{w},\vec{y}) \mid \vec{w}\cdot\vec{y} = \tau r_i^{<b>}\}$ (over $Z_t \xleftarrow{\cup} GL(n_t,\mathbb{F}_q)$).
2. $\gamma(i) = 1$ and $[\rho(i) = \neg(t,\vec{v}_i)\ \wedge\ (t,\vec{x}_t) \in \Gamma\ \wedge\ \vec{v}_i\cdot\vec{x}_t \neq 0]$.
   Then, from Lemma 13, the joint distribution of $(\vec{w}_i^{-,<b>},\vec{y}_t)$ is uniformly and independently distributed on $C_{(\vec{v}_i\cdot\vec{x}_t)\cdot\tau r_i^{<b>}}$ (over $Z_t \xleftarrow{\cup} GL(n_t,\mathbb{F}_q)$).
3. $\gamma(i) = 0$ and $[\rho(i) = (t,\vec{v}_i)\ \wedge\ (t,\vec{x}_t) \in \Gamma]$ (i.e., $\vec{v}_i\cdot\vec{x}_t \neq 0$).
   Then, from Lemma 13, the joint distribution of $(\vec{w}_i^{+,<b>},\vec{y}_t)$ is uniformly and independently distributed on $C_{(\vec{v}_i\cdot\vec{x}_t)\cdot\omega_i + \tau r_i^{<b>}}$ (over $Z_t \xleftarrow{\cup} GL(n_t,\mathbb{F}_q)$) where ω_i is uniformly and independently distributed on $\mathbb{F}_q$. Hence, the joint distribution of $(\vec{w}_i^{+,<b>},\vec{y}_t)$ is uniformly and independently distributed over $\mathbb{F}_q^{2n_t}$.
4. $\gamma(i) = 0$ and $[\rho(i) = \neg(t,\vec{v}_i)\ \wedge\ (t,\vec{x}_t) \in \Gamma]$ (i.e., $\vec{v}_i\cdot\vec{x}_t = 0$).
   Then, from Lemma 13, the joint distribution of $(\vec{w}_i^{-,<b>},\vec{y}_t)$ is uniformly and independently distributed

on C_0 (over $Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$).

5. $[\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \notin \Gamma]$ or $[\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \notin \Gamma]$.
   Then, the distribution of $\vec{w}_i^{+,<b>}$ or $\vec{w}_i^{-,<b>}$ is uniformly and independently distributed on $\mathbb{F}_q^{n_t}$ (over $Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$).

We then observe the joint distribution (or relation) of $\{\vec{w}_i^{+,<b>}\}_{i=1,\ldots,\ell}, \{\vec{w}_i^{-,<b>}\}_{i=1,\ldots,\ell}$ and $\{\vec{y}_t\}_{t=1,\ldots,d}$. Those in cases 3, 4, and 5 are obviously independent from the others. Due to the restriction of adversary $\mathcal{A}$'s key queries, $\vec{1} \notin \mathsf{span}\langle (M_i)_{\overline{\rho}(i)\in\mathcal{T}_{\mathsf{good}} \wedge \gamma(i)=1}, (M_i)_{\overline{\rho}(i)\in\mathcal{T}_{\mathsf{bad}}} \rangle$. Hence, the distribution of $\{\ \tau r_i^{<2>} \mid \text{cases 1 and 2}\ \}$ is equivalent to that of $\{\ \tau r_i^{<3>} \mid \text{cases 1 and 2}\ \}$, since $\tau r_i^{<b>} = \tau M_i \cdot \left(\vec{g}^{<b>}\right)^{\mathrm{T}}$ for $b = 2, 3$, and the distributions of $\vec{g}^{<2>}$ and $\vec{g}^{<3>}$ are equivalent except that $\vec{1} \cdot \left(\vec{g}^{<2>}\right)^{\mathrm{T}} = 0$ and $\vec{1} \cdot \left(\vec{g}^{<3>}\right)^{\mathrm{T}}$ is uniformly distributed on $\mathbb{F}_q$.

