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

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 a large class of (non-monotone) predicates is fully secure (adaptive-predicate unforgeable and perfectly 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) [11, 14, 17, 18, 21–24, 27, 30, 32]. 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 [24] 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

K. Kurosawa and G. Hanaoka (Eds.): PKC 2013, LNCS 7778, pp. 125–142, 2013.

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 [23, 24, 27], 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 the full version of this paper [26] that all MA-ABS schemes in [24] 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 [20] 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 [19] and it may be applicable to the DMA-ABE scheme.

1.2 Our Results

- This paper proposes the first DMA-ABS scheme, which supports a large class of 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 [13, 16] and [12], 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 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 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 [25]. 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 [25]) 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 perfectly 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., [24, 27]). See Table 1 in Section 4.5.
- 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 is 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* [28, 29]. 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, the top level strategy is based on Naor's paradigm [4], which is originally a conversion from identity-based encryption (IBE) to (ordinary) digital signatures, but in our case, an encryption counterpart, DMA-ABE, is converted to DMA-ABS. Therefore, DMA-ABE scheme is designed first, and then DMA-ABS is constructed on it.

To construct a DMA-ABE (or more generally DMA-FE) scheme for this purpose, we follow several established key ideas; dual pairing vector spaces (DPVS) [25, 27], global identifier gid [9], (random oracle) hashing of gid [20], dual system encryption [20, 31], 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 $\delta G := H(\mathsf{gid}) \in \mathbb{G}$ [27], which is essentially different from the technique using $H(\mathsf{gid})$ in [20] (see Section 4.3 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 ABE (FS and FE) schemes in [25, 27]. 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-ABE (DMA-FS and DMA-FE) schemes 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 and DMA-FE, $2n_t$-dimensional) hidden subspaces are employed for *semi-functional* forms of secret-keys and verification-texts. In the previous dual system encryption tricks [25, 27], 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 the full version [26]).

A new idea is also required to achieve the *privacy* condition for DMA-ABS, since no privacy condition is required for DMA-ABE or included in Naor's paradigm. Moreover, a *new re-randomization* technique should be developed in this paper to achieve the privacy of DMA-ABS, since the re-randomization technique for privacy in [27] is not effective in the DMA-ABS setting due to the fully distributed structure (see Section 4.2).

For more details on the techniques in the security proofs of DMA-ABS, see the full version [26].

1.4 Related Works

1. The *mesh signatures* [5] 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, 6–8, 10]. 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 [24], 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 the full version of this paper [26] 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 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 [25].

3 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., $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \le t \le d\}$*, 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 $\Gamma := \{(t, x_t) \mid x_t \in \mathbb{F}_q, 1 \le t \le d\}$.

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 the full version [26] 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* $\vec{f}^{\mathrm{T}} := (f_1, \ldots, f_r)^{\mathrm{T}} \xleftarrow{\cup} \mathbb{F}_q^r$*. 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 Decentralized Multi-Authority Attribute-Based Signatures (DMA-ABS)

4.1 Definitions for DMA-ABS

Definition 6 (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.

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 7 (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.*

Note that the above definition of perfect privacy is weaker than that in [24], since the attribute authorities are assumed to be honest in our definition, while they can be malicious in [24].

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

1. *Run* $\mathsf{gparam} \xleftarrow{\mathsf{R}} \mathsf{GSetup}(1^\lambda)$ *and give* gparam *to 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 *with queries including attribute authorities, t, from $S := T \setminus \widetilde{T}$ alone.*
3. *At the end, the adversary outputs $(m', \mathbb{S}', \sigma')$.*

Let $\Gamma_{\mathsf{gid}} := \{(t, x_t) \mid (t \in S,\ x_t,\ \mathsf{gid})$ *is queried to* $\mathsf{AttrGen}$ *oracle by $\mathcal{A}$}$\}$. *We say the adversary succeeds, if $(m', \mathbb{S}')$ was never queried to* AltSig *oracle, $\mathbb{S}'$ does not accept Γ_{gid} for any* gid, *$\mathbb{S}'$ includes attributes authorities, t, from S alone, and* $\mathsf{Ver}(\mathsf{pk}, m', \mathbb{S}', \sigma') = 1$.

Remark 3. The unforgeability defined above ensures that adversary $\mathcal{A}$ cannot forge a signature regarding uncorrupt authorities even if $\mathcal{A}$ makes key and signature queries to uncorrupt authorities. That is, the forging capability of any $\mathcal{A}$ is limited or localized to that of corrupt authorities as expected in DMA schemes (in contrast, it can be expanded to the whole system in MA schemes).

