Downgradable Identity-Based Signatures and Trapdoor Sanitizable Signatures from Downgradable Affine MACs

Masahito Ishizaka and Shinsaku Kiyomoto

KDDI Research, Inc., Saitama, Japan.
{ma-ishizaka, kiyomoto}@kddi-research.jp

Abstract. Affine message authentication code (AMAC) (CRYPTO'14) is a group-based MAC with a specific algebraic structure. Downgradable AMAC (DAMAC) (CT-RSA'19) is an AMAC with a functionality that we can downgrade a message with an authentication tag while retaining validity of the tag. In this paper, we revisit DAMAC for two independent applications, namely downgradable identity-based signatures (DIBS) and trapdoor sanitizable signatures (TSS) (ACNS'08). DIBS are the digital signature analogue of downgradable identity-based encryption (CT-RSA'19), which allow us to downgrade an identity associated with a secret-key. In TSS, an entity given a trapdoor for a signed-message can partially modify the message while keeping validity of the signature. We show that DIBS can be generically constructed from DAMAC, and DIBS can be transformed into (wildcarded) hierarchical/wicked IBS. We also show that TSS can be generically constructed from DIBS. By instantiating them, we obtain the first wildcarded hierarchical/wicked IBS and the first invisible and/or unlinkable TSS. Moreover, we prove that DIBS are equivalent to not only TSS, but also their naive combination, named downgradable identity-based trapdoor sanitizable signatures.

Keywords: Downgradable Identity-Based Signatures · Trapdoor Sanitizable Signatures · Downgradable Affine Message Authentication Codes · (Wildcarded) Hierarchical/Wicked Identity-Based Signatures.

1 Introduction

Identity-Based Cryptosystems. In public-key encryption (PKE) system, a sender encrypts a plaintext using a public-key of a receiver, then the receiver decrypts it using her secret-key. Identity-based encryption (IBE) [28] is a PKE with an advanced functionality, where a receiver can choose any identity $id \in \{0,1\}^l$ for $l \in \mathbb{N}$ as her public-key. In IBE, we assume the existence of a trusted authority which privately generates a secret-key for an id. Hierarchical IBE (HIBE) [18,20] expresses each id as a vector of some sub-IDs, i.e., $id \in (\{0,1\}^*)^{\leq n}$. A secret-key for an id generates one for any of its descendants. Wicked IBE (WkIBE) [2] generalizes HIBE, where we can leave some sub-IDs blank to be determined in upcoming delegation. Wildcarded IBE (WIBE) [1,6] generalizes IBE, where each ciphertext ID can be *wildcarded*, i.e., $id \in \{0,1,*\}^l$.

Digital signature is a tool to verify by using a public-key of a signer that a digital signature on a digital document was produced from her secret-key. There exist the digital-signature analogue of the IBE primitives, namely identity-based signatures (IBS) [28], HIBS, WkIBS and WIBS. We have known that any $(n+1)$-level HIBE can be transformed into an n-level HIBS [21,18]. Analogously, 2-level HIBE (resp. IBE) can be transformed into IBS (resp. digital signature). The technique cannot be straightforwardly applied to *wildcarded* IBS primitives.

Affine MACs (AMACs). We have known that AMAC [8] is useful to construct various ID-based cryptosystems with (almost) tight security reduction. AMAC is an algebraic MAC with a group description $(\mathbb{G}, p, g)$, where $\mathbb{G}$ is a group, p is a prime and g is a generator of $\mathbb{G}$. For $\boldsymbol{a} \in \mathbb{Z}_p^n$, let $[\boldsymbol{a}]$ denote $(g^{a_1}, \cdots, g^{a_n})^\top \in \mathbb{G}^n$. A tag $\tau = ([\boldsymbol{t}], [u])$ on $msg \in \mathcal{M}$ consists of a randomness $[\boldsymbol{t}] \in \mathbb{G}^n$ and a message-depending $[u] \in \mathbb{G}$, satisfying $u = \sum_{i=0}^{l} f_i(msg)\boldsymbol{x}_i^\top \boldsymbol{t} + \sum_{i=0}^{l'} f_i'(msg)x_i \in \mathbb{Z}_p$, where $f_i, f_i' : \mathcal{M} \to \mathbb{Z}_p$ are public functions, and $\boldsymbol{x}_i \in \mathbb{Z}_p^n$ and $x_i \in \mathbb{Z}_p$ are from the secret-key sk_{MAC}. Pseudo-randomness [8] guarantees that no PPT adversary, who arbitrarily chooses msg^* then receives $([h]_1, [\boldsymbol{h}_0]_1, [h_1]_T)$, can distinguish the case where they are honestly generated, i.e., $h \leftsquigarrow \mathbb{Z}_p$, $\boldsymbol{h}_0 \coloneqq \sum_{i=0}^{l} f_i(msg^*)\boldsymbol{x}_i h$ and $h_1 \coloneqq \sum_{i=0}^{l'} f_i'(msg^*)x_i h$, from the case where they are randomly generated[1]. Note that the adversary can arbitrarily chooses $msg \neq msg^*$ to get a tag on it. Blazy et al. [8] proposed two AMAC schemes, one of which is based on a hash-proof system (HPS) [16] and pseudo-random under k-Lin assumption.

Blazy et al. [8] proposed a generic construction of anonymous identity-based KEM (IBKEM) with identity-length $l \in \mathbb{N}$ from an AMAC scheme with message-length l. The key-issuing authority randomly generates sk_{MAC} for the AMAC and perfectly-hiding commitments $\{Z_i\}$ (resp. $\{\boldsymbol{z}_i\}$) to $\{\boldsymbol{x}_i\}$ (resp. $\{x_i\}$). A secret-key for an identity id is identical to a Bellare-Goldwasser (BG) signature [5]. Specifically, it consists of an AMAC tag $([\boldsymbol{t}]_2, [u]_2)$ on a message id and an NIZK-proof [19] $[\boldsymbol{u}]_2$ w.r.t. the commitments which proves that the tag has been correctly generated. Key-encapsulation and key-decapsulation are a randomized variant of the verification of the NIZK proof. They proved that its adaptive security is tightly reduced to the pseudo-randomness of the AMAC.

In delegatable AMAC (DlgAMAC) [8], each message is a vector of some sub-messages. We can transform a valid tag on a message into another valid tag on any of its descendant messages. The pseudo-randomness for DlgAMAC is a natural extension from the one for AMAC, where the tag-generation oracle returns not only a tag but also variables for *delegating* or *re-randomizing* the tag. They [8] showed that their HPS-based AMAC is delegatable. Their anonymous HIBKEM based on DlgAMAC is a natural extension from the AMAC-based AIBKEM. Each secret-key for a hierarchical ID consists of a BG-signature on the ID and variables for delegating or re-randomizing the BG-signature.

[1] In this paper, $\leftsquigarrow$ means that we select an element uniformly at random from a space.

Sanitizable Signatures (SS). If we modify a message signed by an ordinary digital signature scheme, the signature becomes invalid. SS [3] allow a *sanitizer* to partially modify a (signed-)message. A signer signs $msg \in \{0,1\}^m$ with choosing a (public-key of) sanitizer and a set $\mathbb{T} \subseteq [1,m]$ of its modifiable bits. The sanitizer can modify msg to msg' according to the rule $\mathbb{T}$ by using her secret-key. Various security notions, i.e., (existential) unforgeability, immutability, transparency, privacy, invisibility, unlinkability and signer/sanitizer-accountability, have been formally defined [9,10,22,13,4]. Invisibility [13] guarantees that the set $\mathbb{T}$ of modifiable bits is hidden. Camenisch et al. [13] proposed the first invisible SS scheme. Beck et al. [4] proposed one achieving stronger security notions. Unlinkability [10] guarantees that a sanitized signature cannot be linked to its source. Unlinkable (and non-invisible) SS schemes were proposed in [10,17,11]. Bultel et al. [12] proposed a simple generic construction of (accountable) sanitizable signatures (SS) from non-accountable SS (NASS) and verifiable ring signatures (VRS), from which they obtained the first invisible and unlinkable SS (IUSS), which is an affirmative answer to an open problem posed in [13]. However, their NASS scheme based on equivalence class signatures is secure in the generic group and random oracle model. Such a strong assumption is inherited by their IUSS scheme.

