Decentralized Attribute-Based Signatures

Tatsuaki Okamoto[1] and Katsuyuki Takashima[2]

[1] NTT, okamoto.tatsuaki@lab.ntt.co.jp
[2] Mitsubishi Electric, Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

July 27, 2012

Abstract. We present the first *decentralized* multi-authority attribute-based signature (DMA-ABS) scheme, in which no central authority and no trusted setup are required. The proposed DMA-ABS scheme for general (non-monotone) predicates is fully secure (adaptive-predicate unforgeable and perfect private) under a standard assumption, the decisional linear (DLIN) assumption, in the random oracle model. Our DMA-ABS scheme is comparably as efficient as the most efficient ABS scheme. As a by-product, this paper also presents an adaptively secure DMA functional encryption (DMA-FE) scheme under the DLIN assumption.

1 Introduction

1.1 Background

Recently a versatile and privacy-enhanced class of digital signatures have been studied as attribute-based signatures (ABS) [23, 30–32, 39, 40, 42, 43, 48, 54, 59]. A signing (secret) key, $\mathsf{sk}_{\boldsymbol{x}}$, in ABS is parameterized by *attribute* $\boldsymbol{x}$, and the verification is executed using public key pk and predicate (or policy) Υ. A message m along with predicate Υ can be signed by signing key $\mathsf{sk}_{\boldsymbol{x}}$ (i.e., signature $\sigma := \mathsf{Sig}(\mathsf{sk}_{\boldsymbol{x}}, m, \Upsilon)$), if and only if $\boldsymbol{x}$ satisfies Υ. Signed message (m, Υ, σ) is verified by using public-key pk and predicate Υ, i.e., $\mathsf{Ver}(\mathsf{pk}, m, \Upsilon, \sigma) \in \{0, 1\}$. The *privacy* of a signer in this class of signatures requires that a signature (m, Υ, σ) generated by $\mathsf{sk}_{\boldsymbol{x}}$ (where $\boldsymbol{x}$ satisfies Υ) release no information regarding $\boldsymbol{x}$ except that $\boldsymbol{x}$ satisfies Υ.

There are many applications of ABS such as attribute-based messaging (ABM), attribute-based authentication, trust-negotiation and leaking secrets (see [43] for more details). For example, in a country (say country U), public comments on a new government's policy on scientific research are widely requested, especially to a class of people who should be responsible or heavily related to this topic from academia, government and industries. Comments from this class of people are requested to be signed (authenticated) to prove that the comments are from such people. In addition, the privacy of the people who send comments should be ensured. So there are contradictory requirements on authentication and privacy. The concept of ABS provides a nice solution to this type of problems. For example, a professor of University A sends a comment signed through ABS with a predicate such that ((Affiliation = University A `OR` B `OR` C) `AND` (Position = Professor `OR` Lecturer)) `OR` ((Affiliation = Government of Country U) `AND` (Qualification = PhD)) `OR` ((Affiliation = Company X `OR` Y `OR` Z) `AND` (Position = Chief Scientist `OR` Senior Manager)). A recipient of this signed comment can confirm that the signer of this comment is from the class of people, and the privacy is also preserved since there are too many people who satisfy the predicate and it is hard to identify the actual signer among so many possible signers due to the privacy condition of ABS.

The basic concept of ABS, however, has a serious problem that only a single authority exists in a system. Therefore, the single authority should issue to all users their secret keys

(certificates/credentials) associated with all attributes in the system, i.e., all positions of all organizations (e.g., all positions of Universities A, B and C, Governments of Countries U, V and W, and Companies X, Y and Z). If the party is corrupted, the system will be totally broken.

To overcome the drawback, the concept of *multi-authority* (MA-)ABS, was introduced [42, 43, 48], in which there are multiple authorities and each authority is responsible for issuing a secret key associated with a category or sub-universe of attributes, i.e., a user obtains several secret keys, each of which is issued by each authority. For example, a professor of university A obtains a secret key (for the position) from university A, a secret key for the citizenship from country U, and a secret key for a consultant position from company X, where university A, country U and company X are individual authorities. An important requirement for MA-ABS is the security (unforgeability) against collusion attacks. For example, it is required that a professor of university A, Alice, with a secret key for her position and a student, Bob, with a secret key for his citizenship of country W cannot collude to forge a signature endorsed by a professor of university A with the citizenship of country W.

The existing MA-ABS schemes, however, still have a problem that a special central authority is required in addition to multiple authorities regarding attributes, and if the central authority is corrupted, the security (unforgeability) of the system will be totally broken. As a typical example, we show in Appendix A that all MA-ABS schemes in [43] will be totally broken if the central authority is corrupted.

Any MA-ABS scheme with no central authority, *decentralized* MA-ABS (DMA-ABS) scheme, has not been proposed.

Recently, Lewko and Waters [38] presented the first DMA system for attribute-based encryption (ABE) (but not for ABS). Their scheme, however, still has a problem. It 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. In other words, their system requires a trusted setup. A generic conversion method from a composite-order-group-based system to a prime-order-group-based system has been presented by Lewko [35] and it may be applicable to the DMA-ABE scheme.

1.2 Our Results

– This paper proposes the first DMA-ABS scheme, which supports general relations, non-monotone access structures, 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 hash functions. 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 [33, 25] and [24], or can be included in the specification of the scheme. That is, no trusted setup is necessary in the proposed DMA-ABS system.
  In the proposed DMA-ABS schemes, every process can be executed in a fully decentralized manner; any party can become an authority and issue a (piece of a) secret key to a user without interacting with any other party, and each user obtains a (piece of a) 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) single secret key, composed of the pieces, of the user.

– This paper also proposes a more general signature scheme, DMA functional signature (FS) scheme, which supports more general predicates, non-monotone access structures combined with inner-product relations [47]. The proposed DMA-ABS scheme is a special case of the DMA-FS scheme, where the underlying inner-product relations are specialized to be two-dimensional inner-product relations for equality.
Remark: The general relations (non-monotone access structures combined with inner-product relations [47]) supported by the proposed DMA-FS scheme are: $\boldsymbol{x} := (\vec{x}_1, \ldots, \vec{x}_i) \in \mathbb{F}_q^{n_1+\cdots+n_i}$ for verification, and $\Upsilon := (\hat{M}, (\vec{v}_1, \ldots, \vec{v}_i) \in \mathbb{F}_q^{n_1+\cdots+n_i})$ for a secret key. The component-wise inner-product relations for attribute vector components, e.g., $\{\vec{x}_t \cdot \vec{v}_t = 0 \text{ or not }\}_{t\in\{1,\ldots,i\}}$, are input to span program $\hat{M}$, and $\boldsymbol{x}$ satisfies Υ iff the truth-value vector of $(\mathsf{T}(\vec{x}_1 \cdot \vec{v}_1 = 0), \ldots, \mathsf{T}(\vec{x}_i \cdot \vec{v}_i = 0))$ is accepted by span program $\hat{M}$. If the DMA-FS is specialized to DMA-ABS, 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 $x_t = v_t$.
– This paper proves that the proposed DMA-FS scheme is fully secure (adaptive-predicate unforgeable and perfect private in the DMA security model) under the DLIN assumption in the random oracle model. It implies that the proposed DMA-ABS scheme is fully secure under the DLIN assumption in the random oracle model.
– The efficiency of the DMA-ABS scheme is comparable to those of the existing ABS schemes (e.g., [43, 48]). See Table 1 in Section 5.5.
– Although the main aim of this paper is to propose the first DMA-ABS scheme, there is a by-product, a new DMA-FE (or DMA-ABE) scheme, which an adaptively secure DMA-FE scheme without a trusted setup under the DLIN assumption in the random oracle model.

Our DMA-ABS scheme is considered to be a natural extension of *ring signatures* [51, 53]. 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. 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.

1.3 Key Techniques

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) under a *standard assumption*, the DLIN assumption. It is a challenging task even in the random oracle model. For some notations hereafter, see Section 1.5.

To realize such a DMA-ABS scheme, we follow several established key ideas; dual pairing vector spaces (DPVS) [47, 48], Naor's paradigm (where an encryption counterpart, (2-level) DMA-ABE scheme, is designed first, and then DMA-ABS is constructed on it), global identifier gid [19], (random oracle) hashing of gid [38], dual system encryption [58, 38], and the linear transformation technique to produce $(\delta\vec{x}_t, \ldots)_{\mathbb{B}_t^*}$ by using X_t (the master secret key of authority t) and $\delta G := H(\mathsf{gid}) \in \mathbb{G}$ [48] (see Section 5.3 for the details). Note that, although our design

strategy is based on Naor's paradigm, this paper directly proves the security of the proposed DMA-ABS scheme from the DLIN assumption.

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 ABS and FE schemes in [47, 48]. No such a central space, however, is allowed in our DMA setting, where only spaces, $\mathbb{V}_t$ ($t = 1, \ldots$), generated by decentralized authorities are available. A crucial part of the key techniques in our DMA-ABS (and DMA-FE) scheme is to distribute the dual system encryption trick for the central space in the previous schemes into all the spaces.

More precisely, the secret-key and verification-text (where the negative term case in the span program, i.e., $\rho(i) = \neg(t, \vec{v}_i)$, is used, for simplicity of expression) 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 with a signature. Subspaces with $\{s_i\vec{v}_i\}$ and $\{\vec{x}_t\}$ are used for verification (or decryption), and subspaces with $\{s'_i\vec{v}_i\}$ and $\{\delta\vec{x}_t\}$ are for the *distributed* dual system encryption trick. To execute the trick over the subspaces, we develop a new technique, *swap and conceptual change*, in which 4-dimensional (in DMA-FS, $2n_t$-dimensional) hidden subspaces are employed for *semi-functional* forms of secret-keys and verification-texts. In the previous dual system encryption tricks [47, 48], the semi-functional form of secret-keys and verification-texts in a central space $\mathbb{V}_0$ ($t = 0$) played a key role. In our *distributed* dual system encryption trick, the left 2-dimensional subspaces in the 4-dimensional hidden subspaces are used for a computational change of secret-keys from DLIN and a conceptual change on key query restrictions. The right 2-dimensional subspaces are swapped with the left ones through a computational change from DLIN, and these subspaces for all $\mathbb{V}_t$ ($t = 1, \ldots$) play the key role in a distributed manner that corresponds to that of $\mathbb{V}_0$ ($t = 0$) in the previous schemes (see Appendix C.5).

In addition, a *new re-randomization* technique is developed in this paper to achieve the privacy of our DMA-ABS, since the re-randomization technique for the privacy in [48] is not effective in the DMA-ABS setting due to the fully distributed structure (see Section 5.2).

For more details on the techniques in the security proofs of DMA-ABS, see Appendices C.4–C.6 and D.

1.4 Related Works

1. The *mesh signatures* [13] 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.
2. Another related concept is *anonymous credentials (ACs)* [2, 3, 15, 17, 18, 21]. 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 [43], 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. See Appendix B for more details.

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

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 also has linear transformations $\phi_{i,j}$ *on* $\mathbb{V}$ *s.t.* $\phi_{i,j}(\boldsymbol{a}_j) = \boldsymbol{a}_i$ *and* $\phi_{i,j}(\boldsymbol{a}_k) = \boldsymbol{0}$ *if* $k \neq j$*, which can be easily achieved by* $\phi_{i,j}(\boldsymbol{x}) := (\overbrace{0, \ldots, 0}^{i-1}, G_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $\boldsymbol{x} := (G_1, \ldots, G_N)$*. We call* $\phi_{i,j}$ *"canonical maps".*

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* $\mathcal{G}_{\mathsf{bpg}}$*.*

For the asymmetric version of DPVS, $(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$, see Appendix A.2 in the full version of [47].

3 General Predicates: Non-Monotone Access Structures with Inner-Product Relations

3.1 Span Programs and Non-Monotone Access Structures

Definition 3 (Span Programs [1]). *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-ABS (and DMA-FS, DMA-FE) 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 Appendix C.3 with our DMA-FS 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 [8]). *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*

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

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 Signatures (DMA-ABS)

5.1 Definitions for DMA-ABS

Definition 7 (Decentralized Multi-Authority ABS : DMA-ABS). *A decentralized multi-authority ABS scheme consists of the following algorithms/protocols.*

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 $(1 \leq t \leq d)$ *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.

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

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* $\{\mathsf{usk}_{\mathsf{gid},(t,x_t)} \mid (t, x_t) \in \Gamma\}$ *from the attribute authorities. Then signature* σ *can be generated using* $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,x_t)}\}, m, \mathbb{S})$, *where* $\mathsf{usk}_{\mathsf{gid},(t,x_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, x_t)$.

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* $\mathsf{accept} := 1$ *or* $\mathsf{reject} := 0$.

Definition 8 (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* $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t)$ $(1 \leq t \leq d)$, *all messages* m, *all attribute sets* Γ_1 *associated with* gid_1 *and* Γ_2 *associated with* gid_2, *all signing keys* $\{\mathsf{usk}_{t,1} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_1, x_{t,1})\}_{(t,x_{t,1})\in\Gamma_1}$ *and* $\{\mathsf{usk}_{t,2} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_2, x_{t,2})\}_{(t,x_{t,2})\in\Gamma_2}$, *all access structures* $\mathbb{S}$ *such that* $\mathbb{S}$ *accepts* Γ_1 *and* $\mathbb{S}$ *accepts* Γ_2, *the distributions* $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{t,1} \mid (t, x_{t,1}) \in \Gamma_1\}, m, \mathbb{S})$ *and* $\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{t,2} \mid (t, x_{t,2}) \in \Gamma_2\}, m, \mathbb{S})$ *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 $\{\mathsf{usk}_{\mathsf{gid},(t,x_t)}\}_{(t,x_t)\in\Gamma}$: First, generate $\mathsf{usk}_{\mathsf{gid},(t,x_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, x_t)$ for arbitrary $\Gamma := \{(t, x_t)\}$ which satisfies $\mathbb{S}$, then $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,x_t)}\}, m, \mathbb{S})$. Return σ.

Let T be the set of authorities. We assume each attribute is assigned to one authority.

Definition 9 (Unforgeability of DMA-ABS). *For an adversary, we define* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}ABS,UF}}(\lambda)$ *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. *Run* $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$ *and give* gparam *to the adversary* $\mathcal{A}$. *For authorities* $t \in T$, *run* $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam})$ *and give* $\{\mathsf{apk}_t\}_{t\in T}$ *to* $\mathcal{A}$. *Adversary* $\mathcal{A}$ *specifies a set* $\widetilde{T} \subset T$ *of corrupt attribute authorities, and gets* $\{\mathsf{ask}_t\}_{t\in\widetilde{T}}$.
2. *The adversary* $\mathcal{A}$ *is given access to oracles* $\mathsf{AttrGen}$ *and* AltSig *over* $S := T \setminus \widetilde{T}$.
3. *At the end, the adversary outputs* $(m', \mathbb{S}', \sigma')$.

Let $\Gamma_{\mathsf{gid}_i} := \{(t \in S, x_t)\}$ $(i = 1, \ldots, \nu_H)$ *queried to the* $\mathsf{AttrGen}$ *oracle with* gid_i. *We say the adversary succeeds, if* $(m', \mathbb{S}')$ *was never queried to the* AltSig *oracle,* $\mathbb{S}'$ *does not accept* Γ_{gid_i} *with any* gid_i $(i = 1, \ldots, \nu_H)$ *queried to the* $\mathsf{AttrGen}$ *oracle,* $\mathbb{S}'$ *is specified over* S, *and* $\mathsf{Ver}(\mathsf{pk}, m', \mathbb{S}', \sigma') = 1$.

Remark 3 The model regarding *corrupted authorities* in this definition is weaker than that in [43]. Roughly, the security on this model implies that no adversary $\mathcal{A}$ can forge a signature with a predicate $\mathbb{S}'_S$ unless $\mathcal{A}$ issues key queries for Γ_S such that $\mathbb{S}'_S$ accepts Γ_S, where $\mathbb{S}'_S$ and Γ_S are a predicate and attributes over uncorrupted parties S. On the other hand, the security on the model in [43] implies that no adversary $\mathcal{A}$ can forge a signature with a predicate $\mathbb{S}'_{S\cup\widetilde{T}}$ unless $\mathcal{A}$ issues key queries for Γ_S such that, for some $\Gamma_{\widetilde{T}}$, $\mathbb{S}'_{S\cup\widetilde{T}}$ accepts $(\Gamma_S \cup \Gamma_{\widetilde{T}})$.

5.2 Construction Idea of the Proposed DMA-ABS Scheme

Here we will show some basic idea to construct the proposed DMA-ABS scheme, which is designed on the DMA-FE scheme (Appendix E.2) through Naor's paradigm. Note that the privacy condition is not included in Naor's paradigm.