Thus, the view of adversary $\mathcal{A}$ in Game 3-h-2 is equivalent to that in Game 3-h-3. □

B.7 Proof of Lemma 19

Lemma 19. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{3\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}4)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}2}}^{\mathsf{P3}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{3\text{-}2}(h, \cdot)$.*

Proof. In order to prove Lemma 19, we construct a probabilistic machine $\mathcal{B}_{3\text{-}2}$ against Problem 3 by using an adversary $\mathcal{A}$ in a security game (Game 3-h-3 or Game 3-h-4) as a black box. $\mathcal{B}_{3\text{-}2}$ acts in the same way as $\mathcal{B}_{3\text{-}1}$ in the proof of Lemma 17 except the following three points:

1. In case (b) of step 4; $\mathcal{B}_{3\text{-}2}$ acts in the same way as $\mathcal{B}_{3\text{-}1}$ in case (a) of step 4 in the proof of Lemma 17.
2. In case (b) of step 5; $\boldsymbol{k}_t^{(h)*}$ is calculated using $\mathbb{B}_t^*$ and $\{\boldsymbol{h}_{\beta,t,j}^*\}_{j=1,\ldots,n_t}$ of the Problem 3 instance as follows:

$$\boldsymbol{k}_t^{(h)*} := \sum_{j=1}^{n_t} x_{t,j}^{(h)} \left(\boldsymbol{b}_{t,j}^* + \delta^{(h)} \boldsymbol{b}_{t,n_t+j}^* + \boldsymbol{h}_{\beta,t,j}^*\right),$$

   where $\delta^{(h)} := \delta_{\mathsf{gid}_h}$.
3. In step 7; when $\mathcal{B}_{3\text{-}2}$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ from $\mathcal{A}$, $\mathcal{B}_{3\text{-}2}$ computes (semi-functional) verification text $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ given as Eq. (18) as follows:

$\pi_{t,\iota}, \widetilde{g}_{k,\iota} \xleftarrow{\cup} \mathbb{F}_q$ for $t = 1, \ldots, d;\ k = 1, \ldots, r;\ \iota = 1, 2$;
for $t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t$;
$\boldsymbol{f}_{t,j} := \sum_{\iota=1}^{2} \pi_{t,\iota} \boldsymbol{e}_{t,j,\iota}$, $\widetilde{\boldsymbol{f}}_{t,k,j} := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota} \boldsymbol{e}_{t,j,\iota}$,
for $i = 1 \ldots, \ell$,
if $\rho(i) = (t, \vec{v}_i)$,
$(c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{e}_{t,1} + \theta_i \vec{v}_i, s_i' \vec{e}_{t,1} + \theta_i' \vec{v}_i)$,
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,1}$
$+\theta_i'' \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}\right) + \boldsymbol{q}_i$,
if $\rho(i) = \neg(t, \vec{v}_i)$, $(c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{v}_i, s_i' \vec{v}_i)$,
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,j}$
$+\theta_i'' \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}\right) + \boldsymbol{q}_i$,
$c_{d+1} := g_T^{s_0}$,

where $(M_{i,k})_{i=1,\ldots,\ell;k=1,\ldots,r} := M, \vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, \vec{f}' \xleftarrow{\cup} \{\vec{f}' \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}, s_0 := \vec{1} \cdot \vec{f}'^{\mathrm{T}}, s_i := M_i \cdot \vec{f}^{\mathrm{T}}, s_i' := M_i \cdot \vec{f}'^{\mathrm{T}}, \theta_i, \theta_i', \theta_i'' \xleftarrow{\cup} \mathbb{F}_q$ and $\boldsymbol{q}_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,5n_t+3} \rangle$, and $\{\boldsymbol{b}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,2n_t+2}$, $\{\boldsymbol{e}_{t,j,t}\}_{t=1,\ldots,d;j=1,\ldots,n_t;t=1,2}$ are obtained from the Problem 3 instance. $\mathcal{B}_{3\text{-}2}$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ using Ver with the above $(\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1})$, and outputs $\beta' := 1$ if the verification succeeds, $\beta' := 0$ otherwise.

Claim 3: The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{3\text{-}2}$ given a Problem 3 instance with $\beta \in \{0, 1\}$ is the same as that in Game 3-h-3 (resp. Game 3-h-4) if $\beta = 0$ (resp. $\beta = 1$).

Proof. We consider the joint distribution of $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ generated in step 7 and $\boldsymbol{k}_t^{(h)}$ generated in case (b) of step 5.