Trapdoor Sanitizable Signatures (TSS). In TSS [14,29], each signer does not choose a public-key of a sanitizer in signing. Each signature is associated with a trapdoor, which enables any user sanitize the signature. An advantage of TSS is that each signer can designate any single (or multiple) user as sanitizer at anytime. We believe that an overlooked significant advantage is that it could be a building block of the ordinary SS. We believe that a simple generic SS construction based on TSS and PKE[2] can be the NASS scheme in the IUSS by Bultel et al., where its invisibility (resp. unlinkability) is implied by the same security of the TSS. We propose the first invisible and unlinkable TSS scheme secure under standard assumptions. As a result, we could obtain the first IUSS secure under standard assumptions. Justifying the idea is a future work.

1.1 This Work

Downgradable AMACs. In downgradable affine MAC (DAMAC) [7], we can *downgrade* a message $msg \in \{0,1\}^m$ with an authentication tag to another $msg' \in \{0,1\}^m$. The downgrade relation holds when, for every $i \in [1,m]$, if $msg[i] \neq msg'[i]$, then $msg[i] = 1$. Differently from the definition of DAMAC [7], we introduce an algorithm `Weaken` which weakens *downgradability* of a tag. Each *fresh* tag on msg has the *full* downgradability $\mathbb{I}_1(msg)$[3], which means that every bit of the message whose value is 1 can be changed to 0. The downgradability can be weakened by `Weaken` to any of its subset $\mathbb{J} \subseteq \mathbb{I}_1(msg)$.

[2] A signer generates a TSS signature and its trapdoor using her TSS secret-key, then encrypts the trapdoor under a PKE public-key of a sanitizer. The sanitizer decrypts the ciphertext using his PKE secret-key.

[3] For a binary string $str \in \{0,1\}^m$, $\mathbb{I}_1(str)$ denotes a set $\{i \in [1,m] \text{ s.t. } str[i] = 1\}$.

Our definition of pseudo-randomness for DAMAC is not a naive extension from the one for AMAC (DlgAMAC) in [8], but weaker one. We neither consider the pseudo-randomness of $[\boldsymbol{h}_0]_1$ nor allow the adversary to use tag-generation oracle after the challenge phase. We prove that the HPS-based AMAC [8] is a DAMAC which satisfies the pseudo-randomness under the k-Lin assumption.

Downgradable IBS. In downgradable IBE (DIBE) [7], we can transform a secret-key for an $id \in \{0,1\}^l$ into one for a downgraded $id' \preceq id$. Our downgradable IBS (DIBS) are not the digital-signature analogue of DIBE [7], but stronger because of `Weaken`, which weakens downgradability of a secret-key. As explained below, the algorithm works to construct various more efficient non-wildcarded IBS. We formally define EUF-CMA security and (statistical) signer-privacy which means that each signature has no specific info about the secret-key generating it.

We propose a generic DIBS construction from DAMAC. First, we consider a natural extension from the DlgAMAC-based AHIBKEM [8] to a DAMAC-based DIBKEM. Second, we transform it into a DAMAC-based DIBS using the same technique as the HIBE-to-HIBS transformation [21,18]. Our DIBS (with identity-length l and message-length m) adopt a DAMAC with message-length $l+m$. A secret-key for $id \in \{0,1\}^l$ with downgradability $\mathbb{J} \subseteq \mathbb{I}_1(id)$ consists of a BG-signature $([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2)$ on a message $id||1^m$ and some information for re-randomization or downgrade. Each secret-key initially has the full downgradability i.e., $\mathbb{I}_1(id) \bigcup [l+1, l+m]$. It can be weakened to any $\mathbb{J} \bigcup [l+1, l+m]$ s.t. $\mathbb{J} \subseteq \mathbb{I}_1(id)$. A signer with id generates a signature on msg by re-randomizing the secret-key then downgrading the BG-signature on $id||1^m$ to one on $id||msg$. To verify the signature, we firstly encapsulate a random key under $id||msg$ then decapsulating it using the signature (being a DIBKEM-secret-key for $id||msg$).

We propose two transformations from DIBS to various IBS, i.e., (W)IBS, (W)HIBS and (W)WkIBS, where the initial W means *wildcarded*. The first transformations adopt the same technique as the ones from DIBE to various IBE [7]. The transformations effectively work for all of the IBS (incl. wildcarded ones). We show that by instantiating them by the DAMAC-based DIBS, we obtain a WIBS scheme whose reduction-cost for unforgeability is $\mathcal{O}(q)$[4], which is (asymptotically) smaller than $\mathcal{O}(q^2)$ of the WIBS scheme instantiated from the ABS scheme [27], and also obtain the first WHIBS and WWkIBS schemes secure under standard assumptions. The second transformations effectively use the algorithm `Weaken` and work for only non-wildcarded IBS. We show that the second transformations can produce more efficient IBS schemes than the first ones especially in size of public-parameter.

Trapdoor SS. Our TSS are functionally stronger than the original TSS [14]. Firstly, each signature (and its trapdoor) can be re-randomized. In other words, the sanitizing algorithm `Sanit`[5] is *fully-probabilistic*. The property is necessary

[4] q denotes the number that key-generation and signing oracles are used.

[5] `Sanit` takes a signature σ and trapdoor td (on a message msg and $\mathbb{T}$), and a modified $\overline{msg}$ and $\overline{\mathbb{T}}$, then returns a modified $\overline{\sigma}$ and $\overline{td}$

to achieve our definition of unlinkability. Either of the existing TSS constructions [14,29] cannot achieve it because its `Sanit` is not fully-probabilistic. Secondly, each signature can modify its modifiable parts $\mathbb{T}$ to any subset $\overline{\mathbb{T}} \subseteq \mathbb{T}$. The original TSS assume that $\mathbb{T}$ is permanently fixed.

We define (existential) unforgeability, transparency, (weak) privacy, unlinkability and invisibility. Analogously to the SS, either of transparency and unlinkability implies privacy. We originally define *strong* privacy, which implies either of transparency and unlinkability.

We show that TSS (with message-length m) are constructed from DIBS (with identity-length m). A function $\Phi_{\mathbb{T}}$ transforms a message. $\Phi_{\mathbb{T}}(msg)(=: msg') \in \{0,1\}^m$ is identical to msg except that for any $i \in [1,m]$ if $i \in \mathbb{T}$ and $msg[i] = 0$ then $msg'[i]$ becomes 1. In general, a TSS signature on a message msg with modifiable parts $\mathbb{T}$ and its trapdoor are a DIBS secret-key for identity msg with downgradability $\emptyset$ and one for identity $\Phi_{\mathbb{T}}(msg)$ with downgradability $\mathbb{T}$, respectively. In verification, we verify the DIBS secret-key for identity msg. Specifically, we make it generate a DIBS signature on a random DIBS message then verifies it. We prove that it is secure if the underlying DIBS scheme is secure. As a result, we obtain the first invisible and/or unlinkable TSS scheme.

Equivalence among DIBS, TSS and DIBTSS. We also show that DIBS are generically constructed from TSS. Thus, DIBS and TSS are equivalent.

Moreover, we naturally combine the two primitives, and name it *downgradable identity-based TSS* (DIBTSS). In DIBTSS, each identity for a secret-key can be downgraded, and each signature can be sanitized by a trapdoor. We show that DIBTSS are equivalent to either of DIBS and TSS.

1.2 Paper Organization

In Sect. 2, we explain some notations, asymmetric bilinear pairing, matrix Diffie-Hellman assumption, and (wildcarded) wicked identity-based signatures. In Sect. 3, we define syntax and pseudo-randomness security for DAMAC, then propose a secure DAMAC system. In Sect. 4, we define syntax and security for DIBS, then propose a generic construction based on DAMAC. In Sect. 5, we define syntax and security for TSS, then propose a generic construction from DIBS. We also prove that TSS generically construct DIBS. In Sect. 6, we introduce DIBTSS.