Roughly speaking, a secret signing key sk_Γ with attribute set Γ and a verification text $\vec{\boldsymbol{c}}$ 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 $\vec{\boldsymbol{c}}$ with $\mathbb{S}$ in the DMA-FE scheme, respectively. No counterpart of a signature $\vec{\boldsymbol{s}}^*$ in the DMA-ABS exists in the DMA-FE, and the privacy property for signature $\vec{\boldsymbol{s}}^*$ is also specific in DMA-ABS. Signature $\vec{\boldsymbol{s}}^*$ 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-FE scheme:

- GSetup Almost the same as that in the DMA-FE 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-FE scheme except that $\widehat{\mathbb{B}}^*_t$ is revealed as a *public* parameter in our DMA-ABS, while it is *secret* in the DMA-FE scheme. They are published in our DMA-ABS for the signature generation procedure Sig to meet the *privacy* of signers (for randomization). This is an essential difference between DMA-FE and DMA-ABS.
  Since (a part of) $\widehat{\mathbb{B}}^*_0$ is a master secret in [48], other bases $\{\widehat{\mathbb{B}}^*_t\}_{t>0}$ can be published. However, for lack of $\mathbb{V}_0$ in our DMA-ABS, *modified* sub-bases $(\widetilde{\boldsymbol{b}}^*_{t,\iota})_{\iota=1,2}$ are used in public key $\{\widehat{\mathbb{B}}^*_t\}_{t>0}$ in place of sub-bases $(\boldsymbol{b}^*_{t,\iota})_{\iota=1,2}$, and a new security proof technique is required.
- $\mathsf{AttrGen}$ The same as that in the DMA-FE scheme.
- Sig Specific in DMA-ABS. To meet the privacy condition for $\vec{\boldsymbol{s}}^*$, a novel technique is employed to randomly generate a signature from sk_Γ and $\{\widehat{\mathbb{B}}^*_t\}_{(t,x_t)\in\Gamma}$. In [48], an attribute vector $(1, x_t)$ is encoded on 2-dimensional subspace $\mathsf{span}\langle \boldsymbol{b}^*_{t,1}, \boldsymbol{b}^*_{t,2}\rangle$ for $t > 0$. Since our DMA-ABS lacks the space $\mathbb{V}_0$, however, the vector is also encoded on another subspace $\mathsf{span}\langle \boldsymbol{b}^*_{t,3}, \boldsymbol{b}^*_{t,4}\rangle$. To re-randomize both vectors independently using public $(\widetilde{\boldsymbol{b}}^*_{t,\iota}, \boldsymbol{b}^*_{t,2+\iota})_{\iota=1,2}$ is one of key tricks here.
- Ver The signature verification in our DMA-ABS checks whether a signature (or a specific decryption key) $\vec{\boldsymbol{s}}^*$ works as a decryption key to decrypt a verification text (or a ciphertext) associated with $\mathbb{S}$ and $\mathsf{H}_2(m, \mathbb{S})$.

5.3 Proposed DMA-ABS Scheme

We define function $\widetilde{\rho} : \{1, \ldots, \ell\} \to \{1, \ldots, d\}$ by $\widetilde{\rho}(i) := t$ if $\rho(i) = (t, v)$ or $\rho(i) = \neg(t, v)$, 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 will show how to relax the restriction in Appendix F. We refer to Section 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 $\boldsymbol{v}$ in N-dimensional $\mathbb{V}$, $X(\boldsymbol{v})$ denotes $\sum_{i=1,j=1}^{N,N} \chi_{i,j}\phi_{i,j}(\boldsymbol{v})$ using canonical maps $\{\phi_{i,j}\}$ (Definition 2). Similarly, for matrix $(\vartheta_{i,j}) := (X^{-1})^{\mathrm{T}}$, $(X^{-1})^{\mathrm{T}}(\boldsymbol{v}) := \sum_{i=1,j=1}^{N,N} \vartheta_{i,j}\phi_{i,j}(\boldsymbol{v})$. It holds that $e(X(\boldsymbol{x}), (X^{-1})^{\mathrm{T}}(\boldsymbol{y})) = e(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}$.

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

$G_0 := H_1(0^\lambda) \in \mathbb{G}$, $G_1 := H_1(0^{\lambda-1}, 1) \in \mathbb{G}$, $G_2 := H_1(0^{\lambda-2}, 1, 0) \in \mathbb{G}$, $g_T := e(G_0, G_1)$.

$\mathsf{ASetup}(\mathsf{gparam}, t)$: $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 13, \mathsf{param}_{\mathbb{G}})$,

$X_t \xleftarrow{\mathsf{U}} GL(13, \mathbb{F}_q)$, $(\widetilde{\varphi}_{t,\iota,1}, \widetilde{\varphi}_{t,\iota,2}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$ for $\iota = 1, 2$,

$\boldsymbol{b}_{t,\iota} := X_t((0^{\iota-1},\ G_0,\ 0^{13-\iota}))$, $\boldsymbol{b}^*_{t,\iota} := (X_t^{\mathrm{T}})^{-1}((0^{\iota-1},\ G_1,\ 0^{13-\iota}))$ for $\iota = 1, \ldots, 13$,

$$\widetilde{\boldsymbol{b}}^*_{t,1} := (X_t^{\mathrm{T}})^{-1}\ ((\overbrace{G_2,\ 0}^{2}, \overbrace{0^8}^{8}, \overbrace{\widetilde{\varphi}_{t,1,1}G_1, \widetilde{\varphi}_{t,1,2}G_1}^{2}, \overbrace{0}^{1})),$$

$$\widetilde{\boldsymbol{b}}^*_{t,2} := (X_t^{\mathrm{T}})^{-1}\ ((\overbrace{0,\ G_2}^{2}, \overbrace{0^8}^{8}, \overbrace{\widetilde{\varphi}_{t,2,1}G_1, \widetilde{\varphi}_{t,2,2}G_1}^{2}, \overbrace{0}^{1})),$$

$\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,13})$, $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,13})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,6}, \boldsymbol{b}_{t,13})$,

$\widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1}, \widetilde{\boldsymbol{b}}^*_{t,2}, \boldsymbol{b}^*_{t,3}, \ldots, \boldsymbol{b}^*_{t,6}, \boldsymbol{b}^*_{t,11}, \boldsymbol{b}^*_{t,12})$,

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 $\widetilde{\boldsymbol{b}}^*_{t,1} = (\overbrace{\pi, 0}^{2}, \overbrace{0^8}^{8}, \overbrace{\widetilde{\varphi}_{t,1,1}, \widetilde{\varphi}_{t,1,2}}^{2}, \overbrace{0}^{1})_{\mathbb{B}^*_t}$, $\widetilde{\boldsymbol{b}}^*_{t,2} = (\overbrace{0, \pi}^{2}, \overbrace{0^8}^{8}, \overbrace{\widetilde{\varphi}_{t,2,1}, \widetilde{\varphi}_{t,2,2}}^{2}, \overbrace{0}^{1})_{\mathbb{B}^*_t}$.

$\mathsf{AttrGen}(\mathsf{gparam},\ t,\ \mathsf{ask}_t,\ \mathsf{gid},\ x_t \in \mathbb{F}_q)$: $G_{\mathsf{gid}} := H_1(\mathsf{gid})$, $(\varphi_{t,1}, \varphi_{t,2}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^2$,

$$\boldsymbol{k}^*_t := (X_t^{\mathrm{T}})^{-1}\ ((\overbrace{G_1,\ x_t G_1}^{2}, \overbrace{G_{\mathsf{gid}},\ x_t G_{\mathsf{gid}}}^{2}, \overbrace{0^6}^{6}, \overbrace{\varphi_{t,1}G_1,\ \varphi_{t,2}G_1}^{2}, \overbrace{0}^{1})),$$

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

Remark : Let $\delta \in \mathbb{F}_q$ s.t. $G_{\mathsf{gid}} = \delta G_1$, then $\boldsymbol{k}^*_t = (\overbrace{(1,\ x_t)}^{2}, \overbrace{\delta(1,\ x_t)}^{2}, \overbrace{0^6}^{6}, \overbrace{\varphi_{t,1},\ \varphi_{t,2}}^{2}, 0\ )_{\mathbb{B}^*_t}$.

$\mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,x_t)} := (\mathsf{gid}, (t, x_t), \boldsymbol{k}^*_t)\},\ m,\ \mathbb{S} := (M, \rho))$:

If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, x_t) \in \mathsf{usk}_{\mathsf{gid},(t,x_t)}\}$, 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

$I \subseteq \{i \in \{1, \ldots, \ell\} |\ [\rho(i) = (t, v_i) \ \wedge\ (t, x_t) \in \Gamma \ \wedge\ v_i = x_t]$

$\qquad\qquad \vee\ [\rho(i) = \neg(t, v_i) \ \wedge\ (t, x_t) \in \Gamma \ \wedge\ v_i \neq x_t]\ \}$,

$\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\psi_i := \psi$ if $i \in I$, $\psi_i := 0$ if $i \notin I$ for $i = 1, \ldots, \ell$,

for $i = 1, \ldots, \ell$, $\zeta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\beta_{i,0}), (\beta_{i,1}) \xleftarrow{\mathsf{U}} \{(\beta_1, \ldots, \beta_\ell) \mid \sum_{i=1}^{\ell} \beta_i M_i = \vec{0}\}$,

Remark : If $\det M \neq 0$, the set contains only 0^ℓ, i.e., all $\beta_i = 0$ for $i = 1, \ldots, \ell$.

$$\boldsymbol{s}_i^* := \gamma_i \cdot \boldsymbol{k}_t^* + \psi_i(\boldsymbol{b}_{t,3}^* + x_t \boldsymbol{b}_{t,4}^*) + \sum_{\iota=1}^{2} \left(y_{i,0,\iota} \widetilde{\boldsymbol{b}}_{t,\iota}^* + y_{i,1,\iota} \boldsymbol{b}_{t,2+\iota}^* \right) + \zeta_i \left(\boldsymbol{b}_{t,5}^* + H_2(m, \mathbb{S}) \boldsymbol{b}_{t,6}^* \right) + \boldsymbol{r}_i^*,$$

where $\boldsymbol{r}_i^* \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{t,11}^*, \boldsymbol{b}_{t,12}^* \rangle$, and $\gamma_i, \vec{y}_{i,j} := (y_{i,j,1}, y_{i,j,2})$ for $j = 0, 1$, are defined as

if $i \in I \ \wedge \ \rho(i) = (t, v_i)$, $\gamma_i := \alpha_i$, $\vec{y}_{i,j} := \beta_{i,j}(1, v_i)$,

if $i \in I \ \wedge \ \rho(i) = \neg(t, v_i)$, $\gamma_i := \dfrac{\alpha_i}{v_i - x_t}$, $\vec{y}_{i,j} := \dfrac{\beta_{i,j}}{v_i - y_{i,j}}(1, y_{i,j})$ where $y_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q \setminus \{v_i\}$,

if $i \notin I \ \wedge \ \rho(i) = (t, v_i)$, $\gamma_i := 0$, $\vec{y}_{i,j} := \beta_{i,j}(1, v_i)$,

if $i \notin I \ \wedge \ \rho(i) = \neg(t, v_i)$, $\gamma_i := 0$, $\vec{y}_{i,j} := \dfrac{\beta_{i,j}}{v_i - y_{i,j}}(1, y_{i,j})$ where $y_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q \setminus \{v_i\}$,

return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*)$.

$\mathsf{Ver}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m, \mathbb{S} := (M, \rho), \vec{\boldsymbol{s}}^*)$: $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$, $s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$,

$\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ 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 $i = 1, \ldots, \ell$, $\theta_i, \theta'_i, \theta''_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

if $\rho(i) = (t, v_i)$,

$$\boldsymbol{c}_i := (\overbrace{s_i + \theta_i v_i,\ -\theta_i}^{2},\ \overbrace{s'_i + \theta'_i v_i,\ -\theta'_i}^{2},\ \overbrace{\theta''_i(H_2(m, \mathbb{S}), -1)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t, v_i)$, $\boldsymbol{c}_i := (\overbrace{s_i(v_i,\ -1)}^{2},\ \overbrace{s'_i(v_i,\ -1)}^{2},\ \overbrace{\theta''_i(H_2(m, \mathbb{S}), -1)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\eta_i}^{1})_{\mathbb{B}_t}$,

$c_{d+1} := g_T^{s_0}$, return 1 if $\prod_{i=1}^{\ell} e(\boldsymbol{c}_i, \boldsymbol{s}_i^*) = c_{d+1}$, return 0 otherwise.

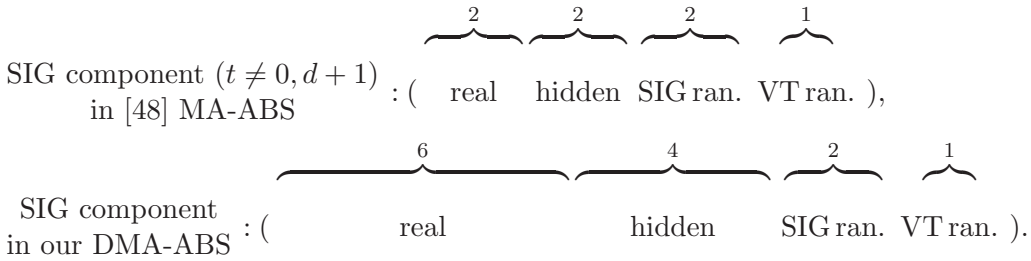
[Correctness] If $\mathbb{S} := (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$,

$$\prod_{i=1}^{\ell} e(\boldsymbol{c}_i, \boldsymbol{s}_i^*) = \prod_{i \in I} \left(e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\gamma_i} e(\boldsymbol{c}_i, \boldsymbol{b}_3^* + x_{t,\iota} \boldsymbol{b}_4^*)^{\psi} \right) \cdot \prod_{i=1}^{\ell} \prod_{\iota=1}^{2} e(\boldsymbol{c}_i, \widetilde{\boldsymbol{b}}_\iota^*)^{y_{i,0,\iota}} e(\boldsymbol{c}_i, \boldsymbol{b}_{2+\iota}^*)^{y_{i,1,\iota}}$$
$$= \prod_{i \in I} g_T^{\alpha_i (s_i + (\delta + \psi) s'_i)} \cdot \prod_{i=1}^{\ell} g_T^{\pi \beta_{i,0} s_i + \beta_{i,1} s'_i} = g_T^{\sum_{i \in I} \alpha_i (s_i + (\delta + \psi) s'_i)} \cdot g_T^{\sum_{i=1}^{\ell} (\pi \beta_{i,0} s_i + \beta_{i,1} s'_i)}$$
$$= g_T^{s_0}, \text{ since } \sum_{i \in I} \alpha_i s_i = s_0 \text{ and } \sum_{i \in I} \alpha_i s'_i = \sum_{i=1}^{\ell} \beta_{i,0} s_i = \sum_{i=1}^{\ell} \beta_{i,1} s'_i = 0.$$

Comparison with the MA-ABS Scheme in [48] Okamoto-Takashima [48] gave a fully secure (non-decentralized) MA-ABS scheme on the DPVS framework. In their scheme, a signature (SIG) associated with a policy of size ℓ consists of $(\ell + 2)$ components, $(s_0^*, \ldots, s_{\ell+1}^*)$, which are categorized into three roles. The first one, $s_0^* \in \mathbb{V}_0$ (for $t = 0$), is for embedding/recovering a secret, the second, $(s_1^*, \ldots, s_\ell^*)$, for secret shares on the policy (access structure), and the last, $s_{\ell+1}^* \in \mathbb{V}_{d+1}$ (for $t = d + 1$), is for embedding/verifying the hashed value, $H_2(m, \mathbb{S})$. The secret share components, $(s_1^*, \ldots, s_\ell^*)$, are 7-dimensional ($7 = 2 + 2 + 2 + 1$), where the first 2-dimensional part is the real-encoding part (real part, for short) for shared secrets, the second

the hidden part for semi-functional signatures, the third the signature randomness part, and the last is the verification text (VT) randomness part.

In the DMA setting, we cannot use special (central) spaces, $\mathbb{V}_0$ and $\mathbb{V}_{d+1}$. Instead, we should distribute the roles of these spaces into the secret share components, $(s_1^*, \ldots, s_\ell^*)$. As a result, these components become 13-dimensional ($13 = 6 + 4 + 2 + 1$), where the real part (hidden part, resp.) is expanded to 6-dimensions (4-dimensions, resp.) (see the figure below). The 6-dimensional real part consists of 2 dimensions to distribute the role of $\mathbb{V}_0$, 2 dimensions for secret shares, and 2 dimensions to distribute the role of $\mathbb{V}_{d+1}$. We also use additional 2 dimensions in the hidden part to execute the *swapping* technique in the security proof.



5.4 Security of the Proposed DMA-ABS

Theorem 1. *The proposed DMA-ABS scheme is perfectly private.*

Theorem 2. *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,

$$\mathsf{Adv}^{\mathsf{DMA\text{-}ABS,UF}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu_S} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h}}(\lambda) + \sum_{h=1}^{\nu_H} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3\text{-}h\text{-}2}}(\lambda) \right) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_4}(\lambda) + \epsilon,$$

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

The (standard) DLIN assumption is given in Appendix 4. Theorems 1 and 2 are immediately obtained from Theorems 3 and 4 (in Appendix C.4) on the proposed DMA-FS, whose proofs are also given in Appendix C.4.