$\boldsymbol{f}_{t,j}$, $\widetilde{\boldsymbol{f}}_{t,k,j}$ for $t = 1, \ldots, d; k = 1, \ldots, r; j = 1, \ldots, n_t$ calculated in step 7 in the above simulation are expressed as:

$$\pi_t := \sum_{\iota=1}^{2} \pi_{t,\iota} \omega_\iota,\ \ \pi_t' := \sum_{\iota=1}^{2} \pi_{t,\iota} \omega_\iota',$$
$$g_k := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota} \omega_\iota,\ \ g_k' := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota} \omega_\iota',$$
$$\boldsymbol{f}_{t,j} = (\overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\pi_t \vec{e}_{t,j}}^{n_t}, \overbrace{(\pi_t' \vec{e}_{t,j}) Z_t}^{n_t}, \overbrace{0^{n_t+1}}^{n_t+1})_{\mathbb{B}_t},$$
$$\widetilde{\boldsymbol{f}}_{t,k,j} = (0^{2n_t+2}, g_k \vec{e}_{t,j}, (g_k' \vec{e}_{t,j}) Z_t, 0^{n_t+1})_{\mathbb{B}_t},$$

where $\omega_\iota, \omega_\iota', \{Z_t\}_{t=1,\ldots,d}$ are defined in Problem 3. Note that variables $\{\pi_t, \pi_t'\}_{t=1,\ldots,d}$ and $\{g_k, g_k'\}_{k=1,\ldots,r}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ are distributed as in Eq. (18).

When $\beta = 0$, secret key $\boldsymbol{k}_t^{(h)*}$ generated in case (b) of step 5 is

$$\boldsymbol{k}_t^{(h)*} = \sum_{j=1}^{n_t} x_{t,j}^{(h)} \left(\boldsymbol{b}_{t,j}^* + \delta^{(h)} \boldsymbol{b}_{t,n_t+j}^* + \boldsymbol{h}_{\beta,t,j}^*\right)$$
$$= (\overbrace{\vec{x}_t^{(h)}, \delta \vec{x}_t^{(h)}}^{2n_t}, \overbrace{0^2}^{2}, \overbrace{\tau \vec{x}_t^{(h)} U_t, 0^{n_t}}^{2n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, 0)_{\mathbb{B}_t^*} \text{ with } \vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

When $\beta = 1$, secret key $\boldsymbol{k}_t^{(h)}$ generated in case (b) of step 5 is

$$\boldsymbol{k}_t^{(h)*} = \sum_{j=1}^{n_t} x_{t,j}^{(h)} \left(\boldsymbol{b}_{t,j}^* + \delta^{(h)} \boldsymbol{b}_{t,n_t+j}^* + \boldsymbol{h}_{\beta,t,j}^*\right)$$
$$= (\overbrace{\vec{x}_t^{(h)}, \delta \vec{x}_t^{(h)}}^{2n_t}, \overbrace{0^2}^{2}, \overbrace{0^{n_t}, \tau' \vec{x}_t^{(h)}}^{2n_t}, \overbrace{\vec{\varphi}_t^{(h)}}^{n_t}, 0)_{\mathbb{B}_t^*} \text{ with } \vec{\varphi}_t^{(h)} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

Therefore, when $\beta = 0$, the distribution by $\mathcal{B}_{3\text{-}2}$'s simulation is equivalent to that in Game 3-h-3. When $\beta = 1$, the distribution by $\mathcal{B}_{3\text{-}2}$'s simulation is equivalent to that in Game 3-h-4. □

From Claim 3, we obtain Lemma 19 in the same manner as in the proof of Lemma 15. □

B.8 Proof of Lemma 20

Lemma 20. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_4$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(3\text{-}\nu_H\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)| \le \mathsf{Adv}^{\mathsf{P2''}}_{\mathcal{B}_4}(\lambda)$.*

Proof. In order to prove Lemma 20, we construct a probabilistic machine $\mathcal{B}_4$ against Problem 2" by using an adversary $\mathcal{A}$ in a security game (Game 3-ν_H-4 or 4) as a black box as follows:

1. $\mathcal{B}_4$ is given a Problem 2" instance,$(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,j}, \boldsymbol{e}_{t,j}\}_{t=1,..,d;j=1,...,n_t}, G_0, G_1)$.
2. $\mathcal{B}_4$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_4$ provides $\mathcal{A}$ public keys gparam as in the proof of Lemma 14 and sets $\widetilde{\boldsymbol{b}}^*_{t,\iota} := \boldsymbol{h}^*_{\beta,t,\iota}$ for $\iota = 1, \ldots, n_t$, $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,5n_t+3}), \widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1}, \ldots, \widetilde{\boldsymbol{b}}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2}), \{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}'_t, \widehat{\mathbb{B}}^*_t)\}_{t\in S}$ for each authority $t \in S$ of Game 3-ν_H-4 (and 4), that are obtained from the Problem 2" instance.
4. When a random oracle query for H_1 is issued for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$, $\mathcal{B}_4$ answers as follows: When gid is not queried before, then a fresh $\delta_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q$ is generated and $\mathcal{B}_4$ answers $\delta_{\mathsf{gid}} G_1$ to $\mathcal{A}$ and records data $(\mathsf{gid}, \delta_{\mathsf{gid}}, \delta_{\mathsf{gid}} G_1)$ to the H list. When gid is already queried, $\mathcal{B}_4$ obtains $\delta_{\mathsf{gid}} G_1$ from the H-list, and answers it to $\mathcal{A}$.
5. When an $\mathsf{AttrGen}$ query for the ι-th global identity $\mathsf{gid} := \mathsf{gid}_\iota$ is issued for a pair of a global identity and an attribute $(\mathsf{gid}, (t, \vec{x}_t))$ for $t \in S$, $\mathcal{B}_4$ calculates semi-functional key $\{\boldsymbol{k}^*_t\}_{t\in S}$ with Eq. (19), that is computed using $\mathbb{B}^*_t$ of the Problem 2" instance and δ_{gid} as
$$\boldsymbol{k}^*_t := (\overbrace{\vec{x}_t,\ \delta_{\mathsf{gid}}\vec{x}_t,\ 0^2}^{2n_t+2},\ \overbrace{0^{n_t},\ \tau'_{\mathsf{gid}}\vec{x}_t}^{2n_t},\ \overbrace{\vec{\varphi}_{\mathsf{gid},t},}^{n_t}\ \overbrace{0}^{1})_{\mathbb{B}^*_t},$$
where $\tau'_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q, \vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.
6. When an AltSig query for $(m, \mathbb{S})$ is issued by $\mathcal{A}$, $\mathcal{B}_4$ computes a semi-functional signature $(\boldsymbol{s}^*_1, \ldots, \boldsymbol{s}^*_\ell)$ for $(m, \mathbb{S})$ as in Eq. (15) using $\{\mathbb{B}^*_t\}_{t=1,...,d}$ in the Problem 2" instance.
7. When $\mathcal{B}_4$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ from $\mathcal{A}$ (where $\mathbb{S}' := (M, \rho)$), $\mathcal{B}_4$ calculates a semi-functional verification text $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})$ given in Eq. (18) as follows:

$\pi'_t, \mu_t, g'_k, \mu'_k \xleftarrow{\cup} \mathbb{F}_q$ for $t = 1, \ldots, d$; $k = 1, \ldots, r$;
for $t = 1, \ldots, d$; $k = 1, \ldots, r$; $j = 1, \ldots, n_t$;
$\quad \boldsymbol{f}_{t,j} := \pi'_t \boldsymbol{e}_{t,j} + \mu_t \boldsymbol{b}_{t,j}$, $\widetilde{\boldsymbol{f}}_{t,k,j} := g'_k \boldsymbol{e}_{t,j} + \mu'_k \boldsymbol{b}_{t,j}$,
$\vec{f}' \xleftarrow{\cup} \{\vec{f}' \in \mathbb{F}_q^r | \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}$, $s'_i := M_i \cdot \vec{f}'^{\mathrm{T}}$ for $i = 1, .., \ell$,
for $i = 1 \ldots, \ell$,
if $\rho(i) = (t, \vec{v}_i)$,
$(c_{i,1}, \ldots, c_{i,2n_t}) := (s'_i \vec{e}_{t,1} + \theta'_i \vec{v}_i, (r''_i \vec{e}_{t,1} + \omega_i \vec{v}_i) \cdot Z_t)$,
$\boldsymbol{c}_i := \sum_{j=1}^{n_t} v_{i,j} \boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,1} + \sum_{j=1}^{n_t} c_{i,j} \boldsymbol{b}_{t,n_t+j}$
$\quad + \theta''_i (H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2})$
$\quad + \sum_{j=1}^{n_t} c_{i,n_t+j} \boldsymbol{b}_{t,2n_t+2+j} + \boldsymbol{q}_i$,
if $\rho(i) = \neg(t, \vec{v}_i)$, $(c_{i,1}, \ldots, c_{i,2n_t}) := (s'_i \vec{v}_i, r''_i \vec{v}_i \cdot Z_t)$,
$\boldsymbol{c}_i := \sum_{j=1}^{n_t} v_{i,j} \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,j} + \sum_{j=1}^{n_t} c_{i,j} \boldsymbol{b}_{t,n_t+j}$
$\quad + \theta''_i (H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2})$
$\quad + \sum_{j=1}^{n_t} c_{i,n_t+j} \boldsymbol{b}_{t,2n_t+2+j} + \boldsymbol{q}_i$,
$c_{d+1} := e(\sum_{k=1}^{r} \widetilde{\boldsymbol{f}}_{1,k,1}, \boldsymbol{b}^*_{1,1})$,