2 Preliminaries

Notations. 1^λ for $\lambda \in \mathbb{N}$ denotes a security parameter. PPTA_λ denotes a set of all probabilistic algorithms which runs in time polynomial in λ. PA denotes all probabilistic algorithms. We say that a function $f : \mathbb{N} \to \mathbb{R}$ is negligible if $\forall c \in \mathbb{N}$, $\exists x_0 \in \mathbb{N}$ s.t. $\forall x \geq x_0$, $f(x) \leq x^{-c}$. NGL_λ denotes a set of all negligible functions in λ. For a binary string $x \in \{0,1\}^n$, $x[i] \in \{0,1\}$ for $i \in [1,n]$ denotes the value of its i-th bit. For a string $x \in \mathbb{X}^n$, e.g., $\mathbb{X}$ is $\{0,1\}$ or $\{0,1,*\}$, $\mathbb{I}_b(x)$ for $b \in \mathbb{X}$ denotes the set $\{i \in [1,n]$ s.t. $x[i] = b\}$. For $x, y \in \{0,1\}^n$, the relation $x \preceq y$

holds if $\bigwedge_{i\in[1,n]} x[i]=1 \implies y[i]=1$. For $x,y\in\{0,1\}^n$ and a set $\mathbb{J}\subseteq \mathbb{I}_1(y)$, the relation $x \preceq_{\mathbb{J}} y$ holds if $\bigwedge_{i\in[1,n]\setminus\mathbb{J}} x[i]=y[i] \bigwedge_{i\in\mathbb{J}} x[i]=1 \implies y[i]=1$. $a \leftsquigarrow A$ means that we extract an element a uniformly at random from a set A. For a matrix $A\in\mathbb{N}^{(k+1)\times k}$, $\bar{A}\in\mathbb{N}^{k\times k}$ denotes the square matrix composed of the first k rows of A, and $\underline{A}\in\mathbb{N}^{1\times k}$ denotes the lowest row of A.

Matrix Diffie-Hellman Assumption. Let $\mathcal{G}_{BG}$ denote a generator of asymmetric bilinear pairing. Let $\lambda\in\mathbb{N}$. $\mathcal{G}_{BG}$ takes 1^λ, then generates $(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g_1,g_2)$. p is a prime of length λ. $(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T)$ are multiplicative groups of order p. g_1 and g_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ is an asymmetric function, computable in polynomial time and satisfying both of the following conditions: (i) Bilinearity: For every $a,b\in\mathbb{Z}_p$, $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$. (ii) Non-degeneracy: $e(g_1,g_2)\neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ denotes the unit element of $\mathbb{G}_T$.

Note that $g_T := e(g_1,g_2)$ is a generator of $\mathbb{G}_T$. For $s\in\{1,2,T\}$ and $a\in\mathbb{Z}_p$, $[a]_s$ denotes $g_s^a\in\mathbb{G}_s$. Generally, for $s\in\{1,2,T\}$ and a matrix $A\in\mathbb{Z}_p^{n\times m}$ whose (i,j)-th element is $a_{ij}\in\mathbb{Z}_p$, $[A]_s\in\mathbb{G}^{n\times m}$ denotes a matrix whose (i,j)-th element is $g_s^{a_{ij}}\in\mathbb{G}_s$. Obviously, from $[a]_s$ and an integer $x\in\mathbb{Z}_p$, $[xa]_s\in\mathbb{G}_s$ is efficiently computable. From $[a]_1$ and $[b]_2$ (for $b\in\mathbb{Z}_p$), $[ab]_T$ is also efficiently computable. Note that for $\boldsymbol{a},\boldsymbol{b}\in\mathbb{Z}_p^n$, $\left[\boldsymbol{a}^\top\boldsymbol{b}\right]_T = e([\boldsymbol{a}]_1,[\boldsymbol{b}]_2)=e([\boldsymbol{b}]_1,[\boldsymbol{a}]_2)$.

Based on [16,8,23], we define matrix Diffie-Hellman assumption.

Definition 1. *Let $k,l\in\mathbb{N}$ s.t. $l>k$. We call a set $\mathcal{D}_{l,k}$ a matrix distribution if it consists of matrices in $\mathbb{Z}_p^{l\times k}$ of full rank k and extracting an element from it uniformly at random can be efficiently done.*

In this paper, $\mathcal{D}_k$ denotes $\mathcal{D}_{k+1,k}$. W.l.o.g., we assume that the first k rows of $A\leftsquigarrow\mathcal{D}_{l,k}$ form an invertible matrix (which implies that A is of full rank k).

Definition 2. *Let $\mathcal{D}_{l,k}$ be a matrix distribution. Let $s\in\{1,2,T\}$. $\mathcal{D}_{l,k}$-matrix Diffie-Hellman (MDDH) assumption holds relative to $\mathcal{G}_{BG}$ in group $\mathbb{G}_s$, if for every $\mathcal{A}\in\mathsf{PPTA}_\lambda$, there exists $\epsilon\in\mathsf{NGL}_\lambda$ s.t. $\mathtt{Adv}^{\mathcal{D}_{l,k}\text{-}\mathit{MDDH}}_{\mathcal{A},\mathcal{G}_{BG},\mathbb{G}_s}(\lambda) := |\Pr[1\leftarrow\mathcal{A}(gd,[A]_s,[A\boldsymbol{w}]_s)]-\Pr[1\leftarrow\mathcal{A}(gd,[A]_s,[\boldsymbol{u}]_s)]|<\epsilon$, where $gd:=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g_1,g_2)\leftarrow\mathcal{G}_{BG}(1^\lambda)$, $A\leftsquigarrow\mathcal{D}_{l,k}$, $\boldsymbol{w}\leftsquigarrow\mathbb{Z}_p^k$ and $\boldsymbol{u}\leftsquigarrow\mathbb{Z}_p^l$.*

Following lemma guarantees that the assumption is self-reducible [16].

Lemma 1. *For any $k,l\in\mathbb{N}$ s.t. $l>k$ and any matrix distribution $\mathcal{D}_{l,k}$, the $\mathcal{D}_{l,k}$-MDDH assumption is random self-reducible. In particular, for any $m\in\mathbb{N}$ s.t. $m>1$ and any $\mathcal{A}\in\mathsf{PPTA}_\lambda$, there exists $\mathcal{B}\in\mathsf{PPTA}_\lambda$ s.t.*

$$(l-k)\mathtt{Adv}^{\mathcal{D}_{l,k}\text{-}\mathit{MDDH}}_{\mathcal{A},\mathcal{G}_{BG},\mathbb{G}_s}(\lambda)+\frac{1}{p-1}$$
$$\geq \mathtt{Adv}^{(\mathcal{D}_{l,k},m)\text{-}\mathit{MDDH}}_{\mathcal{B},\mathcal{G}_{BG},\mathbb{G}_s}(\lambda) := \left|\Pr\left[1\leftarrow\mathcal{B}(gd,[A]_s,[AW]_s)\right]-\Pr\left[1\leftarrow\mathcal{B}(gd,[A]_s,[U]_s)\right]\right|,$$

where $gd=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g_1,g_2)\leftarrow\mathcal{G}_{BG}(1^\lambda)$, $A\leftsquigarrow\mathcal{D}_{l,k}$, $W\leftsquigarrow\mathbb{Z}_p^{k\times m}$ and $U\leftsquigarrow\mathbb{Z}_p^{l\times m}$.

Corollary 1 is directly obtained from *Lemma 4* in [24].

Corollary 1. *For any prime p and $n\in\mathbb{N}$, $\Pr[\mathtt{rank}(S)\neq n \mid S\leftsquigarrow\mathbb{Z}_p^{n\times n}]\leq\frac{1}{p-1}$.*

2.1 Wicked IBS and Wildcarded Wicked IBS (WkIBS, WWkIBS)

We define WWkIBS and WkIBS. Definitions of IBS and wildcarded IBS (WIBS) can be seen in Sect. A.

Syntax. WWkIBS consist of following 4 polynomial time algorithms.

Setup `Setup`**:** $\mathcal{I}_{wk} := (\{0,1\}^l \bigcup \{\#\})^n$ (resp. $\mathcal{I}_{wwk} := (\{0,1,*\}^l \bigcup \{\#\})^n$) denotes the space of identity associated with a secret-key (resp. signature), where # means that sub-identity for the block is undetermined. m denotes length of a message. `Setup` takes 1^λ, l, m and n, then returns master public-key mpk and master secret-key msk (identically a secret-key for $\#^n$). We write $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m, n)$.