The model regarding *corrupt authorities* in this definition, however, is weaker than that in [24]. 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 including uncorrupt parties from S alone. On the other hand, the security on the model in [24] 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 $(\Gamma_S \cup \Gamma_{\widetilde{T}})$. Namely, the scope of forgery in [24] is wider (i.e., it covers a policy over $S \cup \widetilde{T}$) than that in our definition (i.e., it is limited to a policy over S). [1]

4.2 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 A) through Naor's paradigm. For the key techniques to construct DMA-FE from (non-decentralized) FE [25], we refer to Section 1.3. In the paradigm, collusion-resistant identity-based encryption (IBE) is transformed to unforgeable signatures, where (a hash

[1] The proposed scheme in this paper has been proven unforgeable only in our model due to some technical reason caused by no trusted setup (or no trapdoor) of our scheme.

value of) a message is used for an identity in IBE. To realize the Naor-like transformation in our DMA-FE, two-dimensional subspaces $\mathsf{span}\langle \boldsymbol{b}_{t,5}, \boldsymbol{b}_{t,6}\rangle$ (and their dual subspaces) are newly added for identity (message) embedding to all spaces $\mathbb{V}_t$ for $t > 0$. Note that the privacy condition is not included in Naor's paradigm.

In our variant of Naor's paradigm, 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 *published* in our DMA-ABS, while it is *secret* in the DMA-FE scheme. They are used 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.

Here, we remark an important difference in setup between (non-decentralized) ABS and DMA-ABS: While a part of $\widehat{\mathbb{B}}^*_0$, $\boldsymbol{b}^*_{0,1}$, is a master secret in ABS [27], there is no central space $\mathbb{V}_0$ in our DMA-ABS. To obtain unforgeability in our setting, the secret key $\boldsymbol{b}^*_{0,1}$ in ABS is distributed to all $(\boldsymbol{b}^*_{t,\iota})_{t>0;\iota=1,2}$. Therefore, we modify them to $(\widetilde{\boldsymbol{b}}^*_{t,\iota} := \pi \boldsymbol{b}^*_{t,\iota})_{t>0;\iota=1,2}$ with $\pi \xleftarrow{\cup} \mathbb{F}_q$ as a part of public key $\{\widehat{\mathbb{B}}^*_t\}_{t>0}$.

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 $\{\widehat{\mathbb{B}}^*_t\}_{(t,x_t)\in\Gamma}$. Since our DMA-FE (and DMA-ABS) lacks the central space $\mathbb{V}_0$, attribute vectors $(1, x_t)$ and $\delta(1, x_t)$ with $\delta \xleftarrow{\cup} \mathbb{F}_q$ are encoded in subspaces $\mathsf{span}\langle \boldsymbol{b}^*_{t,1}, \boldsymbol{b}^*_{t,2}\rangle$ and $\mathsf{span}\langle \boldsymbol{b}^*_{t,3}, \boldsymbol{b}^*_{t,4}\rangle$, for sk_Γ with $\Gamma := \{(t, x_t)\}$. In signature generation, both vectors are re-randomized independently using $(\widetilde{\boldsymbol{b}}^*_{t,\iota}, \boldsymbol{b}^*_{t,2+\iota})_{\iota=1,2}$, in a manner consistent with predicate $\mathbb{S}$.

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 $\mathsf{H}_2(m, \mathbb{S})$.

4.3 Proposed DMA-ABS Scheme

For matrix $X := (\chi_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N\times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, $\boldsymbol{g}X$ denotes $(\sum_{i=1}^N G_i\chi_{i,1}, \ldots, \sum_{i=1}^N G_i\chi_{i,N}) = (\sum_{i=1}^N \chi_{i,1}G_i, \ldots,$

$\sum_{i=1}^{N} \chi_{i,N} G_i$) by a natural multiplication of a N-dim. row vector and a $N \times N$ matrix. Thus, it holds that $e(\boldsymbol{g}X, \boldsymbol{h}(X^{-1})^{\mathrm{T}}) = e(\boldsymbol{g}, \boldsymbol{h})$ for any $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{V}$. The proposed scheme is given as:

$\mathsf{GSetup}(1^\lambda)$: $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,
$H_1 : \{0,1\}^* \to \mathbb{G}$; $H_2 : \{0,1\}^* \to \mathbb{F}_q$; 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 $\iota = 1, 2$,
$\boldsymbol{b}_{t,\iota} := (0^{\iota-1},\ G_0,\ 0^{13-\iota}) X_t$, $\boldsymbol{b}^*_{t,\iota} := (0^{\iota-1},\ G_1,\ 0^{13-\iota})(X_t^{-1})^{\mathrm{T}}$ for $\iota = 1, \ldots, 13$,