5.5 Performance

In this section, we compare the efficiency and security of the proposed DMA-ABS scheme with the existing MA-ABS schemes in the standard model (instantiation 2 in [43] and MA-ABS in [48]) as well as the ABS scheme in the generic group model (instantiation 3 in [43]) 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 1, 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 [38]). λ is the security parameter (e.g., 128).

Table 1. Comparison with the Existing MA-ABS Schemes

	MPR10 [43] Instantiation 3	MPR10 [43] Instantiation 2	OT11 [48]	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
Authority Corruption Type	strong	strong	weak	weak
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

6 Concluding Remarks

We presented the first DMA-ABS scheme, in which no central authority and no trusted setup are required. An adaptively secure DMA-FE scheme with no trusted setup was also presented.

One of the most important remaining problems in this paper is to construct a DMA-ABS (and DMA-FE) scheme in the standard model (without random oracles). It would be also important to realize a DMA-ABS (and DMA-FE) scheme with no trusted setup in a stronger authority corruption model (like that in [43]), and to introduce a revocation mechanism in a DMA-ABS scheme.

References

1. Beimel, A., Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
2. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 108–125. Springer Heidelberg (2009)
3. Belenkiy, M., Chase, M., Kohlweiss, M., Lysyanskaya, A.: P-signatures and noninteractive anonymous credentials. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 356–374. Springer Heidelberg (2008)
4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Press (2007)
5. Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer Heidelberg (2004)

6. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer Heidelberg (2004)
7. Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer Heidelberg (2005)
8. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
9. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer Heidelberg (2001)
10. Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer Heidelberg (2008)
11. Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)
12. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer Heidelberg (2007)
13. Boyen, X.: Mesh signatures. In: Naor, M. (ed.) EUROCRYPT 2007, LNCS, vol. 4515, pp. 210–227. Springer Heidelberg (2007)
14. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer Heidelberg (2006)
15. Camenisch, J., Groß, T.: Efficient attributes for anonymous credentials. In: CCS 2008. pp.345–356. ACM (2008)
16. Canetti, R., Halevi S., Katz J.: Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer Heidelberg (2004)
17. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optinal anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer Heidelberg (2001)
18. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer Heidelberg (2004)
19. Chase, M.: Multi-authority attribute based encryption. TCC, LNCS, pp. 515–534, Springer Heidelberg (2007).
20. Chase, M. and Chow, S.: Improving privacy and security in multi-authority attribute-based encryption, ACM Conference on Computer and Communications Security, pp. 121–130, ACM (2009).
21. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. In: CACM, vol. 28 (10), pp. 1030–1044. ACM (1985)
22. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, pp. 360–363. Springer Heidelberg (2001)
23. Escala, A., Herranz, J., Morillo, P.: Revocable attribute-based signatures with adaptive security in the standard model, AFRICACRYPT 2011. LNCS, vol. 6737, pp. 224–241. Springer Heidelberg (2011)
24. Estibals, N.: Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves, IACR ePrint Archive: Report 2010/371 (2010).
25. SECURE HASH STANDARD, FIPS PUB 180-1, 180-2, NIST, USA (1995,2002)
26. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer Heidelberg (2006)
27. Gentry, C., Halevi, S.: Hierarchical identity-based encryption with polynomially many levels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 437–456. Springer Heidelberg (2009)
28. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer Heidelberg (2002)
29. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communication Security 2006, pp. 89–98, ACM (2006)
30. S. Guo and Y. Zeng: Attribute-based signature scheme, In: ISA 08, pp. 509–511. IEEE (2008)
31. D. Khader: Attribute based group signatures, ePrint, IACR, `http://eprint.iacr.org/2007/159`.
32. D. Khader: Attribute based group signature with revocation. ePrint, IACR, `http://eprint.iacr.org/2007/241`
33. ISO/IEC 15946-5, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation (2009).
34. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer Heidelberg (2008)

35. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. ePrint, IACR, http://eprint.iacr.org/2011/490
36. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer Heidelberg (2010)
37. Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer Heidelberg (2010)
38. Lewko, A.B., Waters, B.: Decentralizing Attribute-Based Encryption, EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer Heidelberg (2011)
39. Li, J., Au, M.H., Susilo, W., Xie, D., Ren. K.: Attribute-based signature and its application, In: ASIACCS 2010, pp. 60–69. ACM (2010)
40. Li, J., Kim, K.: Attribute-based ring signatures. ePrint, IACR, http://eprint.iacr.org/2008/394
41. H. Lin, Z. Cao, X. Liang, and J. Shao.: Secure threshold multi authority attribute based encryption without a central authority, INDOCRYPT, LNCS, vol. 5365, pp. 426–436, Springer Heidelberg (2008).
42. Maji, H., Prabhakaran, M., Rosulek, M.: Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. ePrint, IACR, http://eprint.iacr.org/2008/328
43. Maji, H., Prabhakaran, M., Rosulek, M.: Attribute-Based Signatures. CT-RSA 2011, LNCS 6558, pp. 376–392 (2011).
44. S. Müller, S. Katzenbeisser, and C. Eckert.; On multi-authority ciphertext-policy attribute-based encryption, Bull. Korean Math Soc. 46, No.4, pp. 803–819 (2009).
45. Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 57–74, Springer Heidelberg (2008)
46. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, In: ASIACRYPT 2009, Springer Heidelberg (2009)
47. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer Heidelberg (2010). Full version is available at http://eprint.iacr.org/2010/563
48. Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model, In: PKC 2011, LNCS, vol. 6571, pp. 35–52. Springer Heidelberg (2011)
49. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communication Security 2007, pp. 195–203, ACM (2007)
50. Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. In: ACM Conference on Computer and Communication Security 2006, pp. 99–112, ACM, (2006)
51. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer Heidelberg (2001)
52. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer Heidelberg (2005)
53. Shacham, H., Waters, B.: Efficient ring signatures without random oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 166–180. Springer Heidelberg (2007)
54. Shahandashti, S.F., Safavi-Naini, R.: Threshold attribute-based signatures and their application to anonymous credential systems. In: Preneel B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 198–216. Springer Heidelberg (2009)
55. Shi, E., Waters, B.: Delegating capability in predicate encryption systems. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldørsson, M.M., Ingølfsdøttir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560–578. Springer Heidelberg (2008)
56. Waters, B.: Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS, vol. 3152, pp.443–459. Springer Verlag, (2005)
57. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: PKC 2011, LNCS, vol. 6571, pp. 53–70. Springer Heidelberg (2011)
58. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer Heidelberg (2009)
59. Yang, P., Cao, Z., Dong, X.: Fuzzy identity based signature (2008). ePrint, IACR, http://eprint.iacr.org/2008/002.

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 [43]. 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 [43]) 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 $\mathsf{ABS.Sign}$ in page 12 of [43]. 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).

B Anonymous Credentials

The notion of anonymous credentials (ACs) [2, 3, 15, 17, 18, 21] provides a functionality for users to demonstrate anonymously possession of attributes, but the goals of ACs and (DMA-)ABS differ in several points.

First of all, (DMA-)ABS is a class of signatures, which are non-interactive primitives and can be used as transferable digital evidence, while ACs are typically (non-transferable) interactive protocols to prove the possession of credentials. Nevertheless, chosen-message-attack secure signatures can be employed to construct an interactive protocol by signing a random number challenge from a verifier, and non-interactive ACs [3] have been proposed. So, we will focus on the other properties of (DMA-)ABS and ACs rather than the difference in signatures and interactive protocols. Since AC considers multiple authorities, we will compare DMA-ABS and AC hereafter.

The first difference between DMA-ABS and ACs is the number of attributes for which an attribute authority is responsible. In DMA-ABS, each authority can issue credentials (or keys) to users for an unbounded number of attributes (e.g., $q = O(2^{\lambda})$ many attributes, where λ is the security parameter), and a user reveals only a predicate on the attributes that the user possesses, rather than the individual attributes themselves. In contrast, an authority in ACs is typically considered to be responsible for only a single attribute. Therefore, the public key size increases linearly with the number of attributes in ACs, while the size in DMA-ABS increases with the number of authorities. Camenisch and Groß [15] introduce an AC system with an

unbounded number of attributes for an authority, but the admissible predicates are limited to a single level of disjunctions or conjunctions of attributes, whereas more general predicates are typically available in our DMA-ABS.

The second difference is the anonymity when a user registers with multiple authorities (or requests multiple authorities to issue credentials/keys with attributes). In ACs the multiple registrations of a user cannot be linked to each other, while they can be linked in DMA-ABS schemes. For example, in this paper a user provides the identity of the user to multiple authorities. However, this information in the registration (key-issuing) stage is the only information that DMA-ABS leaks, and no privacy is revealed after the registration stage, e.g., even colluding authorities cannot identify the user when a user proves some predicate on the credentials in DMA-ABS. This provides sufficient anonymity in many applications.

As a summary, 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.

C Decentralized Multi-Authority Functional Signatures

C.1 Definitions of DMA-FS

Definition 10 (Decentralized Multi-Authority FS : DMA-FS). *A decentralized multi-authority FS scheme consists of the following algorithms/protocols.*

$\mathsf{GSetup}, \mathsf{ASetup}, \mathsf{AttrGen}$ *are the same as those for DMA-ABS 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 $\mathsf{accept} := 1$ or $\mathsf{reject} := 0$.*

C.2 Security Definition of DMA-FS

The definition of perfect privacy for the decentralized multi-authority FS is essentially the same as that of the ABS given in [48].

Definition 11 (Perfect Privacy of DMA-FS). *A DMA-FS 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 $\{\mathsf{usk}_{t,1} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_1, \vec{x}_{t,1})\}_{(t,\vec{x}_{t,1})\in\Gamma_1}$ and $\{\mathsf{usk}_{t,2} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}_2, \vec{x}_{t,2})\}_{(t,\vec{x}_{t,2})\in\Gamma_2}$, 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-FS 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 $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)$ for arbitrary $\Gamma := \{(t, \vec{x}_t)\}$ which satisfies $\mathbb{S}$, then $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}, m, \mathbb{S})$. Return σ.

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

Definition 12 (Unforgeability of DMA-FS). *For an adversary, we define* $\mathsf{Adv}^{\mathsf{DMA\text{-}FS,UF}}_{\mathcal{A}}(\lambda)$ *to be the success probability in the following experiment for any security parameter* λ*. A DMA-FS scheme is existentially unforgeable if the success probability of any polynomial-time adversary is negligible:*

1. *Run* $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$ *and give* gparam *to the adversary* $\mathcal{A}$*. For authorities* $t \in T$*, run* $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam})$ *and give* $\{\mathsf{apk}_t\}_{t\in T}$ *to* $\mathcal{A}$*. Adversary* $\mathcal{A}$ *specifies a set* $T' \subset T$ *of corrupt attribute authorities, and gets* $\{\mathsf{ask}_t\}_{t\in T'}$*.*
2. *The adversary* $\mathcal{A}$ *is given access to oracles* $\mathsf{AttrGen}$ *and* AltSig *over* $S := T \setminus T'$*.*
3. *At the end, the adversary outputs* $(m', \mathbb{S}', \sigma')$*.*

Let $\Gamma_{\mathsf{gid}_i} := \{(t \in S, \vec{x}_t)\}$ *(*$i = 1, \ldots, \nu_H$*) queried to the* $\mathsf{AttrGen}$ *oracle with* gid_i*. We say the adversary succeeds if* $(m', \mathbb{S}')$ *was never queried to the* AltSig *oracle,* $\mathbb{S}'$ *does not accept* Γ_{gid_i} *with any* gid_i *(*$i = 1, \ldots, \nu_H$*), queried to the* $\mathsf{AttrGen}$ *oracle,* $\mathbb{S}'$ *is specified over* S*, and* $\mathsf{Ver}(\mathsf{pk}, m', \mathbb{S}', \sigma') = 1$*.*

C.3 Proposed DMA-FS 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 will show how to relax the restriction in Appendix F. 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 Section 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 $\boldsymbol{v}$ in N-dimensional $\mathbb{V}$, $X(\boldsymbol{v})$ denotes $\sum_{i=1,j=1}^{N,N} \chi_{i,j}\phi_{i,j}(\boldsymbol{v})$ using canonical maps $\{\phi_{i,j}\}$ (Definition 2). Similarly, for matrix $(\vartheta_{i,j}) := (X^{-1})^{\mathrm{T}}$, $(X^{-1})^{\mathrm{T}}(\boldsymbol{v}) := \sum_{i=1,j=1}^{N,N} \vartheta_{i,j}\phi_{i,j}(\boldsymbol{v})$. It holds that $e(X(\boldsymbol{x}), (X^{-1})^{\mathrm{T}}(\boldsymbol{y})) = e(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}$.

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

$G_0 := H_1(0^\lambda) \in \mathbb{G}$, $G_1 := H_1(0^{\lambda-1}, 1) \in \mathbb{G}$, $G_2 := H_1(0^{\lambda-2}, 1, 0) \in \mathbb{G}$, $g_T := e(G_0, G_1)$.

$\mathsf{ASetup}(\mathsf{gparam}, t)$: $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5n_t + 3, \mathsf{param}_{\mathbb{G}})$,
$X_t \xleftarrow{\mathsf{U}} GL(5n_t + 3, \mathbb{F}_q)$,
$\boldsymbol{b}_{t,\iota} := X_t((0^{\iota-1}, G_0, 0^{5n_t+3-\iota}))$, $\boldsymbol{b}^*_{t,\iota} := (X_t^{\mathrm{T}})^{-1}((0^{\iota-1}, G_1, 0^{5n_t+3-\iota}))$ for $\iota = 1, \ldots, 5n_t + 3$,

$\widetilde{\boldsymbol{b}}^*_{t,\iota} := (X_t^{\mathrm{T}})^{-1}\,(($ $\overbrace{\quad 0^{\iota-1},\ G_2,\ 0^{n_t-\iota},\quad}^{n_t}$ $\overbrace{\quad 0^{3n_t+2},\quad}^{3n_t+2}$ $\overbrace{\quad \widetilde{\varphi}_{t,\iota,1}G_1,..,\widetilde{\varphi}_{t,\iota,n_t}G_1,\quad}^{n_t}$ $\overbrace{\quad 0\quad}^{1}$ $))$,

where $\vec{\widetilde{\varphi}}_{t,\iota} := (\widetilde{\varphi}_{t,\iota,1},\ldots,\widetilde{\varphi}_{t,\iota,n_t}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, for $\iota = 1,\ldots,n_t$,

$\mathbb{B}_t := (\boldsymbol{b}_{t,1},\ldots,\boldsymbol{b}_{t,5n_t+3})$, $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1},\ldots,\boldsymbol{b}^*_{t,5n_t+3})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},\ldots,\boldsymbol{b}_{t,2n_t+2},\boldsymbol{b}_{t,5n_t+3})$,

$\widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1},\ldots,\widetilde{\boldsymbol{b}}^*_{t,n_t},\boldsymbol{b}^*_{t,n_t+1},\ldots,\boldsymbol{b}^*_{t,2n_t+2},\boldsymbol{b}^*_{t,4n_t+3},\ldots,\boldsymbol{b}^*_{t,5n_t+2})$,

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 $\iota = 1,..,n_t$.