Key-Generation `KGen`**:** It takes a secret-key sk, an $id \in \mathcal{I}_{wk}$ and an $id' \in \mathcal{I}_{wk}$, then outputs a secret-key sk'. We write $sk' \leftarrow \texttt{KGen}(sk, id, id')$.

Siging `Sig`**:** It takes a secret-key sk, an $id \in \mathcal{I}_{wk}$, a wildcarded $wid \in \mathcal{I}_{wwk}$ and a message $msg \in \{0,1\}^m$, then outputs a signature σ. We write $\sigma \leftarrow \texttt{Sig}(sk, id, wid, msg)$.

Verification `Ver`**:** It takes a signature σ, a wildcarded $wid \in \mathcal{I}_{wwk}$ and a message $msg \in \{0,1\}^m$, then outputs 1 or 0. We write $1/0 \leftarrow \texttt{Ver}(\sigma, wid, msg)$.

We require every WWkIBS scheme to be correct. Let $\mathcal{I} := \{0,1\}^l$ and $\mathcal{I}_w := \{0,1,*\}^l$. We define three relation algorithms. R_w takes $id \in \mathcal{I}$ and $wid \in \mathcal{I}_w$, then outputs 1 if $\forall i \in [1,l]$, $id[i] \neq wid[i] \implies wid[i] = *$, or 0 otherwise. R_{wk} takes $id, id' \in \mathcal{I}_{wk}$, then outputs 1 if $\forall i \in [1,n]$, $id_i \neq id'_i \implies id_i = \#$, or 0 otherwise. $\mathcal{R}_{wwk}$ takes $id \in \mathcal{I}_{wk}$ and $wid \in \mathcal{I}_{wwk}$, then outputs 1 if $\forall i \in [1,n]$, $wid_i = \# \implies id_i = \#$ and $wid_i \in \{0,1,*\}^l \implies 1 \leftarrow R_w(id_i, wid_i)$, or 0 otherwise. We say that a WWkIBS scheme is correct, if $\forall \lambda, l, m, n \in \mathbb{N}$, $\forall (mpk, msk(= sk_{\#^n})) \leftarrow \texttt{Setup}(1^\lambda, l, m, n)$, $\forall id_1 \in \mathcal{I}_{wk}$, $\forall sk_{id_1} \leftarrow \texttt{KGen}(sk_{\#^n}, \#^n, id_1)$, $\forall id_2 \in \mathcal{I}_{wk}$ s.t. $1 \leftarrow R_{wk}(id_1, id_2)$, $\forall sk_{id_2} \leftarrow \texttt{KGen}(sk_{id_1}, id_1, id_2)$, $\cdots$, $\forall id_k \in \mathcal{I}_{wk}$ s.t. $1 \leftarrow R_{wk}(id_{k-1}, id_k)$, $\forall sk_{id_k} \leftarrow \texttt{KGen}(sk_{id_{k-1}}, id_{k-1}, id_k)$, $\forall msg \in \{0,1\}^m$, $\forall wid \in \mathcal{I}_{wwk}$ s.t. $1 \leftarrow \mathcal{R}_{wwk}(id_k, wid)$, $\forall \sigma \leftarrow \texttt{Sig}(sk_{id_k}, id_k, wid, msg)$, $1 \leftarrow \texttt{Ver}(\sigma, wid, msg)$.

Existential Unforgeability. We define existential unforgeability against chosen-messages attacks (EUF-CMA). For a probabilistic algorithm $\mathcal{A}$, the experiment $\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\text{WWkIBS}},\mathcal{A}}$ w.r.t. a WWkIBS scheme Σ_{WWkIBS} is defined as follows.

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\text{WWkIBS}},\mathcal{A}}(1^\lambda, l, m, n)$:
  $(mpk, msk(= sk_{\#^n})) \leftarrow \texttt{Setup}(1^\lambda, l, m, n)$.
  $(\sigma^*, wid^* \in \mathcal{I}_{wwk}, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
.......................................................................
    $-\mathfrak{Reveal}(id \in \mathcal{I}_{wk})$: $sk \leftarrow \texttt{KGen}(msk, \#^n, id)$. $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{id\}$. Rtn $sk$.
    $-\mathfrak{Sign}(id \in \mathcal{I}_{wk}, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$: Rtn $\perp$ if $0 \leftarrow \mathcal{R}_{wwk}(id, wid)$.
      $\sigma \leftarrow \texttt{Sig}(\texttt{KGen}(msk, \#^n, id), wid, msg)$. $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(wid, msg, \sigma)\}$. Rtn $\sigma$.
.......................................................................
  Rtn 0 if $\bigvee_{id \in \mathbb{Q}_r} 1 \leftarrow \mathcal{R}_{wwk}(id, wid^*) \bigvee_{(wid, msg, \cdot) \in \mathbb{Q}_s} (wid, msg) = (wid^*, msg^*)$
  Rtn 1 if $1 \leftarrow \texttt{Ver}(\sigma^*, wid^*, msg^*)$. Rtn 0.
```

Definition 3. *A scheme Σ_{WWkIBS} is* ***EUF-CMA****, if $\forall \lambda, l, m, n \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ s.t. $\boldsymbol{Adv}^{\textit{EUF-CMA}}_{\Sigma_{\mathrm{WWkIBS}},\mathcal{A},l,m,n}(\lambda) := \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{EUF-CMA}}_{\Sigma_{\mathrm{WkIBS}},\mathcal{A}}(1^\lambda, l, m, n)] < \epsilon$.*

Signer-Privacy. Signer-privacy means that a signature associated with a wildcarded identity $wid \in \mathcal{I}_{wwk}$ does not leak any information about the secret-key for id s.t. $1 \leftarrow \mathcal{R}_{wwk}(id, wid)$ which has generated the signature. For an algorithm $\mathcal{A}$, we consider the following two experiments. In the experiment with $b = 0$, every command with grey background is ignored.