where $(M_{i,k})_{i=1,...,\ell;k=1,...,r} := M$, $\vec{f}' \xleftarrow{\cup} \{\vec{f}' \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}$, $s'_i := M_i \cdot \vec{f}'^{\mathrm{T}}, \vec{g} \xleftarrow{\cup} \mathbb{F}_q^r, r''_i := M_i \cdot \vec{g}^{\mathrm{T}}, \theta'_i, \theta''_i, \omega_i \xleftarrow{\cup} \mathbb{F}_q, Z_t \xleftarrow{\cup} GL(n_t, \mathbb{F}_q)$ and $\boldsymbol{q}_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,5n_t+3} \rangle$, and $\{\boldsymbol{b}_{t,j}\}_{t=1,...,d;j=1,...,3n_t+2}$, and $\{\boldsymbol{e}_{t,j}\}_{t=1,...,d;j=1,...,n_t}$ are obtained from the Problem 2" instance. $\mathcal{B}_4$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ using Ver with the above $(\{\boldsymbol{c}_i\}_{i=1,...,\ell}, c_{d+1})$, and outputs $\beta' := 1$ if the verification succeeds, $\beta' := 0$ otherwise.

Claim 4: The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_4$ given a Problem 2" instance with $\beta \in \{0, 1\}$ is the same as that in Game 3-ν_H-4 (resp. Game 4) if $\beta = 0$ (resp. $\beta = 1$).

Proof. We consider the joint distribution of $\{\boldsymbol{c}_i\}_{i=1,...,\ell}$ generated in step 7 and $\{\widetilde{\boldsymbol{b}}^*_{t,\iota}\}_{t=1,...,d;\iota=1,...,n_t}$ generated in step 3.

$\boldsymbol{f}_{t,j}$, $\widetilde{\boldsymbol{f}}_{t,k,j}$ for $t = 1, \ldots, d; k = 1, \ldots, r; j = 1, \ldots, n_t$ calculated in the step 7 in the above simulation are expressed as:

$$\pi_t := \pi'_t \sigma,\ \ \theta_t := \pi'_t \omega + \mu_t,\ \ g_k := g'_k \sigma,\ \ f_k := g'_k \omega + \mu'_k,$$
$$\boldsymbol{f}_{t,j} = (\overbrace{\theta_t \vec{e}_{t,j},}^{n_t}\ \overbrace{0^{2n_t+2},}^{2n_t+2}\ \overbrace{\pi_t \vec{e}_{t,j},}^{n_t}\ \overbrace{0^{n_t+1}}^{n_t+1})_{\mathbb{B}_t},$$
$$\widetilde{\boldsymbol{f}}_{t,k,j} = (f_k \vec{e}_{t,j},\ \ 0^{2n_t+2},\ \ g_k \vec{e}_{t,j},\ \ 0^{n_t+1})_{\mathbb{B}_t},$$

where ω, σ are defined in Problem 2". Note that variables $\{\theta_t, \pi_t\}_{t=1,...,d}$ and $\{f_k, g_k\}_{k=1,...,r}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{c}_i\}_{i=1,...,\ell}$ are distributed as in Eq. (18).