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

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

$\mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,13})$, $\mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,13})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,6}, \boldsymbol{b}_{t,13})$,
$\widehat{\mathbb{B}}^*_t := (\widetilde{\boldsymbol{b}}^*_{t,1}, \widetilde{\boldsymbol{b}}^*_{t,2}, \boldsymbol{b}^*_{t,3}, \ldots, \boldsymbol{b}^*_{t,6}, \boldsymbol{b}^*_{t,11}, \boldsymbol{b}^*_{t,12})$,
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. $G_2 = \pi G_1$,

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

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

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

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

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. $G_{\mathsf{gid}} = \delta G_1$,

$$\text{then } \boldsymbol{k}^*_t = (\ \overbrace{(1,\ x_t),}^{2}\ \overbrace{\delta(1,\ x_t),}^{2}\ \overbrace{0^6}^{6},\ \overbrace{\varphi_{t,1},\ \varphi_{t,2},}^{2}\ 0\ )_{\mathbb{B}^*_t}.$$

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

$$I \subseteq \{i \in \{1,\dots,\ell\} \mid [\rho(i) = (t, v_i) \ \wedge\ (t, x_t) \in \Gamma \ \wedge\ v_i = x_t] \vee [\rho(i) = \neg(t, v_i) \ \wedge\ (t, x_t) \in \Gamma \ \wedge\ v_i \neq x_t]\},$$

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

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

Remark : If $\mathrm{rank}(M) \geq \ell$, the set contains only 0^ℓ, i.e., $\beta_i = 0$ for $i = 1,..,\ell$.

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

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

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

$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\vec{f}' \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$ s.t. $\vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0$, $\vec{s}'^{\mathrm{T}} := (s'_1, \dots, s'_\ell)^{\mathrm{T}} := M \cdot \vec{f}'^{\mathrm{T}}$,

for $i = 1,\dots,\ell$, $\theta_i, \theta'_i, \theta''_i, \eta_i \xleftarrow{\mathsf{U}} \mathbb{F}_q$,

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

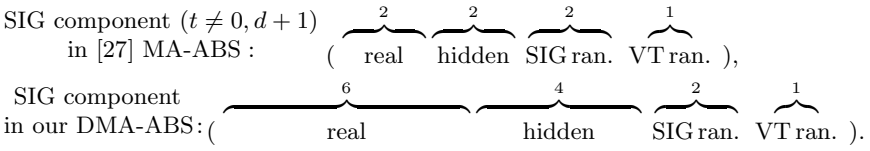
$$\boldsymbol{c}_i := (\overbrace{s_i(v_i,\ -1)}^{2}, \overbrace{s'_i(v_i,\ -1)}^{2}, \overbrace{\theta''_i(H_2(m, \mathbb{S}), -1)}^{2}, \overbrace{0^6}^{6}, \overbrace{\eta_i}^{1})_{\mathbb{B}_t},$$

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

Comparison with the MA-ABS Scheme in [27]. Okamoto-Takashima [27] 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.



4.4 Security of the Proposed DMA-ABS

The (standard) DLIN assumption is given in the full version [26].

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.*

The proofs of Theorems 1 and 2 are given in the full version of this paper [26].

4.5 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 [24] and MA-ABS in [27]) as well as the ABS scheme in the generic group model (instantiation 3 in [24]) 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., $M \in \mathbb{F}_q^{\ell \times r}$.

Table 1. Comparison with the Existing MA-ABS Schemes

	MPR10 [24] Instantiation 3	MPR10 [24] Instantiation 2	OT11 [27]	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

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 [20]). λ is the security parameter (e.g., 128).

5 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 [24]), 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 (1996)
2. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi (ed.) [15], pp. 108–125