```
$\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\mathrm{WWkIBS}},\mathcal{A},b}(1^\lambda, l, m, n)$:   // $b \in \{0, 1\}$.
  $(mpk, msk(= sk_{\#^n})) \leftarrow \mathtt{Setup}(1^\lambda, l, m, n)$. $(mpk, msk'(\ni sk_{\#^n})) \leftarrow \mathtt{Setup}'(1^\lambda, l, m, n)$.
  Rtn $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Delegate},\mathfrak{Sign}}(mpk, msk)$, where
....................................................................................................
  $-\mathfrak{Reveal}(id \in \mathcal{I}_{wk})$: $sk \leftarrow \mathtt{KGen}(sk_{\#^n}, \#^n, id)$. $sk \leftarrow \mathtt{KGen}'(msk', \#^n, id)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id)\}$. Rtn $sk$.
  $-\mathfrak{Delegate}(sk, id, id' \in \mathcal{I}_{wk})$: Rtn $\perp$ if $(sk, id) \notin \mathbb{Q} \bigvee 0 \leftarrow R_{wk}(id, id')$.
    $sk' \leftarrow \mathtt{KGen}(sk, id, id')$. $sk' \leftarrow \mathtt{KGen}'(sk, id, id')$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id')\}$. Rtn $sk'$.
  $-\mathfrak{Sign}(sk, id \in \mathcal{I}_{wk}, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
    Rtn $\perp$ if $(sk, id) \notin \mathbb{Q} \bigvee 0 \leftarrow \mathcal{R}_{wwk}(id, wid)$.
    $\sigma \leftarrow \mathtt{Sig}(sk, id, wid, msg)$. $\sigma \leftarrow \mathtt{Sig}'(msk', wid, msg)$. Rtn $\sigma$.
```

Definition 4. *A scheme Σ_{WWkIBS} is statistically signer private, if for every $\lambda, l, m, n \in \mathbb{N}$ and every probabilistic algorithm $\mathcal{A}$, there exist polynomial time algorithms $\Sigma'_{\mathrm{WWkIBS}} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Sig}'\}$ and a negligible function $\epsilon \in \mathsf{NGL}_\lambda$ such that $\boldsymbol{Adv}^{\textit{SP}}_{\Sigma_{\mathrm{WWkIBS}},\Sigma'_{\mathrm{WWkIBS}},\mathcal{A},l,m,n}(\lambda) := |\Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{SP}}_{\Sigma_{\mathrm{WWkIBS}},\mathcal{A},0}(1^\lambda, l, m, n)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{SP}}_{\Sigma_{\mathrm{WWkIBS}},\mathcal{A},1}(1^\lambda, l, m, n))]|$ is less than ϵ.*

Remarks on WkIBS. WkIBS are the same as WWkIBS except that each identity wid associated with a signature is non-wildcarded, i.e., $wid \in \mathcal{I}_{wk}$. We do not consider signer-privacy for WkIBS.

3 Downgradable Affine MACs (DAMACs)

A randomized message authentication code (MAC) consists of following 3 polynomial-time algorithms. Key-generation $\mathtt{Gen}_{\mathrm{MAC}}$ takes a system parameter par, then randomly generates a secret-key sk_{MAC}. Tag-generation $\mathtt{Tag}$ takes a secret-key sk_{MAC} and a message $msg \in \mathcal{M}$, then randomly generates a tag τ. Tag-verification $\mathtt{Ver}$ takes a secret-key sk_{MAC}, $msg \in \mathcal{M}$ and a tag τ, then (deterministically) returns a bit 1 or 0.

3.1 Our Model

Affine MACs (AMACs) [8] over $\mathbb{Z}_p^n$ (for $n \in \mathbb{N}$) are group-based MACs with a specific algebraic structure. Downgradable AMACs (DAMACs) with message space $\mathcal{M} = \{0,1\}^l$ are AMACs, where we can *downgrade* a message $msg \in \{0,1\}^l$ with a tag to another $msg' \in \{0,1\}^l$ s.t. $msg' \preceq msg$ while keeping validity of the tag (using the algorithm Down). Each tag is associated with a special key for downgrade. Initially, the key has the full downgradability. We can arbitrarily weaken the downgradability (using the algorithm Weaken). Our definition for DAMAC is a natural extension from the one for AMACs in [8] and essentially different from the one for DAMACs in [7].

Definition 5. *We say that a MAC system* $\Sigma_{\mathrm{MAC}} = \{\mathtt{Gen}_{MAC}, \mathtt{Tag}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Ver}\}$ *is downgradable over* $\mathbb{Z}_p^n$ *if it satisfies the following conditions.*

- $\mathtt{Gen}_{MAC}(par)$ *takes a public parameter par including the bilinear groups description* $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$*, then returns* sk_{MAC}*. We parse* sk_{MAC} *as* $(B, \boldsymbol{x}_0, \boldsymbol{x}_1, \cdots, \boldsymbol{x}_l, x)$*, where* $B \in \mathbb{Z}_p^{n \times n'}$*,* $\boldsymbol{x}_i \in \mathbb{Z}_p^n$ *and* $x \in \mathbb{Z}_p$*, for integers* n*,* n' *and* l*. Let* $\mathcal{M} := \{0,1\}^l$*.*
- $\mathtt{Tag}(sk_{\mathrm{MAC}}, msg \in \mathcal{M})$ *chooses* $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$*, computes* $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^n$*, for every* $i \in \mathbb{I}_1(msg)$*,* $d_i := h_i(msg)\boldsymbol{x}_i^\top \boldsymbol{t} \in \mathbb{Z}_p$*, and*

  $$u := \sum_{i=0}^{l} f_i(msg)\boldsymbol{x}_i^\top \boldsymbol{t} + x \in \mathbb{Z}_p, \tag{1}$$

  where the functions $f_i, h_i : \mathcal{M} \to \mathbb{Z}_p$ *are public ones which satisfy that for every* $msg, msg' \in \{0,1\}^l$ *s.t.* $msg' \preceq msg$ *and every* $i \in [1, l]$*, it holds that*

  $$f_i(msg') = \begin{cases} f_i(msg) & (\textit{if } msg'[i] = msg[i]), \\ f_i(msg) - h_i(msg) & (\textit{otherwise}). \end{cases}$$

  It returns $\tau_{msg}^{\mathbb{I}_1(msg)} := ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(msg)\}) \in \mathbb{G}_2^n \times \mathbb{G}_2 \times \mathbb{G}_2^{|\mathbb{I}_1(msg)|}$*.*
- $\mathtt{Weaken}(\tau_{msg}^{\mathbb{J}}, msg \in \mathcal{M}, \mathbb{J} \subseteq \mathbb{I}_1(msg), \mathbb{J}' \subseteq \mathbb{J})$ *parses* $\tau_{msg}^{\mathbb{J}}$ *as* $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{J}\})$*, then returns* $\tau_{msg}^{\mathbb{J}'} := ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{J}'\}) \in \mathbb{G}_2^n \times \mathbb{G}_2 \times \mathbb{G}_2^{|\mathbb{J}'|}$*.*
- $\mathtt{Down}(\tau_{msg}^{\mathbb{J}}, msg \in \mathcal{M}, \mathbb{J} \subseteq \mathbb{I}_1(msg), msg' \preceq_{\mathbb{J}} msg)$ *parses* $\tau_{msg}^{\mathbb{J}}$ *as* $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{J}\})$*, computes* $[u']_2 := \left[u - \sum_{i \in \mathbb{J} \bigcap \mathbb{I}_0(msg')} d_i\right]_2$*, then returns* $\tau_{msg'}^{\mathbb{J}'} := ([\boldsymbol{t}]_2, [u']_2, \{[d_i]_2 \mid i \in \mathbb{J}'\}) \in \mathbb{G}_2^n \times \mathbb{G}_2 \times \mathbb{G}_2^{|\mathbb{J}'|}$*, where* $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(msg')$*.*
- $\mathtt{Ver}(sk_{\mathrm{MAC}}, msg, \tau_{msg}^{\mathbb{J}})$ *returns* 1 *if the equation (1) holds, or* 0 *otherwise.*

Pseudo-Randomness. For the pseudo-randomness of DAMAC, we consider the experiments given below. Our definition is not a natural extension from the one for AMAC (or DlgAMAC) in [8], but weaker in some respects. Firstly, among the 3 variables in the challenge instance, i.e., $([h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$, pseudo-randomness of $[\boldsymbol{h}_0]_1$ is not considered. Secondly, tag-generation oracles cannot be used after the challenge instance is issued. We introduce two types of tag-generation oracles, one of which generates only a tag, and the other of which generates a tag plus variables used to re-randomize or downgrade the tag.

```
$\boldsymbol{Expt}^{\mathtt{PR\text{-}CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{A},0}(par)$:   // $\boldsymbol{Expt}^{\mathtt{PR\text{-}CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{A},1}$
    $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$, where $B \in \mathbb{Z}_p^{n \times n'}$, $\boldsymbol{x}_i \in \mathbb{Z}_p^n$ and $x \in \mathbb{Z}_p$.
    $(msg^* \in \{0,1\}^l, st) \leftarrow \mathcal{A}_0^{\mathfrak{Eval}_0, \mathfrak{Eval}_1}(par)$, where
```

```
−$\mathfrak{Eval}_0(msg \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(msg))$:
    $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(msg)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, msg)$.
    $S \leftarrow\!\!\!\!\sim \mathbb{Z}_p^{n' \times n'}$, $T := BS$, $\boldsymbol{w} := \sum_{i=0}^{l} f_i(msg)\boldsymbol{x}_i^\top T$. For $i \in \mathbb{J}$:   $\boldsymbol{e}_i := h_i(msg)\boldsymbol{x}_i^\top T$.
    $\mathbb{Q}_0 := \mathbb{Q}_0 \bigcup \{(msg, \mathbb{J})\}$. $\mathbf{Rtn}$ $([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2, \{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}\})$.
−$\mathfrak{Eval}_1(msg \in \{0,1\}^l)$:
    $([\boldsymbol{t}]_2, [u]_2, \perp) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, msg)$. $\tau := ([\boldsymbol{t}]_2, [u]_2)$. $\mathbb{Q}_1 := \mathbb{Q}_1 \bigcup \{(msg, \tau)\}$. $\mathbf{Rtn}$ $\tau$.