$\mathsf{AttrGen}(\mathsf{gparam},\ t,\ \mathsf{ask}_t,\ \mathsf{gid},\ \vec{x}_t := (x_{t,1},\ldots,x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ such that $x_{t,1} := 1)$:

$G_{\mathsf{gid}} := H_1(\mathsf{gid})$, $\vec{\varphi}_t := (\varphi_{t,1},\ldots,\varphi_{t,n_t}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$,

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

$\underbrace{0^{2n_t},}_{2n_t}$ $\overbrace{\quad \varphi_{t,1}G_1,..,\varphi_{t,n_t}G_1,\quad}^{n_t}$ $\overbrace{0\quad}^{1}$ $))$,

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

$I \subseteq \{i \in \{1,\ldots,\ell\} |\ [\rho(i) = (t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i\cdot\vec{x}_t = 0]$

$\vee\ [\rho(i) = \neg(t,\vec{v}_i) \wedge (t,\vec{x}_t) \in \Gamma \wedge \vec{v}_i\cdot\vec{x}_t \neq 0]\ \}$,

$\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $\psi_i := \psi$ if $i \in I$, $\psi_i := 0$ if $i \notin I$ for $i = 1,\ldots,\ell$,

for $i = 1,\ldots,\ell$, $\zeta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\beta_{i,0}),(\beta_{i,1}) \xleftarrow{\mathsf{U}} \{(\beta_1,\ldots,\beta_\ell) \mid \sum_{i=1}^{\ell}\beta_i M_i = \vec{0}\}$,

$\boldsymbol{s}^*_i := \gamma_i\cdot\boldsymbol{k}^*_t + \sum_{\iota=1}^{n_t}\left(y_{i,0,\iota}\widetilde{\boldsymbol{b}}^*_{t,\iota} + (\psi_i x_{t,\iota}+y_{i,1,\iota})\boldsymbol{b}^*_{t,n_t+\iota}\right) + \zeta_i\left(\boldsymbol{b}^*_{t,2n_t+1} + H_2(m,\mathbb{S})\boldsymbol{b}^*_{t,2n_t+2}\right) + \boldsymbol{r}^*_i$,

where $\boldsymbol{r}^*_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle\boldsymbol{b}^*_{t,4n_t+3},..,\boldsymbol{b}^*_{t,5n_t+2}\rangle$, and $\gamma_i,\vec{y}_{i,j} := (y_{i,j,1},..,y_{i,j,n_t})$ for $j = 0,1$,

are defined as

if $i \in I \wedge \rho(i) = (t,\vec{v}_i)$, $\gamma_i := \alpha_i$, $\vec{y}_{i,j} \xleftarrow{\mathsf{U}} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\}$,

if $i \in I \wedge \rho(i) = \neg(t,\vec{v}_i)$, $\gamma_i := \alpha_i/(\vec{v}_i\cdot\vec{x}_t)$, $\vec{y}_{i,j} \xleftarrow{\mathsf{U}} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = \beta_{i,j}\}$,

if $i \notin I \wedge \rho(i) = (t,\vec{v}_i)$, $\gamma_i := 0$, $\vec{y}_{i,j} \xleftarrow{\mathsf{U}} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = 0 \wedge y_{i,j,1} = \beta_{i,j}\}$,

if $i \notin I \wedge \rho(i) = \neg(t,\vec{v}_i)$, $\gamma_i := 0$, $\vec{y}_{i,j} \xleftarrow{\mathsf{U}} \{\vec{y}_{i,j} \mid \vec{y}_{i,j}\cdot\vec{v}_i = \beta_{i,j}\}$,

return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}^*_1,\ldots,\boldsymbol{s}^*_\ell)$.

$\mathsf{Ver}(\mathsf{gparam},\ \{\mathsf{apk}_t\},\ m,\ \mathbb{S} := (M,\rho),\vec{\boldsymbol{s}}^*)$:

$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1,\ldots,s_\ell)^{\mathrm{T}} := M\cdot\vec{f}^{\mathrm{T}}$, $s_0 := \vec{1}\cdot\vec{f}^{\mathrm{T}}$,

$\vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r$ 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 $i = 1, \ldots, \ell$,
if $\rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ such that $v_{i,n_t} \neq 0)$, $\theta_i, \theta'_i, \theta''_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_i := (\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i}^{n_t}, \overbrace{\theta''_i(H_2(m,\mathbb{S}), -1)}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

if $\rho(i) = \neg(t, \vec{v}_i)$, $\theta''_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

$$\boldsymbol{c}_i := (\overbrace{s_i\vec{v}_i}^{n_t}, \overbrace{s'_i\vec{v}_i}^{n_t}, \overbrace{\theta''_i(H_2(m,\mathbb{S}), -1)}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

$c_{d+1} := g_T^{s_0}$, 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 $\Gamma := \{(t, \vec{x}_t) \in \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\}$,

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

C.4 Security of the Proposed DMA-FS

Theorem 3. *The proposed DMA-FS scheme is perfectly private.*

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

$\mathsf{AltSig}(\mathsf{gparam}, \{\mathsf{apk_t}, \mathsf{ask}_t\}, m, \mathbb{S})$
$\widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $(\xi_i), (\xi'_i) \xleftarrow{\mathsf{U}} \{(\xi_1, \ldots, \xi_\ell) \mid \sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\}$,
for $i = 1, \ldots, \ell$,

$$\left.\begin{array}{l}
\text{if } \rho(i) = (t, \vec{v}_i), \\
\quad \text{then } (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\mathsf{U}} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0} \cdot \vec{v}_i = \vec{z}_{i,1} \cdot \vec{v}_i = 0, \ z_{i,0,1} = \xi_i, \ z_{i,1,1} = \widetilde{\delta}\xi'_i\}, \\
\text{if } \rho(i) = \neg(t, \vec{v}_i), \\
\quad \text{then } (\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\mathsf{U}} \{\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0} \cdot \vec{v}_i = \xi_i, \ \vec{z}_{i,1} \cdot \vec{v}_i = \widetilde{\delta}\xi'_i\},
\end{array}\right\} \quad (1)$$

$$\boldsymbol{s}_i^* := (\overbrace{\vec{z}_{i,0}, \vec{z}_{i,1}}^{2n_t}, \overbrace{\zeta_i(1, H_2(m,\mathbb{S}))}^{2}, \overbrace{0^{2n_t}}^{2n_t}, \overbrace{\vec{\sigma}_i}^{n_t}, \overbrace{0}^{1})_{\mathbb{B}_i^*} \text{ where } \zeta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, \ \vec{\sigma}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t},$$

return $\vec{\boldsymbol{s}}^* := (\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*)$.

Remark: Theorem 3 implies that AltSig defined above is equivalent to AltSig defined just after Definition 11, 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 $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$, $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t)$, all messages m, all attribute sets Γ associated with gid, all signing keys $\{\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} \xleftarrow{\mathsf{R}} \mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \mathsf{gid}, \vec{x}_t)\}$, 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-FS scheme, $(\boldsymbol{s}_1^*, \ldots, \boldsymbol{s}_\ell^*) \xleftarrow{\mathsf{R}} \mathsf{Sig}(\mathsf{gparam},\ \{\mathsf{apk_t}, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}\},\ m,\ \mathbb{S})$ are expressed by

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

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

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

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

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

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

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

$$
\begin{aligned}
&\Big((\alpha'_1 + \pi\beta_{1,0},\ \widetilde{\delta}\alpha'_1 + \beta_{1,1}), \ldots, (\alpha'_\ell + \pi\beta_{\ell,0},\ \widetilde{\delta}\alpha'_\ell + \beta_{\ell,1})\Big)\\
&\qquad \text{s.t.}\quad \widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\quad (\beta_{i,0}), (\beta_{i,1}) \xleftarrow{\mathsf{U}} \{(\beta_i)\ \mid\ \textstyle\sum_{i=1}^{\ell} \beta_i M_i = \vec{0}\}\ \text{ and}\\
&((\xi_1,\ \widetilde{\delta}\xi'_1), \ldots, (\xi_\ell,\ \widetilde{\delta}\xi'_\ell))\\
&\qquad \text{s.t.}\quad \widetilde{\delta} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\quad (\xi_i), (\xi'_i) \xleftarrow{\mathsf{U}} \{(\xi_i)\ \mid\ \textstyle\sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\ \},
\end{aligned}
$$

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 4. *The proposed DMA-FS 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,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{DMA\text{-}FS,UF}}_{\mathcal{A}}(\lambda) \leq\ & \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \textstyle\sum_{h=1}^{\nu_S} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h}}(\lambda) \\ & + \textstyle\sum_{h=1}^{\nu_H} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3\text{-}h\text{-}2}}(\lambda)\right) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_4}(\lambda) + \epsilon,\end{aligned}$$

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

Proof Outline of Theorem 4: As mentioned in Section 5.2, secret signing keys and verification texts in our DMA-FS are the counterparts of secret decryption keys and ciphertexts in DMA-FE. Based on this correspondence, we follow the dual system encryption methodology proposed by Waters [58], 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.

Table 2. Outline of Game Descriptions: 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.

	chalk.	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.

We denote verification text by $\vec{\boldsymbol{c}} := (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell)$, and keys by $\vec{\boldsymbol{k}}^* := (\boldsymbol{k}^*_t)_{(t,\vec{x}_t)\in\Gamma}$ 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, $\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}$ (with attributes $(t, \vec{x}_t)$), is expressed by Eq. (2), and a normal signature, $\vec{\boldsymbol{s}}^{*\,\mathsf{norm}}$ (with access structure $\mathbb{S}$) is expressed by Eq. (4), which are the correct forms of the secret key and signatures of the proposed DMA-FS scheme, respectively. Similarly, a normal verification text (with $\mathbb{S}$), $\vec{\boldsymbol{c}}^{\mathsf{norm}}$, is expressed by Eq. (5), and normal form of (a part of) public key $\widetilde{\boldsymbol{b}}^{\mathsf{norm}}_{t,\iota}$ is given in Eq. (3). A temporal verification text is expressed by Eq. (6). A semi-functional signature, $\vec{\boldsymbol{s}}^{\mathsf{semi}}$, is expressed by Eq. (7). A pre-semi-functional verification text, $\vec{\boldsymbol{c}}^{\mathsf{pre\text{-}semi}}$, is expressed by Eq. (8) and a pre-semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{pre\text{-}semi}}$, is expressed by Eq. (9). A semi-functional verification text, $\vec{\boldsymbol{c}}^{\mathsf{semi}}$, is expressed by Eq. (10) and a semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{semi}}$, is expressed by Eq. (11). A non-functional verification text, $\vec{\boldsymbol{c}}^{\mathsf{non\text{-}f}}$, is expressed by Eq. (13).

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 $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ 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 7). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 1).

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 8 and 3).

We then show that Game 3-$(h-1)$-4 can be conceptually changed to Game 3-h-1 (Lemma 9), 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, $(\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}, \vec{\boldsymbol{c}}^{\,\mathsf{semi}})$, are equivalent to normal key and pre-semi-functional verification text, $(\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}, \vec{\boldsymbol{c}}^{\,\mathsf{pre\text{-}semi}})$, 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 $r''_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for some coefficient vector in $\vec{\boldsymbol{c}}^{\,\mathsf{semi}}$. This change of coefficient vectors can be done conceptually since zero vector 0^{n_t} is used for the corresponding part in $\vec{\boldsymbol{k}}^{*\,\mathsf{norm}}$.

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 10 and 2).

We then show that Game 3-h-2 can be conceptually changed to Game 3-h-3 (Lemma 11), 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 $r''_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 6.

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 12 and 5).

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 13 and 4).

We then show that Game 4 can be conceptually changed to Game 5 (Lemma 14) 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 4, 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:

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

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

$$\widetilde{\boldsymbol{b}}^*_{t,\iota} := (\ \overbrace{\pi\vec{e}_{t,\iota}}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{0^2}^{2},\ \overbrace{0^{n_t}}^{2n_t},\ \overbrace{\boxed{0^{n_t}}}^{n_t},\ \overbrace{\vec{\widetilde{\varphi}}_{t,\iota}}^{n_t},\ \overbrace{0}^{1}\ )_{\mathbb{B}^*_t} \text{ for } \iota = 1,\ldots,n_t, \tag{3}$$

where $\pi \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\widetilde{\varphi}}_{t,\iota} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, 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:

$$\boldsymbol{s}_i^{(h)*} := (\ \overbrace{\vec{w}_i^{(h)}}^{n_t},\ \overbrace{\vec{w}_i'^{(h)}}^{n_t},\ \overbrace{\zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)}))}^{2},\ \overbrace{0^{n_t}}^{2n_t},\ \overbrace{\boxed{0^{n_t}}}^{n_t},\ \overbrace{\vec{\sigma}_i}^{n_t},\ \overbrace{0}^{1}\ )_{\mathbb{B}^*_t}, \tag{4}$$

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

$$\left.\begin{array}{l} \text{if } \rho(i) = (t, \vec{v}_i), \\ \quad \boldsymbol{c}_i := (\ \overbrace{\boxed{s_i}\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\ \overbrace{\boxed{0^{2n_t}}}^{2n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t}, \\ \text{if } \rho(i) = \neg(t, \vec{v}_i),\ \ \boldsymbol{c}_i := (\ \underbrace{\boxed{s_i}\vec{v}_i}_{n_t},\ \underbrace{s_i'\vec{v}_i}_{n_t},\ \underbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}_{2},\ \underbrace{\boxed{0^{2n_t}}}_{2n_t},\ \underbrace{0^{n_t}}_{n_t},\ \underbrace{\eta_i}_{1}\ )_{\mathbb{B}_t}, \\ c_{d+1} := g_T^{s_0}, \end{array}\right\} \tag{5}$$

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

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:

$$\left.\begin{array}{l} \text{if } \rho(i) = (t, \vec{v}_i), \\ \quad \boldsymbol{c}_i := (\ \overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\ \overbrace{0^{n_t}}^{2n_t},\ \overbrace{\boxed{\vec{z}_i}}^{n_t},\ \overbrace{0^{n_t}}^{1},\ \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t}, \\ \text{if } \rho(i) = \neg(t, \vec{v}_i),\ \ \boldsymbol{c}_i := (\ \underbrace{s_i\vec{v}_i}_{n_t},\ \underbrace{s_i'\vec{v}_i}_{n_t},\ \underbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}_{2},\ \underbrace{0^{n_t}}_{2n_t},\ \underbrace{\boxed{\vec{z}_i}}_{n_t},\ \underbrace{0^{n_t}}_{1},\ \underbrace{\eta_i}_{1}\ )_{\mathbb{B}_t}, \end{array}\right\} \tag{6}$$

where $\vec{z}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, 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 $(m^{(h)}, \mathbb{S}^{(h)})$ is:

$$\boldsymbol{s}_i^{(h)*} := (\ \overbrace{\vec{w}_i^{(h)}}^{n_t},\ \overbrace{\vec{w}_i'^{(h)}}^{n_t},\ \overbrace{\zeta_i(1, H_2(m^{(h)}, \mathbb{S}^{(h)}))}^{2},\ \overbrace{0^{n_t}}^{2n_t},\ \overbrace{\boxed{\vec{u}_i^{(h)}}}^{n_t},\ \overbrace{\vec{\sigma}_i}^{1},\ \overbrace{0}^{}\ )_{\mathbb{B}_t^*}, \tag{7}$$

where $\vec{u}_i^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, 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:

$$\left.\begin{array}{l}
\text{If } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i := (\ \overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\\
\qquad \overbrace{\boxed{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t}}^{2n_t},\ \overbrace{r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{1},\ \overbrace{\eta_i}^{}\ )_{\mathbb{B}_t},\\
\text{If } \rho(i) = \neg(t, \vec{v}_i),\\
\qquad \boldsymbol{c}_i := (\ \overbrace{s_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\ \overbrace{\boxed{r_i\vec{v}_i\cdot Z_t}}^{2n_t},\ \overbrace{r_i'\vec{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{1},\ \overbrace{\eta_i}^{}\ )_{\mathbb{B}_t},
\end{array}\right\} \tag{8}$$

where $\vec{g} \xleftarrow{\mathsf{U}} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1}\cdot\vec{g}^{\mathrm{T}} = 0\}, \vec{g}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r_i := M_i\cdot\vec{g}^{\mathrm{T}}, r_i' := M_i\cdot\vec{g}'^{\mathrm{T}}, Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q),\ \omega_i, \omega_i' \xleftarrow{\mathsf{U}} \mathbb{F}_q$, 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 $t \in S$ is:

$$\boldsymbol{k}_t^{(h)*} := (\ \overbrace{\vec{x}_t^{(h)}}^{n_t},\ \overbrace{\delta^{(h)}\vec{x}_t^{(h)}}^{n_t},\ \overbrace{0^2}^{2},\ \overbrace{\boxed{\tau^{(h)}\vec{x}_t^{(h)}\cdot U_t}}^{2n_t},\ \overbrace{0^{n_t}}^{n_t}\ \overbrace{\vec{\varphi}_t^{(h)}}^{1},\ \overbrace{0}^{}\ )_{\mathbb{B}_t^*} \tag{9}$$

where $\tau^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$ used in Eq. (8), 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:

$$\left.\begin{array}{l}
\text{if } \rho(i) = (t, \vec{v}_i),\ \ \boldsymbol{c}_i := (\ \overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\\
\qquad (\overbrace{\boxed{r_i''}\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t}^{2n_t},\ \overbrace{r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{1},\ \overbrace{\eta_i}^{}\ )_{\mathbb{B}_t},\\
\text{if } \rho(i) = \neg(t, \vec{v}_i),\\
\qquad \boldsymbol{c}_i := (\ \overbrace{s_i\vec{v}_i}^{n_t},\ \overbrace{s_i'\vec{v}_i}^{n_t},\ \overbrace{\theta_i''(H_2(m', \mathbb{S}'), -1)}^{2},\ \overbrace{\boxed{r_i''}\vec{v}_i\cdot Z_t}^{2n_t},\ \overbrace{r_i'\vec{v}_i}^{n_t},\ \overbrace{0^{n_t}}^{1},\ \overbrace{\eta_i}^{}\ )_{\mathbb{B}_t},
\end{array}\right\} \tag{10}$$

where $\vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r_i'' := M_i \cdot \vec{g}^{\mathrm{T}}$, and the other variables are generated as in Game 3-h-2.