When $\beta = 0$, a part of authority public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, generated in step 3 is
$$\widetilde{\boldsymbol{b}}^*_{t,j} = \boldsymbol{h}^*_{\beta,t,j} = (\overbrace{\delta \vec{e}_{t,j},}^{n_t}\ \overbrace{0^{3n_t+2},}^{3n_t+2}\ \overbrace{\delta_{t,j},}^{n_t}\ 0)_{\mathbb{B}^*_t}$$
with $\delta \xleftarrow{\cup} \mathbb{F}_q$, $\delta_{t,j} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$. When $\beta = 1$, a part of authority public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, generated in step 3 is
$$\widetilde{\boldsymbol{b}}^*_{t,j} = \boldsymbol{h}^*_{\beta,t,j} = (\overbrace{\delta \vec{e}_{t,j},}^{n_t}\ \overbrace{0^{2n_t+2},}^{2n_t+2}\ \overbrace{\tau \vec{e}_{t,j},}^{n_t}\ \overbrace{\delta_{t,j},}^{n_t}\ 0)_{\mathbb{B}^*_t}$$
with $\delta, \tau \xleftarrow{\cup} \mathbb{F}_q$, $\delta_{t,j} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.

Therefore, when $\beta = 0$, the distribution by $\mathcal{B}_4$'s simulation is equivalent to that in Game 3-ν_H-4. When $\beta = 1$, the distribution by $\mathcal{B}_4$'s simulation is equivalent to that in Game 4. □

From Claim 4, we obtain Lemma 20 in the same manner as in the proof of Lemma 15. □

B.9 Proof of Lemma 21

Lemma 21. *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)$.*

Proof. To prove Lemma 21, we will show distribution $(\mathsf{gparam}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t=1,\dots,d}, \{\boldsymbol{s}^{(h)*}_i\}_{h=1,\dots,\nu_S;i=1,\dots,\ell}, \{\boldsymbol{k}^{(h)*}_t\}_{h=1,\dots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(h)}}, \{\boldsymbol{c}_i\}_{i=1,\dots,\ell})$ in Game 4 and that in Game 5 are equivalent. For that purpose, we define new bases $\mathbb{D}_t$ of $\mathbb{V}_t$ and $\mathbb{D}^*_t$ of $\mathbb{V}^*_t$ as follows: We generate random $\xi \xleftarrow{\cup} \mathbb{F}_q^\times$, and set

$$\boldsymbol{d}_{t,3n_t+2+\iota} := \boldsymbol{b}_{t,3n_t+2+\iota} - \xi\boldsymbol{b}_{t,\iota},\ \boldsymbol{d}^*_{t,\iota} := \boldsymbol{b}^*_{t,\iota} + \xi\boldsymbol{b}^*_{t,3n_t+2+\iota}$$

for $\iota = 1, \dots, n_t$, That is,

$$\begin{pmatrix} \boldsymbol{b}_{t,1} \\ \vdots \\ \boldsymbol{b}_{t,3n_t+2} \\ \boldsymbol{d}_{t,3n_t+3} \\ \vdots \\ \boldsymbol{d}_{t,4n_t+2} \\ \boldsymbol{b}_{t,4n_t+3} \\ \vdots \\ \boldsymbol{b}_{t,5n_t+3} \end{pmatrix} := \begin{pmatrix} I_{n_t} & & & \\ & I_{2n_t+2} & & \\ -\xi I_{n_t} & & I_{n_t} & \\ & & & I_{n_t+1} \end{pmatrix} \begin{pmatrix} \boldsymbol{b}_{t,1} \\ \vdots \\ \vdots \\ \boldsymbol{b}_{t,5n_t+3} \end{pmatrix},$$

$$\begin{pmatrix} \boldsymbol{d}^*_{t,1} \\ \vdots \\ \boldsymbol{d}^*_{t,n_t} \\ \boldsymbol{b}^*_{t,n_t+1} \\ \vdots \\ \boldsymbol{b}^*_{t,5n_t+3} \end{pmatrix} := \begin{pmatrix} I_{n_t} & & \xi I_{n_t} & \\ & I_{2n_t+2} & & \\ & & I_{n_t} & \\ & & & I_{n_t+1} \end{pmatrix} \begin{pmatrix} \boldsymbol{b}^*_{t,1} \\ \vdots \\ \vdots \\ \boldsymbol{b}^*_{t,5n_t+3} \end{pmatrix}.$$