$\mathbf{Abt}$ if $\bigvee_{(msg,\mathbb{J}) \in \mathbb{Q}_0} msg^* \preceq_{\mathbb{J}} msg \bigvee_{msg \in \mathbb{Q}_1} msg^* = msg$.
$h \leftarrow\!\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{h}_0 := \sum_{i=0}^{l} f_i(msg^*)\boldsymbol{x}_i h$, $h_1 := xh$. $h_1 \leftarrow\!\!\!\!\sim \mathbb{Z}_p$
$\mathbf{Rtn}$ $b' \leftarrow \mathcal{A}_1(st, [h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$.
```

Definition 6. *A DAMAC Σ_{DAMAC} is PR-CMA1 if $\forall \lambda \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ s.t. $\boldsymbol{Adv}^{\text{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) := |\sum_{b=0}^{1}(-1)^b \Pr[1 \leftarrow \boldsymbol{Expt}^{\text{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{A},b}(par)]| < \epsilon$.*

3.2 Construction

Our DAMACs scheme Π_{DAMAC} is formally described below. The scheme is essentially the same as the AMACs scheme based on hash-proof system in [8] except for the downgrading-key associated with each tag, i.e., $\{[d_i]_2 \in \mathbb{G}_2 \mid i\}$, and the newly-introduced algorithms, i.e., `Weaken`, `Down`. Thus, the AMACs scheme is not only delegatable as shown in [8], but also downgradable.

```
$\mathtt{Gen}_{\mathrm{MAC}}(par)$:
    $\mathbf{Rtn}$ $sk_{\mathrm{MAC}} := (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x)$, where $B \leftarrow\!\!\!\!\sim \mathcal{D}_k$, $\boldsymbol{x}_0, \cdots, \boldsymbol{x}_l \leftarrow\!\!\!\!\sim \mathbb{Z}_p^k$ and $x \leftarrow\!\!\!\!\sim \mathbb{Z}_p$.
$\mathtt{Tag}\left(sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x), msg \in \{0,1\}^l\right)$:
    $\mathbf{Rtn}$ $\tau_{msg}^{\mathbb{I}_1(msg)} := ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(msg)\})$, where
        $\boldsymbol{s} \leftarrow\!\!\!\!\sim \mathbb{Z}_p^k$, $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^{k+1}$, $u := (\boldsymbol{x}_0^\top + \sum_{i \in \mathbb{I}_1(msg)} \boldsymbol{x}_i^\top)\boldsymbol{t} + x \in \mathbb{Z}_p$ and $d_i := \boldsymbol{x}_i^\top \boldsymbol{t} \in \mathbb{Z}_p$.
$\mathtt{Weaken}\left(\tau_{msg}^{\mathbb{J}} = \left([\boldsymbol{t}]_2, [u]_2, \left\{[d_i]_2 \mid i \in \mathbb{J}\right\}\right), msg \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(msg), \mathbb{J}' \subseteq \mathbb{I}_1(msg)\right)$:
    $\mathbf{Rtn}$ $\perp$ if $\mathbb{J}' \nsubseteq \mathbb{J}$. $\mathbf{Rtn}$ $\tau_{msg'}^{\mathbb{J}'} := ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{J}'\})$.
$\mathtt{Down}\left(\tau_{msg}^{\mathbb{J}} = \left([\boldsymbol{t}]_2, [u]_2, \left\{[d_i]_2 \mid i \in \mathbb{J}\right\}\right), msg \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(msg), msg' \in \{0,1\}^l\right)$:
    $\mathbf{Rtn}$ $\perp$ if $msg' \npreceq_{\mathbb{J}} msg$. $\mathbf{Rtn}$ $\tau_{msg'}^{\mathbb{J}'} := ([\boldsymbol{t}]_2, [u']_2, \{[d_i]_2 \mid i \in \mathbb{J}'\})$,
        where $[u']_2 := \left[u - \sum_{i \in \mathbb{J} \bigcap \mathbb{I}_0(msg')} d_i\right]_2$ and $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(msg')$.
$\mathtt{Ver}\left(sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x), msg \in \{0,1\}^l, \tau_{msg}^{\mathbb{J}} = \left([\boldsymbol{t}]_2, [u]_2, \left\{[d_i]_2 \mid i \in \mathbb{J}\right\}\right)\right)$:
    $\mathbf{Rtn}$ 1 if $[u]_2 = \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$. $\mathbf{Rtn}$ 0, otherwise.
```

3.3 Pseudo-Randomness

Theorem 1 guarantees that Π_{DAMAC} is pseudo-random under the MDDH assumption. A proof of the theorem is skipped to Subsect. B.1 because of the page restriction. We modify the proof of a theorem for pseudo-randomness of the delegatable AMACs sheme in [8].

Theorem 1. *The DAMAC scheme Π_{DAMAC} is PR-CMA1 if the $\mathcal{D}_k$-MDDH assumption w.r.t. $\mathcal{G}_{BG}$ and $\mathbb{G}_2$ holds. Formally, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$ s.t. $\boldsymbol{Adv}^{\text{PR-CMA1}}_{\Pi_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) \leq 2\{(k+1)q_e + q'_e\}(\frac{1}{p} + \frac{1}{p^{k+1}}) + \frac{4q_e}{p-1} + 2(q_e + q'_e)\boldsymbol{Adv}^{\mathcal{D}_k\text{-MDDH}}_{\mathcal{B},\mathcal{G}_{BG},\mathbb{G}_2}(\lambda)$.*

4 Downgradable Identity-Based Signatures (DIBS)

4.1 Our DIBS Model

Syntax. DIBS consist of following 6 polynomial time algorithms, where `Setup`, `KGen`, `Weaken`, `Down` and `Sig` are probabilistic and `Ver` is deterministic.

Setup `Setup`: Let $l \in \mathbb{N}$ (resp. $m \in \mathbb{N}$) denote length of an identity (resp. a message). It takes 1^λ, l and m as input, then outputs a master public-key mpk and a master secret-key msk. We write $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$.

Key-generation `KGen`: It takes msk, an identity $id \in \{0,1\}^l$, then outputs a secret-key $sk_{id}^{\mathbb{J}}$ for the identity and a set $\mathbb{J} := \mathbb{I}_1(id)$ indicating its downgradable bits. We write $sk_{id}^{\mathbb{J}} \leftarrow \texttt{KGen}(msk, id)$.

Weakening `Weaken`: It takes a secret-key $sk_{id}^{\mathbb{J}}$ for an identity $id \in \{0,1\}^l$ and a set $\mathbb{J} \subseteq \mathbb{I}_1(id)$ indicating its downgradable bits, and a set $\mathbb{J}' \subseteq \mathbb{J}$, then outputs a secret-key $sk_{id}^{\mathbb{J}'}$ for id and $\mathbb{J}'$. We write $sk_{id}^{\mathbb{J}'} \leftarrow \texttt{Weaken}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, \mathbb{J}')$.

Downgrade `Down`: It takes a secret-key $sk_{id}^{\mathbb{J}}$ for an identity $id \in \{0,1\}^l$ and a set $\mathbb{J} \subseteq \mathbb{I}_1(id)$, and a downgraded identity $id' \in \{0,1\}^l$ s.t. $id' \preceq_{\mathbb{J}} id$, then outputs a secret-key $sk_{id'}^{\mathbb{J}'}$ for id' and $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$. We write $sk_{id'}^{\mathbb{J}'} \leftarrow \texttt{Down}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, id')$.

Signing `Sig`: It takes a secret-key $sk_{id}^{\mathbb{J}}$ for an identity id and a set $\mathbb{J} \subseteq \mathbb{I}_1(id)$, and a message $msg \in \{0,1\}^m$, then outputs a signature σ. We write $\sigma \leftarrow \texttt{Sig}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, msg)$.

Verification `Ver`: It takes a signature σ, an identity $id \in \{0,1\}^l$ and a message $msg \in \{0,1\}^m$, then outputs a bit 1/0. We write $1/0 \leftarrow \texttt{Ver}(\sigma, id, msg)$.

We require every DIBS scheme to be correct. We say that a DIBS scheme Σ_{DIBS} is correct, if $\forall\lambda \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall m \in \mathbb{N}$, $\forall(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$, $\forall id_0 \in \{0,1\}^l$, $\forall sk_{id_0}^{\mathbb{I}_1(id_0)} \leftarrow \texttt{KGen}(msk, id_0)$, $\forall \mathbb{J}'_0 \subseteq \mathbb{I}_1(id_0)$, $\forall sk_{id_0}^{\mathbb{J}'_0} \leftarrow \texttt{Weaken}(sk_{id_0}^{\mathbb{I}_1(id_0)}, id_0, \mathbb{I}_1(id_0), \mathbb{J}_0)$, $\forall id_1 \in \{0,1\}^l$ s.t. $id_1 \preceq_{\mathbb{J}'_0} id_0$, $\forall sk_{id_1}^{\mathbb{J}_1} \leftarrow \texttt{Down}(sk_{id_0}^{\mathbb{J}'_0}, id_0, \mathbb{J}'_0, id_1)$, where $\mathbb{J}_1 := \mathbb{J}'_0 \setminus \mathbb{I}_0(id_1)$, $\cdots$, $\forall \mathbb{J}'_{n-1} \subseteq \mathbb{J}_{n-1}$, $\forall sk_{id_{n-1}}^{\mathbb{J}'_{n-1}} \leftarrow \texttt{Weaken}(sk_{id_{n-1}}^{\mathbb{J}_{n-1}}, id_{n-1}, \mathbb{J}_{n-1}, \mathbb{J}'_{n-1})$, $\forall id_n \in \{0,1\}^l$ s.t. $id_n \preceq_{\mathbb{J}'_{n-1}} id_{n-1}$, $\forall sk_{id_n}^{\mathbb{J}_n} \leftarrow \texttt{Down}(sk_{id_{n-1}}^{\mathbb{J}'_{n-1}}, id_{n-1}, \mathbb{J}'_{n-1}, id_n)$, where $\mathbb{J}_n := \mathbb{J}'_{n-1} \setminus \mathbb{I}_0(id_n)$, $\forall msg \in \{0,1\}^m$, $\forall \sigma \leftarrow \texttt{Sig}(sk_{id_n}^{\mathbb{J}_n}, id_n, \mathbb{J}_n, msg)$, $1 \leftarrow \texttt{Ver}(\sigma, id_n, msg)$.

Existential Unforgeability [25,27]. For a scheme Σ_{DIBS} and a probabilistic algorithm $\mathcal{A}$, we define the (weak) `EUF-CMA` by Def. 7 using the following experiment.

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\text{DIBS}},\mathcal{A}}(1^\lambda, l, m)$:
  $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$. $(\sigma^*, id^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
.............................................................................
  $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:
    $sk \leftarrow \texttt{KGen}(msk, id)$. $sk' \leftarrow \texttt{Weaken}(sk, id, \mathbb{I}_1(id), \mathbb{J})$. $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$. Rtn $sk'$.
  $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
    $sk \leftarrow \mathtt{KGen}(msk, id)$. $\sigma \leftarrow \mathtt{Sig}(sk, id, \mathbb{I}_1(id), msg)$. $\mathbb{Q}_s \coloneqq \mathbb{Q}_s \bigcup \{(id, msg, \sigma)\}$. Rtn $\sigma$.
..........................................................................
  Rtn 0 if $0 \leftarrow \mathtt{Ver}(\sigma^*, id^*, msg^*) \bigvee_{(id,\mathbb{J}) \in \mathbb{Q}_r} id^* \preceq_{\mathbb{J}} id$.
  Rtn 1 if $\bigwedge_{(id,msg,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*)$. Rtn 0.
```