Game 3-h-4 ($h = 1, \ldots, \nu_H$) : 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 $t \in S$ is:

$$\boldsymbol{k}_t^{(h)*} = (\overbrace{\quad \vec{x}_t^{(h)}, \quad}^{n_t} \overbrace{\quad \delta^{(h)}\vec{x}_t^{(h)}, \quad}^{n_t} \overbrace{\quad 0^2, \quad}^{2} \overbrace{\quad \boxed{0^{n_t}, \quad \tau'^{(h)}\vec{x}_t^{(h)}}, \quad}^{2n_t} \overbrace{\quad \vec{\varphi}_t^{(h)}, \quad}^{n_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}_t^*} \tag{11}$$

where $\tau'^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, 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, $\{\widetilde{\boldsymbol{b}}_{t,\iota}^*\}_{\iota=1,\ldots,n_t}$, for $t \in S$ is:

$$\widetilde{\boldsymbol{b}}_{t,\iota}^* := (\overbrace{\quad \pi\vec{e}_{t,\iota}, \quad}^{n_t} \overbrace{\quad 0^{n_t}, \quad}^{n_t} \overbrace{\quad 0^2, \quad}^{2} \overbrace{\quad 0^{n_t}, \boxed{\eta\vec{e}_{t,\iota}}, \quad}^{2n_t} \overbrace{\quad \vec{\widetilde{\varphi}}_{t,\iota}, \quad}^{n_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}_t^*}, \tag{12}$$

where $\eta \xleftarrow{\mathsf{U}} \mathbb{F}_q$, 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, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1}$, for $(m', \mathbb{S}')$ with $\mathbb{S}' := (M, \rho)$ in the final step is:

$$\left.\begin{array}{l}
\text{If } \rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\})\ (v_{i,n_t} \neq 0), \\
\boldsymbol{c}_i := (\overbrace{\quad \boxed{\tilde{s}_i}\vec{e}_{t,1} + \theta_i\vec{v}_i, \quad}^{n_t} \overbrace{\quad s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i, \quad}^{n_t} \overbrace{\quad \theta_i''(H_2(m', \mathbb{S}'), -1), \quad}^{2} \\
\qquad \overbrace{\quad (r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t, \quad r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i, \quad}^{2n_t} \overbrace{\quad 0^{n_t}, \quad}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\
\text{If } \rho(i) = \neg(t, \vec{v}_i), \\
\boldsymbol{c}_i := (\overbrace{\quad \boxed{\tilde{s}_i}\vec{v}_i, \quad}^{n_t} \overbrace{\quad s_i\vec{v}_i, \quad}^{n_t} \overbrace{\quad \theta_i''(H_2(m', \mathbb{S}'), -1), \quad}^{2} \overbrace{\quad r_i\vec{v}_i \cdot Z_t, \quad r_i'\vec{v}_i, \quad}^{2n_t} \overbrace{\quad 0^{n_t}, \quad}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\
c_{d+1} := g_T^{\boxed{s_0}},
\end{array}\right\} \tag{13}$$

where $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, \widetilde{s}_i := M_i \cdot \vec{f}^{\mathrm{T}}$ and $s_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. 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 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}FS,UF}}(\lambda)$ in Game 0, and $\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda), \ldots, \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}4)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda), \mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $1, 2\text{-}h, 3\text{-}h\text{-}1, \ldots, 3\text{-}h\text{-}4, 4, 5$, respectively.

It is obtained that $\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda) = 1/q$ by Lemma 15. We will show eight lemmas (Lemmas 7–14) 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 $h = 1, \ldots, \nu_S$, $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda), \ldots, \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}4)}(\lambda)$ for $h = 1, \ldots, \nu_H$, $\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$ and $\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)$. From these lemmas and Lemmas 1, 2 and 5, we obtain $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DMA\text{-}FS,UF}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) \leq \left|\mathsf{Adv}_{\mathcal{A}}^{(0)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| + \sum_{h=1}^{\nu_S} \left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)\right| + \sum_{h=1}^{\nu_H} \left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda)\right| +$

$\sum_{\iota=1}^{3}\sum_{h=1}^{\nu_H}\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}\iota)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}(\iota+1))}(\lambda)\right|+\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}\nu_H\text{-}4)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)\right|+\left|\mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)\right|$
$+\mathsf{Adv}_{\mathcal{A}}^{(5)}(\lambda)\leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda)+\sum_{h=1}^{\nu_S}\mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2}}(\lambda)+\sum_{h=1}^{\nu_H}\left(\mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}1}}^{\mathsf{P2}}(\lambda)+\mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}1}}^{\mathsf{P3}}(\lambda)\right)+\mathsf{Adv}_{\mathcal{B}_4}^{\mathsf{P2}}(\lambda)+$
$((d+1)\nu_S+2d\nu_H+2d+1)/q\leq \mathsf{Adv}_{\mathcal{E}_1}^{\mathsf{DLIN}}(\lambda)+\sum_{h=1}^{\nu_S}\mathsf{Adv}_{\mathcal{E}_{2\text{-}h}}^{\mathsf{DLIN}}(\lambda)+\sum_{h=1}^{\nu_H}\left(\mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda)+\mathsf{Adv}_{\mathcal{E}_{3\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda)\right)+$
$\mathsf{Adv}_{\mathcal{E}_4}^{\mathsf{DLIN}}(\lambda)+((d+6)\nu_S+(2d+10)\nu_H+3d+11)/q$. This completes the proof of Theorem 4. □

C.5 Structure of Reductions for Theorem 4

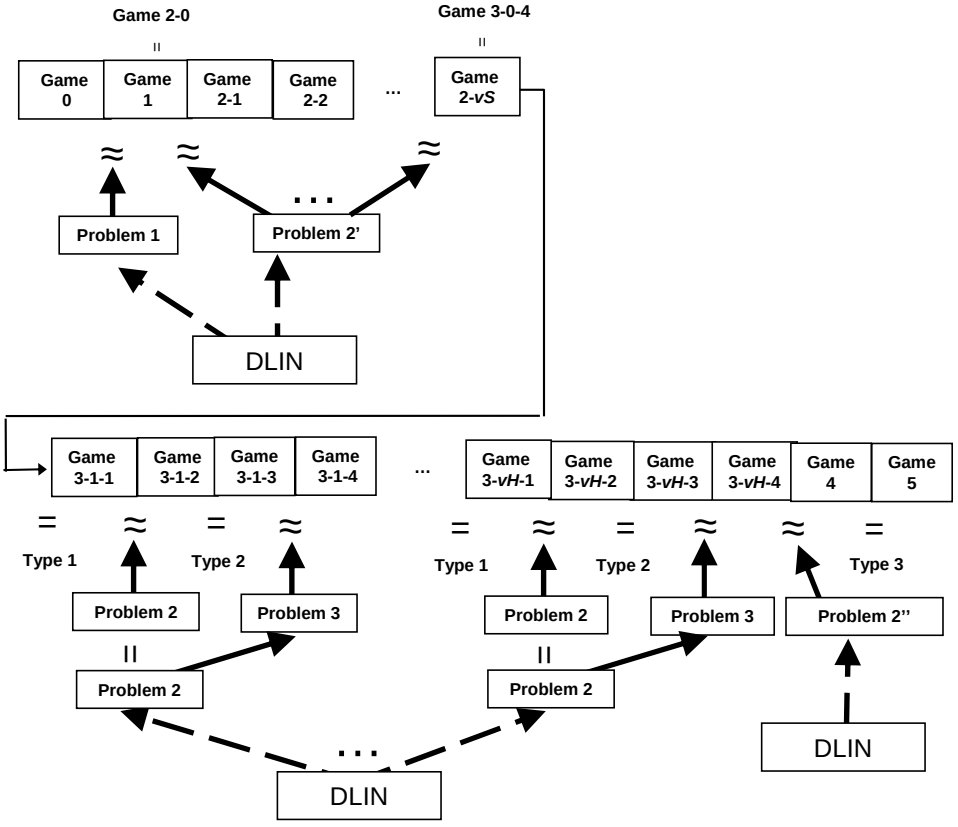


Fig. 1. Structure of Reductions

In Figure 1, an equality between neighboring games indicates 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 12), 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 13, 14, 15, 16, 17, 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 [47]. They are indicated in Figure 1 by dotted arrows.

We show that the intractability of Problems 3 is reduced to that of Problem 2 in Lemmas 16 and 17. Problem 1 is used for evaluating the gap between advantages of adversary in Game 0 and 1 (Lemma 7). 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 10 (resp. Lemma 8, Lemma 13). Problem 3 is used for evaluating the gap of those in Game 3-h-3 and 3-h-4 (Lemma 12). They are indicated in Figure 1 by arrows. The rest of gaps between games are evaluated without computational assumptions (Lemmas 9, 11 and 14).

C.6 Lemmas for the Proof of Theorem 4

We will show fifteen lemmas for the proof of Theorem 4. The proofs of Lemmas 2 and 5 are given in Appendix D. Lemma 1 is proven similarly to Lemma 1 in [47], and Lemma 6 is proven in Appendix C in [47]. We describe random dual orthonormal bases generator $\mathcal{G}_{\mathsf{ob}}$ below, which is used as a subroutine in the following problems.

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

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 13 (Problem 1). *Problem 1 is to guess β, given*

$(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, \boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=2,..,2n_t}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, \vec{n})$, *where*

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic machine* $\mathcal{B}$, *we define the advantage of* $\mathcal{B}$ *as the quantity* $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, \vec{n})\right] - \mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_1(1^\lambda, \vec{n})\right]\right|$.

Lemma 1. *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, $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + (d+5)/q$.

Lemma 1 is proven similarly to Lemma 1 in [47]. □

Definition 14 (Problem 2). *Problem 2 is to guess* β, *given* $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1, \delta G_1) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, \vec{n})$, *where*

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 2,* $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 2. *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, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

Lemma 2 is proven similarly to Lemma 2 in [47]. □

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

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2', $\mathsf{Adv}^{\mathsf{P2}'}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 13.

Lemma 3. *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, $\mathsf{Adv}^{\mathsf{P2}'}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

The proof of Lemma 3 can be reduced to that of Lemma 2. □

Definition 16 (Problem 2"). *Problem 2" is to guess β, given* $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}''}_\beta(1^\lambda, \vec{n})$*, where*

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *For a probabilistic adversary* $\mathcal{B}$, *the advantage of* $\mathcal{B}$ *for Problem 2,* $\mathsf{Adv}^{\mathsf{P2}''}_{\mathcal{B}}(\lambda)$, *is similarly defined as in Definition 13.*

Lemma 4. *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, $\mathsf{Adv}^{\mathsf{P2}''}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

The proof of Lemma 4 can be reduced to that of Lemma 2. □

Definition 17 (Problem 3). *Problem 3 is to guess* β, *given* $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i,\iota}\}_{t=1,\ldots,d;i=1,\ldots,n_t;\iota=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_{\beta}(1^\lambda, \vec{n})$, *where*

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

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. *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 13.*

Lemma 5. *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, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.

Lemma 6 (Lemma 3 in [47]). *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* $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$.

Lemma 7. *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.

Lemma 8. *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, $|\mathsf{Adv}^{(2\text{-}(h-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2\text{-}h}}(\lambda) + 4/q$, *where* $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.

Lemma 9. *For any adversary* $\mathcal{A}$, *for any security parameter* λ, $|\mathsf{Adv}^{(3\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \leq 2d/q$.

Lemma 10. *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 $\mathcal{B}_{3\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{3\text{-}1}(h, \cdot)$.*

Lemma 11. *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 12. *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, $|\mathsf{Adv}^{(3\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3\text{-}h\text{-}2}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{3\text{-}2}(h, \cdot)$.*

Lemma 13. *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(3\text{-}\nu_H\text{-}4)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda)$.*

Lemma 14. *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, $|\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_4}(\lambda)$.*

Lemma 15. *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 5 and Lemmas 7–14 are given in Appendix D.

D Proofs of Lemmas 5 and 7–14

D.1 Proof of Lemma 5

Lemma 5. *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, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Problem 3 is the hybrid of the following Experiment 3-0, 3-1 and 3-2, i.e., $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}^{3\text{-}0}_{\mathcal{B}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 16, 17 and 2, there exist probabilistic machines $\mathcal{C}$ and $\mathcal{E}$, whose running time are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,

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

This completes the proof of Lemma 5. □

Definition 18 (Experiment 3-α ($\alpha = 0, 1, 2$)). *We define Exp-3-α instance generator, $\mathcal{G}_\alpha^{\mathsf{Exp\text{-}3}}(1^\lambda, \vec{n})$, where*

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

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

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

Lemma 16. *For any adversary $\mathcal{B}$, for any security parameter λ,* $\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}0}(\lambda) \to 1\right] = \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}1}(\lambda) \to 1\right]$.

Proof. Let $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$. If we set

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

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

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

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

Lemma 17. *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, for any security parameter λ,* $\left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}1}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}2}(\lambda) \to 1\right]\right| = \mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda)$.

Proof. In order to prove Lemma 17, we construct a probabilistic machine $\mathcal{C}$ 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: $\mathcal{C}$ is given a Problem 2 instance, $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, \boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d;i=1,\ldots,n}, G_0, G_1, \delta G_1)$. $\mathcal{C}$ sets

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

where $\mathcal{C}$ 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 $\mathcal{C}$ 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. $\mathcal{C}$ 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 $\beta' \in \{0,1\}$. $\mathcal{C}$ then outputs $1-\beta'$.

Then,

$$
\begin{array}{rccccccc}
 & \overbrace{\ }^{n_t} & \overbrace{\qquad}^{n_t} & \overbrace{\ }^{2} & \overbrace{\qquad}^{n_t} & \overbrace{\qquad}^{n_t} & \overbrace{\qquad}^{n_t} & \overbrace{\ }^{1} & \\
\boldsymbol{h}^*_{0,t,i} := (\ 0^{n_t}, & \delta\vec{e}_{t,i}, & 0^2, & 0^{n_t}, & 0^{n_t}, & \vec{\delta}_{t,i}, & 0 &)_{\mathbb{B}^*_t}\\
= (\ 0^{n_t}, & 0^{n_t}, & 0^2, & 0^{n_t}, & \delta\vec{e}_{t,i}, & \vec{\delta}_{t,i}, & 0 &)_{\mathbb{D}^*_t},\\
\boldsymbol{h}^*_{1,t,i} := (\ 0^{n_t}, & \delta\vec{e}_{t,i}, & 0^2, & \tau\vec{e}_{t,i}\cdot U_t, & 0^{n_t}, & \vec{\delta}_{t,i}, & 0 &)_{\mathbb{B}^*_t}\\
= (\ 0^{n_t}, & 0^{n_t}, & 0^2, & \tau\vec{e}_{t,i}\cdot U_t, & \delta\vec{e}_{t,i}, & \vec{\delta}_{t,i}, & 0 &)_{\mathbb{D}^*_t},\\
\boldsymbol{e}_{t,i,1} := (\ 0^{n_t}, & \omega\vec{e}_{t,i}, & 0^2, & \sigma\vec{e}_{t,i}\cdot Z_t, & 0^{n_t}, & 0^{n_t}, & 0 &)_{\mathbb{B}_t}\\
= (\ 0^{n_t}, & 0^{n_t}, & 0^2, & \sigma\vec{e}_{t,i}\cdot Z_t, & \omega\vec{e}_{t,i}, & 0^{n_t}, & 0 &)_{\mathbb{D}_t},\\
\boldsymbol{e}_{t,i,2} := (\ 0^{n_t}, & (\eta_1+\eta_2\omega)\vec{e}_{t,i}, & 0^2, & \eta_2\sigma\vec{e}_{t,i}\cdot Z_t, & 0^{n_t}, & 0^{n_t}, & 0 &)_{\mathbb{B}_t}\\
= (\ 0^{n_t}, & 0^{n_t}, & 0^2, & \eta_2\sigma\vec{e}_{t,i}\cdot Z_t, & (\eta_1+\eta_2\omega)\vec{e}_{t,i}, & 0^{n_t}, & 0 &)_{\mathbb{D}_t},
\end{array}
$$

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 $\delta, \tau, \omega, \sigma, \eta_1, \eta_2 \xleftarrow{\mathsf{U}} \mathbb{F}_q$.