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. 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)
5. Boyen, X.: Mesh Signatures. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 210–227. Springer, Heidelberg (2007)
6. Camenisch, J., Groß, T.: Efficient attributes for anonymous credentials. In: Ning, P., Syverson, P.F., Jha, S. (eds.) ACM Conference on Computer and Communications Security. pp. 345–356. ACM (2008)
7. Camenisch, J., Lysyanskaya, A.: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
8. Camenisch, J., Lysyanskaya, A.: Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
9. Chase, M.: Multi-authority Attribute Based Encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)
10. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Commun. ACM 28(10), 1030–1044 (1985)
11. Escala, A., Herranz, J., Morillo, P.: Revocable Attribute-Based Signatures with Adaptive Security in the Standard Model. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 224–241. Springer, Heidelberg (2011)
12. Estibals, N.: Compact Hardware for Computing the Tate Pairing over 128-Bit-Security Supersingular Curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. LNCS, vol. 6487, pp. 397–416. Springer, Heidelberg (2010)
13. FIPS PUB 180-1, 180-2: Secure hash standard. NIST (1995, 2002)
14. Guo, S., Zeng, Y.: Attribute-based signature scheme. In: ISA, pp. 509–511. IEEE (2008)
15. Halevi, S. (ed.): CRYPTO 2009. LNCS, vol. 5677. Springer, Heidelberg (2009)
16. ISO/IEC 15946-5: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation. ISO/IEC (2009)
17. Khader, D.: Attribute based group signature with revocation. IACR Cryptology ePrint Archive 2007, 241 (2007)
18. Khader, D.: Attribute based group signatures. IACR Cryptology ePrint Archive 2007, 159 (2007)
19. Lewko, A.: Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012)
20. Lewko, A., Waters, B.: Decentralizing Attribute-Based Encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011)
21. Li, J., Au, M.H., Susilo, W., Xie, D., Ren, K.: Attribute-based signature and its applications. In: Feng, D., Basin, D.A., Liu, P. (eds.) ASIACCS, pp. 60–69. ACM (2010)
22. Li, J., Kim, K.: Attribute-based ring signatures. IACR Cryptology ePrint Archive 2008, 394 (2008)

23. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. IACR Cryptology ePrint Archive 2008, 328 (2008)
24. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-Based Signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011)
25. 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`
26. Okamoto, T., Takashima, K.: Decentralized attribute-based signatures. IACR Cryptology ePrint Archive 2011, 701 (2011), full version of this paper, `http://eprint.iacr.org/2011/701`
27. Okamoto, T., Takashima, K.: Efficient Attribute-Based Signatures for Non-monotone Predicates in the Standard Model. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 35–52. Springer, Heidelberg (2011), full version is available at `http://eprint.iacr.org/2011/700`
28. 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)
29. 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)
30. 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)
31. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi (ed.) [15], pp. 619–636
32. Yang, P., Cao, Z., Dong, X.: Fuzzy identity based signature. IACR Cryptology ePrint Archive 2008, 2 (2008)

A Proposed DMA-FE

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 the full version [26]. In the description of the scheme, we assume that input vector $\vec{x}_t := (x_{t,1}, \ldots, x_{t,n_t})$ is normalized such that $x_{t,1} := 1$. (If $\vec{x}_t$ is not normalized, change it to a normalized one by $(1/x_{t,1}) \cdot \vec{x}_t$ assuming that $x_{t,1}$ is non-zero). In addition, we assume that input vector $\vec{v}_i := (v_{i,1}, \ldots, v_{i,n_t})$ satisfies that $v_{i,n_t} \neq 0$. For matrix $X := (\chi_{i,j})_{i,j=1,\ldots,N} \in \mathbb{F}_q^{N \times N}$ and element $\boldsymbol{g} := (G_1, \ldots, G_N)$ in N-dimensional $\mathbb{V}$, for notation $\boldsymbol{g}X$, refer to Section 4.3.

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

Remark : Given gparam, the following values can be computed by

anyone and shared by all parties:

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

$\mathsf{ASetup}(\mathsf{gparam}, t, n_t) : \mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, 5n_t+1, \mathsf{param}_{\mathbb{G}}),$

$X_t \xleftarrow{\mathsf{U}} GL(5n_t+1, \mathbb{F}_q),\ \boldsymbol{b}_{t,i} := (0^{i-1}, G_0, 0^{5n_t+1-i})X_t$ for $i = 1, \ldots, 5n_t+1,$

$\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,2n_t}, \boldsymbol{b}_{t,5n_t+1}),\ \ \mathsf{ask}_t := X_t,\ \ \mathsf{apk}_t := (\mathsf{param}_{\mathbb{V}_t}, \widehat{\mathbb{B}}_t),$

return $(\mathsf{ask}_t,\ \mathsf{apk}_t)$.

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

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

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

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

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

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

$\mathsf{Enc}(\mathsf{gparam}, \{\mathsf{apk}_t\},\ m,\ \mathbb{S} := (M, \rho)) :$

$\vec{f} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r,\ \vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}},\ s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}, \vec{f}' \xleftarrow{\mathsf{R}} \mathbb{F}_q^r \text{ s.t. } \vec{1} \cdot \vec{f}'^{\mathrm{T}} = 0,$

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

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

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

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

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

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

$\mathsf{Dec}(\mathsf{gparam}, \{\mathsf{apk}_t, \mathsf{usk}_{\mathsf{gid},(t,\vec{x}_t)} := (\mathsf{gid}, (t, \vec{x}_t), \boldsymbol{k}_t^*)\}, \mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell, c_{d+1})) :$

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

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

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

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

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