Definition 7. *A scheme Σ_{DIBS} is* ***EUF-CMA****, if* $\forall \lambda \in \mathbb{N}$, $\forall l, m \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{Adv}^{\textit{EUF-CMA}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) \coloneqq \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{EUF-CMA}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A}}(1^\lambda, l, m)] < \epsilon$.

Signer Privacy. For a DIBS scheme Σ_{DIBS}, simulation algorithms $\Sigma'_{\mathrm{DIBS}} \coloneqq \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$, and a probabilistic algorithm $\mathcal{A}$, we consider the following two experiments. In the experiment with $b = 0$, every command with grey background is ignored.

```
$\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},b}(1^\lambda, l, m)$:   // $b \in \{0, 1\}$.
  $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $(mpk, msk') \leftarrow \mathtt{Setup}'(1^\lambda, l, m)$.
  Rtn $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where
..........................................................................
  $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
    $sk \leftarrow \mathtt{KGen}(msk, id)$. $sk \leftarrow \mathtt{KGen}'(msk', id)$. $\mathbb{Q} \coloneqq \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. Rtn $sk$.
  $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J}, \mathbb{J}' \subseteq [1, l])$:   Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
    $sk' \leftarrow \mathtt{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$. $sk' \leftarrow \mathtt{Weaken}'(sk, id, \mathbb{J}, \mathbb{J}')$.
    $\mathbb{Q} \coloneqq \mathbb{Q} \bigcup \{(sk', id, \mathbb{J}')\}$. Rtn $sk'$.
  $-\mathfrak{Down}(sk, id, id' \in \{0,1\}^l, \mathbb{J} \subseteq [1, l])$:   Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
    $sk' \leftarrow \mathtt{Down}(sk, id, \mathbb{J}, id')$. $sk' \leftarrow \mathtt{Down}'(sk, id, \mathbb{J}, id')$.
    $\mathbb{Q} \coloneqq \mathbb{Q} \bigcup \{(sk', id', \mathbb{J} \setminus \mathbb{I}_0(id'))\}$. Rtn $sk'$.
  $-\mathfrak{Sign}(sk, id, id' \in \{0,1\}^l, \mathbb{J} \subseteq [1, l], msg \in \{0,1\}^m)$:
    Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
    $sk' \leftarrow \mathtt{Down}(sk, id, \mathbb{J}, id')$. $\sigma \leftarrow \mathtt{Sig}(sk, id', \mathbb{J} \setminus \mathbb{I}_0(id'), msg)$.
    $\sigma \leftarrow \mathtt{Sig}'(msk', id', msg)$. Rtn $\sigma$.
```

Definition 8. *A DIBS scheme Σ_{DIBS} is statistically signer private, if for every $\lambda, l, m \in \mathbb{N}$, and every probabilistic algorithm $\mathcal{A}$, there exist polynomial time algorithms $\Sigma'_{\mathrm{DIBS}} \coloneqq \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$ and a negligible function $\epsilon \in \mathsf{NGL}_\lambda$ s.t.* $\boldsymbol{Adv}^{\textit{SP}}_{\Sigma_{\mathrm{DIBS}},\Sigma'_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) \coloneqq |\sum_{b=0}^{1} (-1)^b \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{SP}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},0}(1^\lambda, l, m)]|$ *is less than ϵ.*

4.2 Our DIBS Construction (DAMACtoDIBS)

DAMACtoDIBS (interchangeably $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$) with $\{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Ver}\}$ is described in Fig. 1.

The idea behind DAMACtoDIBS comes from anonymous hierarchical IBKEM based on delegatable AMAC (shortly DlgAMACtoAHIBKEM) in [8]. DlgAMACtoAHIBKEM uses a DlgAMAC with message-length l. mpk includes $(\{Z_i \mid i \in [0, l]\}, \boldsymbol{z})$, which are perfectly hiding commitments to $(\{\boldsymbol{x}_i \mid i \in [0, l]\}, x)$ in sk_{MAC}. Each secret-key for $id \in \{0,1\}^l$ includes $([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2)$, where $\boldsymbol{t} \in \mathbb{Z}_p^n$, $u \coloneqq \sum_{i=0}^{l} f_i(id) \boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $\boldsymbol{u} \coloneqq \sum_{i=0}^{l} f_i(id) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. Actually, they are Bellare-Goldwasser (BG) signature [5] on a message id, where $([\boldsymbol{t}]_2, [u]_2)$ are a DlgAMAC-tag on the message id and $[\boldsymbol{u}]_2$ is the NIZK-proof [19] which proves that the DlgAMAC-tag has been correctly generated w.r.t. the commitments $(\{Z_i \mid i \in [0, l]\}, \boldsymbol{z})$.