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 $\mathcal{G}_1^{\mathsf{Exp}\text{-}3}(1^\lambda, \vec{n})$ (resp. $\mathcal{G}_2^{\mathsf{Exp}\text{-}3}(1^\lambda, \vec{n})$) when $\beta = 1$ (resp. $\beta = 0$). This completes the proof of Lemma 17. □

D.2 Proof of Lemma 7

Lemma 7. *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.*

Proof. In order to prove Lemma 7, 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 $t \in S$, $\mathcal{B}_1$ sets

$$\mathbb{D}_t := (\boldsymbol{d}_{t,j})_{j=1,\ldots,5n_t+3} := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,n+2}, \ldots, \boldsymbol{b}_{t,2n_t-1}, \boldsymbol{b}_{t,2n_t}, \boldsymbol{b}_{t,2n_t+1}, \ldots, \boldsymbol{b}_{t,5n_t+3}),$$
$$\mathbb{D}^*_t := (\boldsymbol{d}^*_{t,j})_{j=1,\ldots,5n_t+3} := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,n_t}, \boldsymbol{b}^*_{t,n+2}, \ldots, \boldsymbol{b}^*_{t,2n_t-1}, \boldsymbol{b}^*_{t,2n_t}, \boldsymbol{b}^*_{t,2n_t+1}, \ldots, \boldsymbol{b}^*_{t,5n_t+3}),$$
$$\widehat{\mathbb{D}}_t := (\boldsymbol{d}_{t,1}, \ldots, \boldsymbol{d}_{t,2n_t+2}, \boldsymbol{d}_{t,5n_t+3}),$$
$$\widehat{\mathbb{D}}^*_t := (\widetilde{\boldsymbol{d}}^*_{t,1}, \ldots, \widetilde{\boldsymbol{d}}^*_{t,n_t}, \boldsymbol{d}^*_{t,n_t+1}, \ldots, \boldsymbol{d}^*_{t,2n_t+2}, \boldsymbol{d}^*_{t,4n_t+3}, \ldots, \boldsymbol{d}^*_{t,5n_t+2}),$$
$$\text{where } \pi \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \boldsymbol{r}_{t,\iota} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2}\rangle,\ \widetilde{\boldsymbol{d}}^*_{t,\iota} := \pi \boldsymbol{d}^*_{t,\iota} + \boldsymbol{r}_{t,\iota} \text{ for } \iota = 1, \ldots, n_t.$$

   $\mathcal{B}_1$ 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 $\{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{D}}_t, \widehat{\mathbb{D}}^*_t)\}_{t\in S}$ 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 $\delta_{\mathsf{gid}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 $\mathsf{AttrGen}$ query is issued for a pair of a global identity and an attribute $(\mathsf{gid}, (t, \vec{x}_t))$ for $t \in S$, $\mathcal{B}_1$ first asks a random oracle H_1 query for gid, then obtains the scalar δ_{gid} from the H-list. $\mathcal{B}_1$ calculates

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

   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 an AltSig query is issued by $\mathcal{A}$, $\mathcal{B}_1$ answers a correct signature computed by using $\{\widehat{\mathbb{B}}^*_t\}_{t=1,\ldots,d}$ given in Problem 1, i.e., normal signature.
7. When $\mathcal{B}_1$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ 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:

$$\boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t-1} c_{i,n_t+j} \boldsymbol{e}_{t,j+1} + c_{i,2n_t} \boldsymbol{e}_{\beta,t,1} + \sum_{j=2n_t+1}^{2n_t+2} c_{i,j} \boldsymbol{b}_{t,j} \quad \text{for } i = 1, \ldots, \ell,$$
$$c_{d+1} := g_T^{s_0},$$

   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. $\mathcal{B}_1$ 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 $(\ell + d)/q \leq 2d/q$ since $\ell \leq d$. □

D.3 Proof of Lemma 8

Lemma 8. *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, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2}}(\lambda) + (d+1)/q$, where $\mathcal{B}_{2\text{-}h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Proof. In order to prove Lemma 8, 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, $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,2}, G_0, G_1)$.
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 7 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 $\pi \xleftarrow{\cup} \mathbb{F}_q, \widetilde{\boldsymbol{b}}_{t,\iota}^* := \pi \boldsymbol{b}_{t,\iota}^* + \boldsymbol{r}_{t,\iota}^*$ 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 $t \in S$, that are obtained from the Problem 2' instance. The H-list is initialized as in the proof of Lemma 7.
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 $\delta_{\mathsf{gid}} \xleftarrow{\cup} \mathbb{F}_q$ 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 $\mathsf{AttrGen}$ 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 $t \in S$, $\mathcal{B}_2$ calculates normal key $\boldsymbol{k}_t^*$ with Eq. (2), that is computed using $\mathbb{B}_t^*$ of the Problem 2 instance and δ_{gid} as

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

   where $\vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.
6. When the ι-th AltSig query for $(m, \mathbb{S})$ is issued by $\mathcal{A}$, $\mathcal{B}_2$ 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. (7) 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:

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

   where $\widetilde{\delta} \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\sigma}_i \xleftarrow{\cup} \mathbb{F}_q^{n_t}$, $(\xi_i), (\xi_i') \xleftarrow{\cup} \{(\xi_1, \ldots, \xi_\ell) \mid \sum_{i=1}^{\ell} \xi_i M_i = \vec{1}\}$, and for $i = 1, \ldots, \ell$, if $\rho(i) = (t, \vec{v}_i)$, then $(\vec{z}_{i,0}, \vec{z}_{i,1}) \xleftarrow{\cup} \{(\vec{z}_{i,0}, \vec{z}_{i,1}) \mid \vec{z}_{i,0} \cdot \vec{v}_i = \vec{z}_{i,1} \cdot \vec{v}_i = 0, \ \ z_{i,0,1} = \xi_i, \ z_{i,1,1} = \widetilde{\delta} \xi_i' \}$, 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. (4) using $\{\mathbb{B}_t^*\}_{t=1,\ldots,d}$ in the Problem 2' instance.

7. When $\mathcal{B}_2$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ 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:

$$\boldsymbol{c}_i := \textstyle\sum_{j=1}^{2n_t} c_{i,j}\boldsymbol{b}_{t,j} + H_2(m', \mathbb{S}')(\widetilde{\chi}_{i,1}\boldsymbol{b}_{t,2n_t+1} + \widetilde{\chi}_{i,2}\boldsymbol{e}_{t,1}) - (\widetilde{\chi}_{i,1}\boldsymbol{b}_{t,2n_t+2} + \widetilde{\chi}_{i,2}\boldsymbol{e}_{t,2}) + \eta_i\boldsymbol{b}_{t,5n_t+3} \quad \text{for } i = 1, \ldots, \ell,$$

$$c_{d+1} := g_T^{s_0},$$

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. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0, \vec{s}'^{\mathrm{T}} := (s'_1, \ldots, s'_\ell)^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$, $\eta_i, \theta_i, \theta'_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $i = 1, \ldots, \ell$, and if $\rho(i) = (t, \vec{v}_i)$, then $\vec{c}_i := (s_i\vec{e}_{t,1} + \theta_i\vec{v}_i, s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i) \in \mathbb{F}_q^{2n_t}$, 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 $i = 1, \ldots, \ell$, $\widetilde{\chi}_{i,j} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 7 and $\{\boldsymbol{s}_i^* := \boldsymbol{s}_i^{(h)*}\}_{i=1,\ldots,\ell}$ generated in case (b) of step 6.

$\boldsymbol{c}_i$ for $i = 1, \ldots, \ell$ calculated in step 7 in the above simulation are expressed as:

$$\boldsymbol{c}_i = (\overbrace{\ \vec{c}_i,\ }^{2n_t}\overbrace{\ \omega_i(H_2(m', \mathbb{S}'), -1),\ }^{2}\overbrace{\ 0^{n_t},\ }^{n_t}\overbrace{\ \sigma_i(H_2(m', \mathbb{S}'), -1, 0^{n_t-2}) \cdot Z_t,\ }^{n_t}\overbrace{\ 0^{n_t},\ }^{n_t}\overbrace{\ \eta_i\ }^{1})_{\mathbb{B}_t}, \tag{14}$$

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 7 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 6 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 6 above, and $\vec{\varphi}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$. When $\beta = 1$, replied signature $\boldsymbol{s}_i^*$ generated in case (b) of step 6 is

$$\boldsymbol{s}_i^* := (\overbrace{\ \vec{z}_{i,0}, \vec{z}_{i,1},\ }^{2n_t}\overbrace{\ \delta_i(1, H_2(m, \mathbb{S})),\ }^{2}\overbrace{\ 0^{n_t},\ }^{n_t}\overbrace{\ \tau_i(1, H_2(m, \mathbb{S}), 0^{n_t-2}) \cdot U_t,\ }^{n_t}\overbrace{\ \vec{\varphi}_i,\ }^{n_t}\overbrace{\ 0\ }^{1})_{\mathbb{B}_t^*}, \tag{15}$$

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 6 above, and $\vec{\varphi}_i \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$. 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. (14) is not equal to $(m, \mathbb{S})$ in Eq. (15), 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 6, 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 $\mathsf{Pr}_0 := \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P2}'}(1^\lambda, n)\right]$ $\left(\text{resp. } \mathsf{Pr}_1 := \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P2}'}(1^\lambda, n)\right]\right)$, $\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda) \leq \mathsf{Pr}_0 + \frac{1}{q}$ $\left(\text{resp. } \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda) \leq \mathsf{Pr}_1 + \frac{d}{q}\right)$ from Shoup's difference lemma. Therefore, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h)}(\lambda)| \leq |\mathsf{Pr}_0 - \mathsf{Pr}_1| + \frac{4}{q} = \mathsf{Adv}_{\mathcal{B}_{2\text{-}h}}^{\mathsf{P2}'}(\lambda) + \frac{d+1}{q}$. This completes the proof of Lemma 8. □

D.4 Proof of Lemma 9

Lemma 9. *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda)| \leq 2d/q$.*

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

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 9 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 $F_t \xleftarrow{\mathsf{U}} GL(2n_t, \mathbb{F}_q)$ 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

$$\text{for } i = 1, \ldots, \ell,\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{0^{n_t}, \vec{z}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{D}_t}, \tag{16}$$

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 $\omega_i, \omega_i' \xleftarrow{\mathsf{U}} \mathbb{F}_q, Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q), \vec{g} \xleftarrow{\mathsf{U}} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0\}, \vec{g}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r_i := M_i \cdot \vec{g}^{\mathrm{T}}, r_i' := M_i \cdot (\vec{g}')^{\mathrm{T}}$ 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

$$\text{for } i = 1, \ldots, \ell,\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{z}_i'}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{2n_t}, \overbrace{\cdots}^{n_t+1})_{\mathbb{D}_t}, \tag{17}$$

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. (16) and that of Eq. (17) 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 $\left|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda)\right| \leq 2d/q$ for $h \geq 2$:

To prove Lemma 9 in this case, we will show distribution $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}_t^*\}_{t\in S}, \{\boldsymbol{k}_t^{(j)*}\}_{j=1,\ldots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(j)}}, \{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}, c_{d+1})$ 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

$$\begin{aligned}
&\text{if } \rho(i) = (t,\vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i''\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t},\\
&\text{if } \rho(i) = \neg(t,\vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i''\vec{v}_i)\cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t},
\end{aligned} \tag{18}$$

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 $\{\boldsymbol{k}_t^{(j)*}\}_{(t,\vec{x}_t)\in\Gamma^{(j)}}$ 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 $\{\boldsymbol{s}_i^{(j)*}\}_{i=1,\ldots,\ell}$ for $j = 1,\ldots,\nu_S$.

And, no r_i, ω_i are zero except with negligible probability d/q, vectors $\vec{\chi}_i := ((r_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t)\cdot F_t$ 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 $\omega_i \xleftarrow{\cup} \mathbb{F}_q, Z_t \xleftarrow{\cup} GL(n_t,\mathbb{F}_q), \vec{g} \xleftarrow{\cup} \{\vec{g}\in\mathbb{F}_q^r \mid \vec{1}\cdot\vec{g}^{\mathrm{T}} = 0\}, r_i := M_i\cdot\vec{g}^{\mathrm{T}}$. 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

$$\begin{aligned}
&\text{if } \rho(i) = (t,\vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t},\\
&\text{if } \rho(i) = \neg(t,\vec{v}_i),\ \boldsymbol{c}_i = (\overbrace{\cdots}^{2n_t+2}, \overbrace{(r_i\vec{v}_i)\cdot Z_t}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{B}_t} = (\overbrace{\cdots}^{2n_t+2}, \overbrace{\vec{\chi}_i}^{n_t}, \overbrace{\cdots}^{2n_t+1})_{\mathbb{D}_t},
\end{aligned} \tag{19}$$

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. (18) and that of Eq. (19) 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. □

D.5 Proof of Lemma 10

Lemma 10. *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, $|\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{3\text{-}h\text{-}1}}^{\mathsf{P2}}(\lambda)$, where $\mathcal{B}_{3\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{3\text{-}1}(h, \cdot)$.*

Proof. In order to prove Lemma 10, 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, $(\mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t, \mathbb{B}_t^*, \boldsymbol{h}_{\beta,t,i}^*, \boldsymbol{e}_{t,i}\}_{t=1,..,d;i=1,..,n_t}, G_0, G_1, \delta G_1)$.
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 7 and $\{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t', \widehat{\mathbb{B}}_t^*)\}_{t\in S}$ of Game 3-h-1 (and 3-h-2), 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 $t \in S$, that are obtained from the Problem 2 instance. The H-list is initialized as in the proof of Lemma 7.
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 $\delta_{\mathsf{gid}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 $t \in S$, $\mathcal{B}_{3\text{-}1}$ 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. (11) to $\mathcal{A}$, that is computed using $\mathbb{B}_t^*$ of the Problem 2 instance and δ_{gid} as

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

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

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

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

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

where $\vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\cup} \mathbb{F}_q^{n_t}$.

6. When an AltSig query is issued by $\mathcal{A}$, $\mathcal{B}_{3\text{-}1}$ answers a semi-functional signature (Eq. (7)) computed by using $\{\mathbb{B}_t^*\}_{t=1,\ldots,d}$ given in the Problem 2 instance.
7. When $\mathcal{B}_{3\text{-}1}$ receives an output $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ from $\mathcal{A}$ (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. (8) as follows:

$$\begin{aligned}
&\pi'_t, \mu_t, g'_k, \widetilde{\mu}_k \xleftarrow{\cup} \mathbb{F}_q \ \text{ for } t = 1, \ldots, d;\ k = 1, \ldots, r-1;\\
&g'_r := -\textstyle\sum_{k=1}^{r-1} g'_k,\ \widetilde{\mu}_r := -\sum_{k=1}^{r-1} \widetilde{\mu}_k, \quad i.e., \quad \sum_{k=1}^{r} g'_k = 0,\ \sum_{k=1}^{r} \widetilde{\mu}_k = 0,\\
&\text{for } t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t;\\
&\quad \boldsymbol{f}_{t,j} := \pi'_t \boldsymbol{e}_{t,j} + \mu_t \boldsymbol{b}_{t,n_t+j}, \quad \widetilde{\boldsymbol{f}}_{t,k,j} := g'_k \boldsymbol{e}_{t,j} + \widetilde{\mu}_k \boldsymbol{b}_{t,n_t+j},\\
&\text{for } i = 1 \ldots, \ell,\\
&\quad \text{if } \rho(i) = (t, \vec{v}_i), \quad (c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{e}_{t,1} + \theta_i \vec{v}_i, r'_i \vec{e}_{t,1} + \omega'_i \vec{v}_i),\\
&\qquad \boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,1}\\
&\qquad\qquad + \theta''_i \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}\right) + \sum_{j=1}^{n_t} c_{i,n_t+j} \boldsymbol{b}_{t,3n_t+2+j} + \boldsymbol{q}_i,\\
&\quad \text{if } \rho(i) = \neg(t, \vec{v}_i), \quad (c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{v}_i, r'_i \vec{v}_i),\\
&\qquad \boldsymbol{c}_i := \textstyle\sum_{j=1}^{n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,j} + \theta''_i \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2}\right)\\
&\qquad\qquad + \textstyle\sum_{j=1}^{n_t} c_{i,n_t+j} \boldsymbol{b}_{t,3n_t+2+j} + \boldsymbol{q}_i,\\
&c_{d+1} := g_T^{s_0},
\end{aligned}$$

where $(M_{i,k})_{i=1,\ldots,\ell;k=1,\ldots,r} := M, \vec{f} \xleftarrow{\cup} \mathbb{F}_q^r, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, s_i := M_i \cdot \vec{f}^{\mathrm{T}}, \vec{g}' \xleftarrow{\cup} \mathbb{F}_q^r, r'_i := M_i \cdot (\vec{g}')^{\mathrm{T}}, \theta_i, \theta''_i, \omega'_i, \xleftarrow{\cup} \mathbb{F}_q, \boldsymbol{q}_i \xleftarrow{\cup} \mathsf{span}\langle \boldsymbol{b}_{t,5n_t+3} \rangle$ and $\{\boldsymbol{b}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,2n_t+2,3n_t+3,\ldots,4n_t+2}$, $\{\boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t}$ are obtained from the Problem 2 instance. $\mathcal{B}_{3\text{-}1}$ verifies the signature $(m', \mathbb{S}', \vec{\boldsymbol{s}}'^*)$ 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:

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

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 $\{f_k, g_k\}_{k=1,\ldots,r}$ are independently and uniformly distributed with only two relations $\sum_{k=1}^{r} f_k = 0$ and $\sum_{k=1}^{r} g_k = 0$. Therefore, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ are distributed as in Eq. (8).

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

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

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

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

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 10 in the same manner as in the proof of Lemma 8. □

D.6 Proof of Lemma 11

Lemma 11. *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 $r_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$, i.e., $\vec{g}^{<2>} \xleftarrow{\mathsf{U}} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0\}$, $\vec{g}^{<3>} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$, $r_i^{<b>} := M_i \cdot (\vec{g}^{<b>})^{\mathrm{T}}$ for $b = 2, 3; i = 1, \ldots, \ell$.