We set

$$\mathbb{D}_t := (\boldsymbol{b}_{t,1}, \dots, \boldsymbol{b}_{t,3n_t+2}, \boldsymbol{d}_{t,3n_t+3}, \dots, \boldsymbol{d}_{t,4n_t+2}, \boldsymbol{b}_{t,4n_t+3}, \dots, \boldsymbol{b}_{t,5n_t+3}),$$
$$\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,1}, \dots, \boldsymbol{d}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+1}, \dots, \boldsymbol{b}^*_{t,5n_t+3}).$$

We then easily verify that $\mathbb{D}_t$ and $\mathbb{D}^*_t$ are dual orthonormal.

Signatures, keys, a part of authority public keys, and verification text, $\{\boldsymbol{s}^{(h)*}_i\}_{h=1,\dots,\nu_S;i=1,\dots,\ell}$, $\{\boldsymbol{k}^{(h)*}_t\}_{h=1,\dots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(h)}}$, $\{\widetilde{\boldsymbol{b}}^*_{t,\iota}\}_{t\in S;\iota=1,\dots,n_t}, \{\boldsymbol{c}_i\}_{i=1,\dots,\ell}$, in Game 4 are expressed over bases $\mathbb{B}_t$ and $\mathbb{B}^*_t$ as

$$\boldsymbol{s}^{(h)*}_t = (\vec{w}^{(h)}_i, \vec{w}'^{(h)}_i, \zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)})), 0^{n_t}, \boxed{\vec{u}^{(h)}_i}, \vec{\sigma}^{(h)}_i, 0)_{\mathbb{B}^*_t}$$
$$\boldsymbol{k}^{(h)*}_t = (\vec{x}^{(h)}_t,\ \delta^{(h)}\vec{x}^{(h)}_t,\ 0^{n_t+2},\ \boxed{\tau'^{(h)}}\vec{x}^{(h)}_t,\ \vec{\varphi}^{(h)}_t,\ 0)_{\mathbb{B}^*_t}$$
$$\widetilde{\boldsymbol{b}}^*_{t,\iota} = (\pi\vec{e}_{t,\iota},\ 0^{2n_t+2},\ \boxed{\eta}\vec{e}_{t,\iota},\ \vec{\varphi}_{t,\iota},\ 0)_{\mathbb{B}^*_t}$$
$$\boldsymbol{c}_i = (\boxed{s_i}\vec{e}_{t,1} + \boxed{\theta_i}\vec{v}_i,\ s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i,\ (r''_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t,$$
$$r'_i\vec{e}_{t,1} + \omega'_i\vec{v}_i,\ 0^{n_t},\ \eta_i)_{\mathbb{B}_t} \text{ if } \rho(i) = (t, \vec{v}_i),$$
$$\boldsymbol{c}_i := (\boxed{s_i}\vec{v}_i, s'_i\vec{v}_i, r''_i\vec{v}_i\cdot Z_t, r'_i\vec{v}_i, 0^{n_t}, \eta_i)_{\mathbb{B}_t}, \text{ if } \rho(i) = \neg(t, \vec{v}_i),$$

where a part framed by a box indicates coefficients which were changed in expression over bases $\mathbb{D}_t$ and $\mathbb{D}^*_t$. That is,