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. $\gamma(i)$ 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 6, 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 $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).
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 6, 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 $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$).
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 6, 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 $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$) 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 6, 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, $\vec{1} \notin \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$. Hence, the distribution of $\{ \tau r_i^{<2>} \mid$ cases 1 and 2 $\}$ is equivalent to that of $\{ \tau r_i^{<3>} \mid$ 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. □

D.7 Proof of Lemma 12

Lemma 12. *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 12, 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 10 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 10.
2. In case (b) of step 5; $\boldsymbol{k}_t^{(h)*}$ is calculated using $\mathbb{B}_t^*$ and $\{\boldsymbol{h}_{\beta,t,j}^*\}_{j=1,..,n_t}$ of the Problem 3 instance as follows:
$$\boldsymbol{k}_t^{(h)*} := \textstyle\sum_{j=1}^{n_t} x_{t,j}^{(h)} \left(\boldsymbol{b}_{t,j}^* + \delta^{(h)} \boldsymbol{b}_{t,n_t+j}^* + \boldsymbol{h}_{\beta,t,j}^* \right),$$
   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. (10) 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 $t = 1, \ldots, d;\ k = 1, \ldots, r;\ j = 1, \ldots, n_t;$
$\boldsymbol{f}_{t,j} := \sum_{\iota=1}^{2} \pi_{t,\iota} \boldsymbol{e}_{t,j,\iota}, \quad \widetilde{\boldsymbol{f}}_{t,k,j} := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota} \boldsymbol{e}_{t,j,\iota},$
for $i = 1 \ldots, \ell,$
if $\rho(i) = (t, \vec{v}_i), \quad (c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{e}_{t,1} + \theta_i \vec{v}_i, s_i' \vec{e}_{t,1} + \theta_i' \vec{v}_i),$
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \boldsymbol{f}_{t,j} + \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,1}$
$+\theta_i'' \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2} \right) + \boldsymbol{q}_i,$
if $\rho(i) = \neg(t, \vec{v}_i), \quad (c_{i,1}, \ldots, c_{i,2n_t}) := (s_i \vec{v}_i, s_i' \vec{v}_i),$
$\boldsymbol{c}_i := \sum_{j=1}^{2n_t} c_{i,j} \boldsymbol{b}_{t,j} + \sum_{j=1}^{n_t} v_{i,j} \sum_{k=1}^{r} M_{i,k} \widetilde{\boldsymbol{f}}_{t,k,j} + \theta_i'' \left(H_2(m', \mathbb{S}') \boldsymbol{b}_{t,2n_t+1} - \boldsymbol{b}_{t,2n_t+2} \right) + \boldsymbol{q}_i,$
$c_{d+1} := g_T^{s_0},$

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 $\{\boldsymbol{b}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,2n_t+2}$, $\{\boldsymbol{e}_{t,j,\iota}\}_{t=1,\ldots,d;j=1,\ldots,n_t;\iota=1,2}$ 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:

$$\pi_t := \textstyle\sum_{\iota=1}^{2} \pi_{t,\iota}\omega_\iota, \quad \pi'_t := \sum_{\iota=1}^{2} \pi_{t,\iota}\omega'_\iota, \quad g_k := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota}\omega_\iota, \quad g'_k := \sum_{\iota=1}^{2} \widetilde{g}_{k,\iota}\omega'_\iota,$$

$$\begin{aligned}
\boldsymbol{f}_{t,j} &= (\ \overbrace{0^{2n_t+2}}^{2n_t+2},\ \overbrace{\pi_t \vec{e}_{t,j}}^{n_t},\ \overbrace{(\pi'_t \vec{e}_{t,j}) Z_t}^{n_t},\ \overbrace{0^{n_t}}^{n_t},\ \overbrace{0}^{1}\ )_{\mathbb{B}_t}, \\
\widetilde{\boldsymbol{f}}_{t,k,j} &= (\ 0^{2n_t+2},\ g_k \vec{e}_{t,j},\ (g'_k \vec{e}_{t,j}) Z_t,\ 0^{n_t},\ 0\ )_{\mathbb{B}_t},
\end{aligned}$$

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. (10).

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

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

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

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

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 12 in the same manner as in the proof of Lemma 8. □

D.8 Proof of Lemma 13

Lemma 13. *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}_{\mathcal{A}}^{(3\text{-}\nu_H\text{-}4)}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{(4)}(\lambda)$.*

Proof. In order to prove Lemma 13, 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 7 and sets $\widetilde{\boldsymbol{b}}^*_{t,\iota} := \boldsymbol{h}^*_{\beta,t,\iota}$ for $\iota = 1, \ldots, n_t$, $\widehat{\mathbb{B}}'_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t+2}, \boldsymbol{b}_{t,5n_t+3}), \widehat{\mathbb{B}}^* := (\widetilde{\boldsymbol{b}}^*_{t,1}, \ldots, \widetilde{\boldsymbol{b}}^*_{t,n_t}, \boldsymbol{b}^*_{t,n_t+1}, \ldots, \boldsymbol{b}^*_{t,2n_t+2}, \boldsymbol{b}^*_{t,4n_t+3}, \ldots, \boldsymbol{b}^*_{t,5n_t+2}), \{\mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}'_t, \widehat{\mathbb{B}}^*_t)\}_{t\in S}$ 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 $\delta_{\mathsf{gid}} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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. (11), that is computed using $\mathbb{B}^*_t$ of the Problem 2" instance and δ_{gid} as

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

   where $\tau'_{\mathsf{gid}} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\varphi}_{\mathsf{gid},t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$.
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. (7) using $\{\mathbb{B}^*_t\}_{t=1,\ldots,d}$ 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. (10) as follows:

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

   where $(M_{i,k})_{i=1,\ldots,\ell;k=1,\ldots,r} := M, \vec{f}' \xleftarrow{\mathsf{U}} \{\vec{f}' \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0\}, s'_i := M_i \cdot \vec{f}'^{\mathrm{T}}, \vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r''_i := M_i \cdot \vec{g}^{\mathrm{T}}, \theta'_i, \theta''_i, \omega_i \xleftarrow{\mathsf{U}} \mathbb{F}_q, Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$ and $\boldsymbol{q}_i \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_{t,5n_t+3} \rangle$, and $\{\boldsymbol{b}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,3n_t+2}$, and $\{\boldsymbol{e}_{t,j}\}_{t=1,\ldots,d;j=1,\ldots,n_t}$ are obtained from the Problem 2" instance. $\mathcal{B}_4$ 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 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 $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ generated in step 7 and $\{\widetilde{\boldsymbol{b}}^*_{t,\iota}\}_{t=1,\ldots,d;\iota=1,\ldots,n_t}$ 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:

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

where ω, σ are defined in Problem 2". Note that variables $\{\theta_t, \pi_t\}_{t=1,\ldots,d}$ and $\{f_k, g_k\}_{k=1,\ldots,r}$ are independently and uniformly distributed. Therefore, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ are distributed as in Eq. (10).

When $\beta = 0$, a part of authority public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, generated in step 3 is

$$\widetilde{\boldsymbol{b}}^*_{t,j} = \boldsymbol{h}^*_{\beta,t,j} = (\overbrace{\delta\vec{e}_{t,j}}^{n_t}, \overbrace{0^{3n_t+2}}^{3n_t+2}, \overbrace{\delta_{t,j}}^{n_t}, 0)_{\mathbb{B}^*_t} \text{ with } \delta \xleftarrow{\cup} \mathbb{F}_q, \ \delta_{t,j} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

When $\beta = 1$, a part of authority public key, $\widetilde{\boldsymbol{b}}^*_{t,\iota}$, generated in step 3 is

$$\widetilde{\boldsymbol{b}}^*_{t,j} = \boldsymbol{h}^*_{\beta,t,j} = (\overbrace{\delta\vec{e}_{t,j}}^{n_t}, \overbrace{0^{2n_t+2}}^{2n_t+2}, \overbrace{\tau\vec{e}_{t,j}}^{n_t}, \overbrace{\delta_{t,j}}^{n_t}, 0)_{\mathbb{B}^*_t} \text{ with } \delta, \tau \xleftarrow{\cup} \mathbb{F}_q, \ \delta_{t,j} \xleftarrow{\cup} \mathbb{F}_q^{n_t}.$$

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 13 in the same manner as in the proof of Lemma 8. □

D.9 Proof of Lemma 14

Lemma 14. *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, $|\mathsf{Adv}^{(4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(5)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_4}(\lambda)$.*

Proof. To prove Lemma 14, we will show distribution $(\mathsf{gparam}, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t=1,\ldots,d}, \{\boldsymbol{s}^{(h)*}_i\}_{h=1,\ldots,\nu_S;i=1,\ldots,\ell}, \{\boldsymbol{k}^{(h)*}_t\}_{h=1,\ldots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(h)}}, \{\boldsymbol{c}_i\}_{i=1,\ldots,\ell})$ 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

$$\boldsymbol{d}_{t,3n_t+2+\iota} := \boldsymbol{b}_{t,3n_t+2+\iota} - \xi\boldsymbol{b}_{t,\iota}, \qquad \boldsymbol{d}^*_{t,\iota} := \boldsymbol{b}^*_{t,\iota} + \xi\boldsymbol{b}^*_{t,3n_t+2+\iota} \quad \text{for } \iota = 1,\ldots,n_t,$$

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

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

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

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

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,

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

where

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

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

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

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

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 $\widetilde{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,n_t+1}^*, \ldots, \boldsymbol{b}_{t,2n_t+2}^*, \boldsymbol{b}_{t,4n_t+3}^*, \ldots, \boldsymbol{b}_{t,5n_t+2}^*)$. Therefore, $\{\boldsymbol{s}_i^{(h)*}\}_{h=1,\ldots,\nu_S;i=1,\ldots,\ell}$, $\{\boldsymbol{k}_t^{(h)*}\}_{h=1,\ldots,\nu_H;(t,\vec{x}_t)\in\Gamma^{(h)}}$, $\{\widetilde{\boldsymbol{b}}_{t,\iota}^*\}_{t\in S;\iota=1,\ldots,n_t}$, $\{\boldsymbol{c}_i\}_{i=1,\ldots,\ell}$ 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. □

E Decentralized Multi-Authority Functional Encryption

E.1 Definitions of DMA-FE

Definition 19 (Decentralized Multi-Authority FE). *A decentralized multi-authority (DMA) FE 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-FE 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 [38], or an attribute is considered to be of the form of $(t,\vec{x}_t)$.

Definition 20 (Adaptive Payload Hiding of DMA-FE). *For an adversary, we define* $\mathsf{Adv}^{\mathsf{DMA\text{-}FE,PH}}_{\mathcal{A}}(\lambda)$ *to be the success probability in the following experiment for any security parameter* λ*. A DMA-FE 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* $\mathcal{A}$*. For each authority* $t \in S$*, the challenger runs* $(\mathsf{ask}_t, \mathsf{apk}_t) \xleftarrow{\mathsf{R}} \mathsf{ASetup}(\mathsf{gparam}, t, n_t)$ *and gives* $\{\mathsf{apk}_t\}_{t\in S}$ *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 private keys, attribute secret key* $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$*.*

Challenge *Let* $\Gamma_{\mathsf{gid}_i} := \{(t, \vec{x})\}$ *(*$i = 1, \ldots, \nu$*) queried to the* $\mathsf{AttrGen}$ *oracle with* gid_i*. 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* Γ_{gid_i} *with any* gid_i *(*$i = 1, \ldots, \nu$*). The challenger flips a random coin* $b \xleftarrow{\mathsf{U}} \{0, 1\}$*, and computes* $\mathsf{ct}^{(b)}_{\mathbb{S}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\}, m^{(b)}, \mathbb{S})$*. It gives* $\mathsf{ct}^{(b)}_{\mathbb{S}}$ *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 oracle* $\mathsf{AttrGen}(\mathsf{gparam}, t, \mathsf{ask}_t, \cdot, \cdot)$ *for private keys, attribute secret key* $\mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)}$*. provided that* $\mathbb{S}$ *does not accept* Γ_{gid_i} *with any* gid_i *(*$i = 1, \ldots, \nu$*).*

Guess *The adversary outputs a guess* b' *of* b*.*

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

E.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 will show how to relax the restriction in Appendix F. 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 Section 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 $\boldsymbol{v}$ in N-dimensional $\mathbb{V}$, $X(\boldsymbol{v})$ denotes $\sum_{i=1,j=1}^{N,N} \chi_{i,j}\phi_{i,j}(\boldsymbol{v})$ using canonical maps $\{\phi_{i,j}\}$ (Definition 2). Similarly, for matrix $(\vartheta_{i,j}) := (X^{-1})^{\mathrm{T}}$, $(X^{-1})^{\mathrm{T}}(\boldsymbol{v}) := \sum_{i=1,j=1}^{N,N} \vartheta_{i,j}\phi_{i,j}(\boldsymbol{v})$. It holds that $e(X(\boldsymbol{x}), (X^{-1})^{\mathrm{T}}(\boldsymbol{y})) = e(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{V}$.

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

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

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

$\mathsf{AttrGen}(\mathsf{gparam},\ t,\ \mathsf{ask}_t,\ \mathsf{gid},\ \vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ such that $x_{t,1} := 1)$:

$G_{\mathsf{gid}}\ (= \delta G_1)\ := H(\mathsf{gid}) \in \mathbb{G},\ \vec{\varphi}_t := (\varphi_{t,1}, \ldots, \varphi_{t,n_t}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$,

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

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

Remark : Let $\boldsymbol{b}_i^* := (X_t^{-1})^{\mathrm{T}}((0^{i-1},\ G_1,\ 0^{5n_t+1-i}))$ and $\mathbb{B}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,5n_t+1}^*)$.

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. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0,\ \vec{s}'^{\mathrm{T}} := (s_1', \ldots, s_\ell')^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}},\ \eta_i, \theta_i, \theta_i' \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (i = 1, .., \ell)$,

for $i = 1, \ldots, \ell$,

if $\rho(i) = (t, \vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ such that $v_{i,n_t} \neq 0)$,

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

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

$I \subseteq\ \{i \in \{1, \ldots, \ell\} |\ [\rho(i) = (t, \vec{v}_i)\ \wedge\ (t, \vec{x}_t) \in \Gamma\ \wedge\ \vec{v}_i \cdot \vec{x}_t = 0]$

$\vee\ \ [\rho(i) = \neg(t, \vec{v}_i)\ \wedge\ (t, \vec{x}_t) \in \Gamma\ \wedge\ \vec{v}_i \cdot \vec{x}_t \neq 0]\ \}$,

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

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

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

$$\prod_{i \in I\ \wedge\ \rho(i) = (t, \vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i} \cdot \prod_{i \in I\ \wedge\ \rho(i) = \neg(t, \vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}_t^*)^{\alpha_i / (\vec{v}_i \cdot \vec{x}_t)}$$
$$= \prod_{i \in I\ \wedge\ \rho(i) = (t, \vec{v}_i)} g_T^{\alpha_i (s_i + \delta s_i')} \prod_{i \in I\ \wedge\ \rho(i) = \neg(t, \vec{v}_i)} g_T^{(\alpha_i (s_i + \delta s_i'))(\vec{v}_i \cdot \vec{x}_t) / (\vec{v}_i \cdot \vec{x}_t)}$$

$$= g_T^{\sum_{i\in I}(\alpha_i s_i + \delta\alpha_i s'_i)} = g_T^{s_0}, \quad \text{since } \textstyle\sum_{i\in I}\alpha_i s_i = s_0 \text{ and } \sum_{i\in I}\alpha_i s'_i = 0.$$

Comparison with the CP-FE Scheme in [47] Okamoto-Takashima [47] gave an adaptively secure CP-FE 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-FE 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 [47] CP-FE, 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 [47] 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 [47] CP-FE : ($\overbrace{\text{real}}^{n_t}$ $\overbrace{\text{hidden}}^{n_t}$ $\overbrace{\text{SK ran.}}^{n_t}$ $\overbrace{\text{CT ran.}}^{1}$),

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

E.3 Security of the Proposed DMA-FE

Theorem 5. *The proposed DMA-FE 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,

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

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

E.4 Proof Outline of Theorem 5

At the top level strategy of the security proof, an extended form of the dual system encryption by Waters [58] 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 random oracle queries are issued by an adversary, there are 4ν 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-1, Game 2-ν-2, Game 2-ν-3, Game 2-ν-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-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.

Table 3. Outline of Game Descriptions

	challenge ciphertext	queried keys						
		1	$\cdots$	$h-1$	h	$h+1$	$\cdots$	ν
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-4	semi-func.	semi-func.						semi-func.
3	non-func.	semi-func.						

We summarize these changes in Table 3, 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-FE scheme, and is expressed by Eq. (20). Similarly, a normal ciphertext (with access structure $\mathbb{S}$), $\vec{\boldsymbol{c}}^{\mathsf{norm}}$, is expressed by Eq. (21). A temporal ciphertext is expressed by Eq. (22). A pre-semi-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{pre\text{-}semi}}$, is expressed by Eq. (23) and a pre-semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{pre\text{-}semi}}$, is expressed by Eq. (24). A semi-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{semi}}$, is expressed by Eq. (25) and a semi-functional secret key, $\vec{\boldsymbol{k}}^{*\,\mathsf{semi}}$, is expressed by Eq. (26). An non-functional ciphertext, $\vec{\boldsymbol{c}}^{\mathsf{non\text{-}f}}$, is expressed by Eq. (27).

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 $\beta \xleftarrow{\mathsf{U}} \{0, 1\}$ 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 18). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 1).

We then show that Game 2-$(h-1)$-4 can be conceptually changed to Game 2-h-1 (Lemma 19), 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 $r''_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 20 and 2).

We then show that Game 2-h-2 can be conceptually changed to Game 2-h-3 (Lemma 21), 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 $r''_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ 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 6.

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 22 and 5).

We then show that Game 2-ν-4 can be conceptually changed to Game 3 (Lemma 23) 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 $t \in S$, and the challenge ciphertext for $(m^{(0)}, m^{(1)}, \mathbb{S} :=$

(M, ρ)) are:

$$\boldsymbol{k}_t^{(h)*} := (\overbrace{\quad \vec{x}_t, \quad}^{n_t} \overbrace{\quad \delta^{(h)}\vec{x}_t, \quad}^{n_t} \overbrace{\boxed{0^{2n_t}}, \quad}^{2n_t} \overbrace{\quad \vec{\varphi}_t^{(h)}, \quad}^{n_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}_t^*} \tag{20}$$

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\boxed{s_i}\vec{e}_{t,1} + \theta_i\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i,}^{n_t} \overbrace{\boxed{0^{2n_t}},}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\quad \boxed{s_i}\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{v}_i,}^{n_t} \overbrace{\quad \boxed{0^{2n_t}},}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad c_{d+1} := g_T^{\boxed{s_0}} m^{(b)}, \end{array}\right\} \tag{21}$$

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

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

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{e}_{t,1} + \theta_i\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i,}^{n_t} \overbrace{\quad \boxed{z_i\vec{e}_{t,1}},}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{v}_i,}^{n_t} \overbrace{\quad \boxed{z_i\vec{e}_{t,1}},}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad c_{d+1} := g_T^{s_0} m^{(b)}, \end{array}\right\} \tag{22}$$

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

Game 2-h-1 ($h = 1, \ldots, \nu$) : 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:

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{e}_{t,1} + \theta_i\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{e}_{t,1} + \theta_i'\vec{v}_i,}^{n_t} \\ \qquad \overbrace{\boxed{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t, \quad r_i'\vec{e}_{t,1} + \omega_i'\vec{v}_i}}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{v}_i,}^{n_t} \overbrace{\quad s_i'\vec{v}_i,}^{n_t} \overbrace{\quad \boxed{r_i\vec{v}_i \cdot Z_t,\ r_i'\vec{v}_i},}^{2n_t} \overbrace{\quad 0^{n_t},}^{n_t} \overbrace{\quad \eta_i \quad}^{1})_{\mathbb{B}_t}, \\ \quad c_{d+1} := g_T^{s_0} m^{(b)}, \end{array}\right\} \tag{23}$$

where $\vec{g} \xleftarrow{\mathsf{U}} \{\vec{g} \in \mathbb{F}_q^r \mid \vec{1} \cdot \vec{g}^{\mathrm{T}} = 0\}, \vec{g}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r_i := M_i \cdot \vec{g}^{\mathrm{T}}, r'_i := M_i \cdot \vec{g}'^{\mathrm{T}}, Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q), \ \ \omega_i, \omega'_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and the other variables are generated as in Game 2-$(h-1)$-4.

Game 2-h-2 ($h = 1, \ldots, \nu$): 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 $t \in S$) is:

$$\boldsymbol{k}_t^{(h)*} := (\overbrace{\quad \vec{x}_t, \quad}^{n_t} \overbrace{\quad \delta^{(h)}\vec{x}_t, \quad}^{n_t} \overbrace{\quad \boxed{\tau^{(h)}\vec{x}_t \cdot U_t}, \ 0^{n_t} \quad}^{2n_t} \overbrace{\quad \vec{\varphi}_t^{(h)}, \quad}^{n_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}_t^*} \tag{24}$$

where $\tau^{(h)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $U_t := (Z_t^{-1})^{\mathrm{T}}$ for $Z_t \xleftarrow{\mathsf{U}} GL(n_t, \mathbb{F}_q)$ used in Eq. (23), and the other variables are generated as in Game 2-h-1.

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

$$\left.\begin{array}{l} \text{for } i = 1, \ldots, \ell, \\ \quad \text{if } \rho(i) = (t, \vec{v}_i), \ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{e}_{t,1} + \theta_i\vec{v}_i, \quad}^{n_t} \overbrace{\quad s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i, \quad}^{n_t} \\ \qquad \overbrace{\quad (\boxed{r''_i}\vec{e}_{t,1} + \omega_i\vec{v}_i) \cdot Z_t, \quad r'_i\vec{e}_{t,1} + \omega'_i\vec{v}_i, \quad 0^{n_t}, \quad \eta_i \quad}^{2n_t} \overbrace{\quad \quad}^{n_t} \overbrace{\quad \quad}^{1})_{\mathbb{B}_t}, \\ \quad \text{if } \rho(i) = \neg(t, \vec{v}_i), \ \boldsymbol{c}_i := (\overbrace{\quad s_i\vec{v}_i, \quad}^{n_t} \overbrace{\quad s'_i\vec{v}_i, \quad}^{n_t} \overbrace{\quad \boxed{r''_i}\vec{v}_i \cdot Z_t, \ r'_i\vec{v}_i, \quad 0^{n_t}, \quad \eta_i \quad}^{2n_t} \overbrace{\quad \quad}^{n_t} \overbrace{\quad \quad}^{1})_{\mathbb{B}_t}, \\ \quad c_{d+1} := g_T^{s_0} m^{(b)}, \end{array}\right\} \tag{25}$$

where $\vec{g} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, r''_i := M_i \cdot \vec{g}^{\mathrm{T}}$, and the other variables are generated as in Game 2-h-2.

Game 2-h-4 ($h = 1, \ldots, \nu$) : 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 $t \in S$) is:

$$\boldsymbol{k}_t^{(h)*} = (\overbrace{\quad \vec{x}_t, \quad}^{n_t} \overbrace{\quad \delta^{(h)}\vec{x}_t, \quad}^{n_t} \overbrace{\quad \boxed{0^{n_t}, \quad \tau'^{(h)}\vec{x}_t}, \quad}^{2n_t} \overbrace{\quad \vec{\varphi}_t^{(h)}, \quad}^{n_t} \overbrace{\quad 0 \quad}^{1})_{\mathbb{B}_t^*} \tag{26}$$

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

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

for $i = 1, \ldots, \ell$,

$$\text{if } \rho(i) = (t, \vec{v}_i),\ \boldsymbol{c}_i := (\ \overbrace{\boxed{\tilde{s}_i}\vec{e}_{t,1} + \theta_i\vec{v}_i}^{n_t},\quad \overbrace{s'_i\vec{e}_{t,1} + \theta'_i\vec{v}_i}^{n_t},$$
$$\overbrace{(r_i\vec{e}_{t,1} + \omega_i\vec{v}_i)\cdot Z_t,\quad r'_i\vec{e}_{t,1} + \omega'_i\vec{v}_i,}^{2n_t}\quad \overbrace{0^{n_t}}^{n_t},\quad \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t},$$

$$\text{if } \rho(i) = \neg(t, \vec{v}_i),\ \boldsymbol{c}_i := (\ \overbrace{\boxed{\tilde{s}_i}\vec{v}_i}^{n_t},\quad \overbrace{s'_i\vec{v}_i}^{n_t},\quad \overbrace{r_i\vec{v}_i\cdot Z_t,\quad r'_i\vec{v}_i,}^{2n_t}\quad \overbrace{0^{n_t}}^{n_t},\quad \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t},$$

$$c_{d+1} := g_T^{\boxed{s_0}} m^{(b)},$$

where $\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r, \widetilde{s}_i := M_i \cdot \vec{f}^{\mathrm{T}}$ and $s_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q$. The other variables are generated as in Game 2-ν-4. Here, we note that s_0 is independent from all the other variables.

Let $\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda)$ be $\mathsf{Adv}^{\mathsf{DMA\text{-}FE,PH}}_{\mathcal{A}}(\lambda)$ 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 $1, 2\text{-}h\text{-}1, \ldots, 2\text{-}h\text{-}4, 3$, respectively.

It is obtained that $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$ by Lemma 24. We will show five lemmas (Lemmas 18-23) 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 $h = 1, \ldots, \nu$, and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$. From these lemmas and Lemmas 1, 2 and 5, we obtain

$\mathsf{Adv}^{\mathsf{DMA\text{-}FE,PH}}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=1}^{\nu}\left|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)\right|$
$+ \sum_{\iota=1}^{3}\sum_{h=1}^{\nu}\left|\mathsf{Adv}^{(2\text{-}h\text{-}\iota)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}(\iota+1))}_{\mathcal{A}}(\lambda)\right| + \left|\mathsf{Adv}^{(2\text{-}\nu\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) +$
$\sum_{h=1}^{\nu}\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h}}(\lambda) + \sum_{h=1}^{\nu}\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3,h}}(\lambda) + (2d\nu + 2d)/q \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu}\left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2,h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{3,h}}(\lambda)\right) +$
$((2d + 10)\nu + 2d + 5)/q$. This completes the proof of Theorem 5. □

Lemma 18. *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, $|\mathsf{Adv}^{(0)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + 2d/q$.*

Lemma 19. *For any adversary $\mathcal{A}$, for any security parameter λ, $|\mathsf{Adv}^{(2\text{-}(h-1)\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)| \leq 2d/q$.*

Lemma 20. *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, $|\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2,h}}(\lambda)$, where $\mathcal{B}_{2,h}(\cdot) := \mathcal{B}_2(h, \cdot)$.*

Lemma 21. *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 22. *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, $|\mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{3,h}}(\lambda)$, where $\mathcal{B}_{3,h}(\cdot) := \mathcal{B}_3(h, \cdot)$.*

Lemma 23. *For any adversary $\mathcal{A}$, for any security parameter λ, $\mathsf{Adv}^{(2\text{-}\nu\text{-}4)}_{\mathcal{A}}(\lambda) = \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$.*

Lemma 24. *For any adversary $\mathcal{A}$, $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) = 0$.*

The proofs of Lemmas 18–23 are given in the full version of this paper.

F How to Relax the Restriction that $\widetilde{\rho}$ Is Injective

The following technique can be also applied to DMA-FS (and DMA-ABS).

F.1 Generalized Version of Lemma 6

Let V is n-dimensional vector space $\mathbb{F}_q^n$, and V^* its dual. For $\vec{p} := (p_1, \dots, p_s) \in \mathbb{F}_q^s$, let

$$C_{\vec{p}} := \left\{ (\vec{x}, \vec{v}_1, \dots, \vec{v}_s) \;\middle|\; \begin{array}{l} \vec{x} \neq \vec{0},\ \vec{x} \cdot \vec{v}_i = p_i \text{ for } i = 1, \dots, s \\ \{\vec{v}_i\}_{i=1,\dots,s} \text{ are linearly independent over } \mathbb{F}_q, \end{array} \right\} \subset V \times (V^*)^s.$$

Lemma 25 (Lemma 23 in [47]). *For all $\vec{p}$ such that $C_{\vec{p}} \neq \emptyset$, for all $(\vec{x}, \vec{v}_1, \dots, \vec{v}_s) \in C_{\vec{p}}$, and $(\vec{r}, \vec{w}_1, \dots, \vec{w}_s) \in C_{\vec{p}}$,*

$$\Pr_{Z \xleftarrow{\cup} GL(n, \mathbb{F}_q),} [\vec{x}U = \vec{r} \ \wedge\ \vec{v}_i Z = \vec{w}_i \text{ for } i = 1, \dots, s] = \frac{1}{\sharp C_{\vec{p}}},$$

where $U := (Z^{-1})^{\mathrm{T}}$.

F.2 The Modified DMA-FE Scheme

We assume that $\varphi \in \mathbb{N}$ is given in the system. For any access structure $\mathbb{S} := (M, \rho)$ for ciphertext in the DMA-FE scheme, $\varphi \geq \max_{t=1}^{d} \#\{i \mid \widetilde{\rho}(i) = t\}$. (In the proposed DMA-FE scheme in Section E.2, we assume that $\varphi := 1$.)

We will show how to modify the DMA-FE scheme to allow $\varphi > 1$ with preserving the security of the DMA-FE scheme in Section E.2.

1. As for ASetup, given $(\mathsf{gparam},\ t,\ n_t)$, execute $\mathsf{ASetup}(\mathsf{gparam},\ t,\ n'_t)$ such that $n'_t := n_t + \varphi$.
2. As for $\mathsf{AttrGen}$, given $(\mathsf{gparam},\ t, \mathsf{ask}_t,\ \mathsf{gid},\ \vec{x}_t)$ execute the same procedure as $\mathsf{AttrGen}$ except that:

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

3. As for Enc, given $(\mathsf{pk},\ m,\ \mathbb{S} := (M, \rho))$, execute the same procedure as Enc except that:

$$\mathsf{if}\ \rho(i) = (t, \vec{v}_i := (v_{i,1}, \dots, v_{i,n_t}) \in \mathbb{F}_q^{n_t}) \qquad \eta_i, \theta_i, \theta'_i, \tau_i, \tau'_i \xleftarrow{\cup} \mathbb{F}_q,$$

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

$$\mathsf{if}\ \rho(i) = \neg(t, \vec{v}_i), \qquad \eta_i, \tau_i, \tau'_i \xleftarrow{\cup} \mathbb{F}_q,$$

$$\boldsymbol{c}_i := (\ \overbrace{s_i\vec{v}_i, 0^{\kappa-1}, \tau_i, 0^{\varphi-\kappa},}^{n'_t}\ \overbrace{s'_i\vec{v}_i, 0^{\kappa-1}, \tau'_i, 0^{\varphi-\kappa},}^{n'_t}\ \overbrace{0^{3n'_t},}^{2n'_t}\ \overbrace{0^{2n'_t},}^{n'_t}\ \overbrace{\eta_i}^{1}\ )_{\mathbb{B}_t},$$

where i is the κ-th index such that $\widetilde{\rho}(i) = t$, i.e., $\widetilde{\rho}(i) = t$ and $\sharp\{j < i \mid \widetilde{\rho}(j) = t\} = \kappa - 1$.

F.3 Security

We can prove the security of the modified DMA-FE scheme in a manner similar to that of Theorem 5 except that Problem 2 is changed to Modified Problem 2, Lemma 20 is changed, where $\mathcal{B}_{2,h}$'s simulation is executed on Modified Problem 2, Game 2-h-1 is changed to Modified Game 2-h-1.

Here we only show the essence of the change by using Modified Game 2-h-1. The Modified Game 2-h-1 is the same as Game 2-h-1 except that $Z_t \xleftarrow{\cup} GL(n'_t, \mathbb{F}_q),\ U_t := (Z_t^{-1})^{\mathrm{T}}$ for $t = 1, \ldots, d$, where for each t there is a set $I_t := \{i_\kappa \mid \widetilde{\rho}(i_\kappa) = t,\ 1 \le \kappa \le \varphi\}$, and for $\kappa = 1, \ldots, \varphi$, the framed parts of Eq. (23) are changed to

$$\begin{aligned}
\vec{w}_\kappa &:= ((r_i \vec{e}_{t,1} + \omega_i \vec{v}_i, 0^{\kappa-1}, \xi_i, 0^{\varphi-\kappa}) \cdot Z_t,\quad r'_i \vec{e}_{t,1} + \omega'_i \vec{v}_i, 0^{\kappa-1}, \xi'_i, 0^{\varphi-\kappa}),\\
\vec{\overline{w}}_\kappa &:= ((r_i \vec{v}_i, 0^{\kappa-1}, \xi_i, 0^{\varphi-\kappa}) \cdot Z_t,\quad r'_i \vec{v}_i, 0^{\kappa-1}, \xi'_i, 0^{\varphi-\kappa}),
\end{aligned}$$

where $\xi_i, \xi'_i \xleftarrow{\cup} \mathbb{F}_q$.

By using Modified Problem 2, for $\rho(i_\kappa) = (t, \vec{v})$, $\mathcal{B}_{2,h}$ can simulate ciphertexts, $\boldsymbol{c}_{i_\kappa} := (\cdots, \vec{w}_\kappa, \cdots)_{\mathbb{B}_t}$ or $\boldsymbol{c}_{i_\kappa} := (\cdots, \vec{\overline{w}}_\kappa, \cdots)_{\mathbb{B}_t}$. By applying Lemma 25, we can prove Lemma 21 in a manner similar to the proof of Lemma 21.