$$\boldsymbol{s}^{(h)*}_t = (\vec{w}^{(h)}_i, \vec{w}'^{(h)}_i, \zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)})), 0^{n_t}, \boxed{\vec{\vec{u}}^{(h)}_i}, \vec{\sigma}^{(h)}_i, 0)_{\mathbb{D}^*_t}$$
$$\boldsymbol{k}^{(h)*}_t = (\vec{x}^{(h)}_t,\ \delta^{(h)}\vec{x}^{(h)}_t,\ 0^{n_t},\ \boxed{\widetilde{\tau}'^{(h)}}\vec{x}^{(h)}_t,\ \vec{\varphi}^{(h)}_t,\ 0)_{\mathbb{D}^*_t}$$
$$\widetilde{\boldsymbol{b}}^*_{t,\iota} = (\pi\vec{e}_{t,\iota},\ 0^{2n_t+2},\ \boxed{\widetilde{\eta}}\vec{e}_{t,\iota},\ \vec{\vec{\varphi}}_{t,\iota},\ 0)_{\mathbb{D}^*_t}$$
$$\boldsymbol{c}_i = (\boxed{\widetilde{s}_i}\vec{e}_{t,1} + \boxed{\widetilde{\theta}_i}\vec{v}_i,\ s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i,\ (r''_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t,$$
$$r'_i\vec{e}_{t,1} + \omega'_i\vec{v}_i,\ 0^{n_t},\ \eta_i)_{\mathbb{D}_t} \text{ if } \rho(i) = (t, \vec{v}_i),$$
$$\boldsymbol{c}_i := (\boxed{\widetilde{s}_i}\vec{v}_i, s'_i\vec{v}_i, r''_i\vec{v}_i\cdot Z_t, r'_i\vec{v}_i, 0^{n_t}, \eta_i)_{\mathbb{D}_t} \text{ if } \rho(i) = \neg(t, \vec{v}_i),$$

where

$$\vec{\vec{u}}^{(h)}_i := \vec{u}^{(h)}_i - \xi\vec{w}'^{(h)}_i,\ \widetilde{\tau}'^{(h)} := \tau'^{(h)} - \xi,$$
$$\widetilde{\eta} := \eta - \xi\pi,\ \widetilde{\theta}_i := \theta_i + \xi\omega'_i,$$

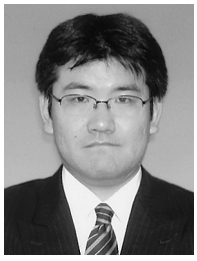
are uniformly, independently distributed since $\vec{u}^{(h)}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, $\tau'^{(h)}, \eta, \theta_i \xleftarrow{\cup} \mathbb{F}_q$, and

$$\widetilde{s}_i := s_i + \xi r'_i,$$

are a tuple of shared secrets $\{\widetilde{s}_i\}_{i=1,\dots,\ell}$ for access structure M, independent from s_0 in c_{d+1}, which are distributed as in Game 5 since $\xi \xleftarrow{\cup} \mathbb{F}_q^\times$.

In the light of the adversary's view, both $(\mathbb{B}_t, \mathbb{B}^*_t)$ and $(\mathbb{D}_t, \mathbb{D}^*_t)$ are consistent with public keys, $\mathsf{gparam} := (\mathsf{param}_{\mathbb{G}}, H_1, H_2)$ and apk_t except for $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, i.e., $(\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t, \widetilde{\mathbb{B}}^*_t)$, where $\widetilde{\mathbb{B}}^*_t := (\boldsymbol{b}^*_{t,n_t+1}, \dots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, \dots, \boldsymbol{b}^*_{t,5n_t+2})$. Therefore, $\{\boldsymbol{s}^{(h)*}_i\}_{h=1,\dots,\nu_S;i=1,\dots,\ell}, \{\boldsymbol{k}^{(h)*}_t\}_{h=1,\dots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(h)}}$, $\{\widetilde{\boldsymbol{b}}^*_{t,\iota}\}_{t\in S;\iota=1,\dots,n_t}, \{\boldsymbol{c}_i\}_{i=1,\dots,\ell}$ above can be expressed as signatures, keys, a part of authority public keys, and verification text in two ways, in Game 4 over bases $(\mathbb{B}_t, \mathbb{B}^*_t)$ and in Game 5 over bases $(\mathbb{D}_t, \mathbb{D}^*_t)$. Thus, Game 4 can be conceptually changed to Game 5. □

Tatsuaki Okamoto received the B.E., M.E. and Dr.E. degrees from the University of Tokyo, Tokyo, Japan, in 1976, 1978 and 1988, respectively. He is a Fellow of NTT, Nippon Telegraph and Telephone Corporation, and working with NTT Research Inc., California, USA. He is presently engaged in research on cryptography and information security.



Katsuyuki Takashima received the B.S., M.S. and PhD degrees from Kyoto University, Kyoto, Japan, in 1993, 1995 and 2009, respectively. He is presently engaged in research on cryptography and information security at Information Technology R&D center, Mitsubishi Electric Corporation. He was awarded the SCIS 2000 paper prize and 2003 annual award of JSIAM papers. He is a member of IPSJ, JSIAM, MSJ and IACR.