In DAMAC$\texttt{to}$DIBS, we adopt a DAMAC with message space $\{0,1\}^{l+m}$. To generate a secret-key for $id \in \{0,1\}^l$, we firstly generate a BG-signature on $id||1^m$, specifically a DAMAC-tag $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2\})$ on $id||1^m$ and the $[\boldsymbol{u}]_2$. We also generate auxiliary variables, namely $[T]_2, [\boldsymbol{w}]_2, [W]_2, \{[\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid | \, i \in \mathbb{I}_1(id||1^m)\}$, which are used to *re-randomize* or *downgrade* the BG-signature. To generate a signature on $msg \in \{0,1\}^m$ by using a secret-key sk for $id \in \{0,1\}^l$, we firstly re-randomize the BG-signature on $id||1^m$ included in sk, then downgrade it to a BG-signature on $id||msg$. Note that a signature on msg and id in DAMAC$\texttt{to}$DIBS is identical to a secret-key for $id||msg$ in DlgAMAC$\texttt{to}$AHIBKEM. To verify a signature on msg and id, we firstly *encapsulate* a (random) key, then attempt to *decapsulate* it by using the signature (being the secret-key for $id||msg$). If the decapsulation is successfully done, the signature is judged as a correct one.

Its correctness and security are guaranteed by Theorem 2, proven in B.2.

Theorem 2. *$\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ is correct. $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ is* ***EUF-CMA*** *if the $\mathcal{D}_k$-MDDH assumption on $\mathbb{G}_1$ holds and the underlying Σ_{DAMAC} is* ***PR-CMA1****. $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ is statistically signer-private.*

4.3 Generic Transformations from DIBS into the Major IBS

We propose two types of generic transformation from a DIBS into one of the 6 types of IBS-primitives, namely (W)IBS, (W)HIBS and (W)WkIBS. The first-type transformations work for all of the IBS-primitives. The second-typpe ones work for only the non-wildcarded IBS-primitives.

The First-Type Transformations. The transformations work for all of the IBS-primitives. Their technique is basically the same as the one to transform any DIBE into the major IBE-primitives in [7]. They do not use $\texttt{Weaken}$ of the DIBS scheme. We only present the details of the transformation into WWkIBS, denoted by DIBS$\texttt{to}$WWkIBS1. The transformations into the weaker IBS-primitives, i.e., (W)IBS, (W)HIBS and WkIBS, are obtained from it.

DIBS$\texttt{to}$WWkIBS1 uses a DIBS scheme with identity-length $2ln$. We transform each (wildcarded) identity $id \in \mathcal{I}_{wwk}$ into an identity $did \in \{0,1\}^{2ln}$ based on two functions ϕ and ϕ_{wwk}. ϕ takes $id \in \{0,1,*\}^l$, then outputs $||_{i=1}^{l} did_i \in \{0,1\}^{2l}$, where did_i is set to 01 (if $id[i] = 0$), 10 (if $id[i] = 1$), or 00 (if $id[i] = *$). ϕ_{wwk} takes $id \in \mathcal{I}_{wwk}$, then outputs $||_{i=1}^{n} did_i \in \{0,1\}^{2ln}$, where did_i is set to 1^{2l} (if $id_i = \#$), or $\phi(id_i)$ (if $id_i \in \{0,1,*\}^l$). A secret-key for an $id \in \mathcal{I}_{wk}$ is a (randomly-generated) DIBS secret-key for $\phi_{wwk}(id) \in \{0,1\}^{2ln}$. Any secret-key for an $id \in \mathcal{I}_{wk}$ can generate a secret-key for any of its descendant $id' \in \mathcal{I}_{wk}$ s.t. $1 \leftarrow R_{wk}(id, id')$ based on $\texttt{Down}'$ of the DIBS scheme since $did' \preceq_{\mathbb{I}_1(did)} did$ holds, where $did \coloneqq \phi_{wwk}(id)$ and $did' \coloneqq \phi_{wwk}(id')$. It can also generate a signature on

```
$\texttt{Setup}(1^\lambda, l, m)$:
  $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} \leftarrow \texttt{Gen}_{\mathrm{MAC}}(1^\lambda, l+m)$.
  Parse $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x)$.
    // $B \in \mathbb{Z}_p^{n \times n'}$, $\boldsymbol{x}_i \in \mathbb{Z}_p^n$, $x \in \mathbb{Z}_p$.
  For $i \in [0, l+m]$:
    $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $Z_i := (Y_i \mid \boldsymbol{x}_i)\, A \in \mathbb{Z}_p^{n \times k}$.
  $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A \in \mathbb{Z}_p^{1 \times k}$.
  $mpk := \left([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1\right)$.
  $msk := \left(sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y}\right)$.
  Rtn $(mpk, msk)$.

$\texttt{Down}(sk_{id}^{\mathbb{J}}, id, \mathbb{J} \subseteq \mathbb{I}_1(id), id')$:
  Rtn $\perp$ if $id' \not\preceq_{\mathbb{J}} id$.
  $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{KRnd}(sk_{id}^{\mathbb{J}}, id, \mathbb{J})$.
  Parse $(sk_{id}^{\mathbb{J}})'$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
  $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$. $\mathbb{I}^* := \mathbb{I}_1(id) \bigcap \mathbb{I}_0(id')$.
  $[u']_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$.
  $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
  $[\boldsymbol{w}']_2 := \left[\boldsymbol{w} - \sum_{i \in \mathbb{I}^*} \boldsymbol{e}_i\right]_2$.
  $[W']_2 := \left[W - \sum_{i \in \mathbb{I}^*} E_i\right]_2$.
  Rtn $sk_{id'}^{\mathbb{J}'} := \big([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2, [T]_2, [\boldsymbol{w}']_2,$
  $[W']_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}' \bigcup \mathbb{K}\big\}\big)$.

$\texttt{Sig}(sk_{id}^{\mathbb{J}}, id, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m)$:
  $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{KRnd}(sk_{id}^{\mathbb{J}}, id, \mathbb{J})$.
  Parse $(sk_{id}^{\mathbb{J}})'$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
  $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\mathbb{I}^* := \mathbb{I}_0(1^l || msg)$. $[u']_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$.
  $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
  Rtn $\sigma := \left([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2\right)$.

$\texttt{Ver}(\sigma, id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
  Parse $\sigma$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2\right)$. $\boldsymbol{r} \leftsquigarrow \mathbb{Z}_p^k$.
  $[\boldsymbol{v}_0]_1 := [A\boldsymbol{r}]_1 \in \mathbb{G}^{k+1}$. $[v]_1 := [\boldsymbol{z}\boldsymbol{r}]_1 \in \mathbb{G}$.
  $[\boldsymbol{v}_1]_1 := \left[\sum_{i=0}^{l+m} f_i(id || msg) Z_i \boldsymbol{r}\right]_1 \in \mathbb{G}^n$.
  Rtn 1 if $e\left([\boldsymbol{v}_0]_1, \begin{bmatrix} \boldsymbol{u} \\ u \end{bmatrix}_2\right) \cdot e\left([\boldsymbol{v}_1]_1, [\boldsymbol{t}]_2\right)^{-1}$
  $= e\left([v]_1, [1]_2\right)$.   Rtn 0 otherwise.

$\texttt{KGen}(msk, id \in \{0,1\}^l)$:
  $\tau \leftarrow \texttt{Tag}(sk_{\mathrm{MAC}}, id || 1^m)$.
  Parse $\tau = ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id || 1^m)\})$.
    // $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^n$.
    // $d_i := h_i(id || 1^m) \boldsymbol{x}_i^\top \boldsymbol{t}$.
    // $u := \sum_{i=0}^{l+m} f_i(id || 1^m) \boldsymbol{x}_i^\top \boldsymbol{t} + x \in \mathbb{Z}_p$.
  $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id || 1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top \in \mathbb{Z}_p^k$.
  $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $T := BS \in \mathbb{Z}_p^{n \times n'}$.
  $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id || 1^m) \boldsymbol{x}_i^\top T \in \mathbb{Z}_p^{1 \times n'}$.
  $W := \sum_{i=0}^{l+m} f_i(id || 1^m) Y_i^\top T \in \mathbb{Z}_p^{k \times n'}$.
  For $i \in \mathbb{I}_1(id || 1^m)$: $\boldsymbol{d}_i := h_i(id || 1^m) Y_i^\top \boldsymbol{t}$,
    $\boldsymbol{e}_i := h_i(id || 1^m) \boldsymbol{x}_i^\top T$, $E_i := h_i(id || 1^m) Y_i^\top T$.
  Rtn $sk_{id}^{\mathbb{I}_1(id)} :=$
  $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2,$
  $\big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id) \bigcup \mathbb{K}\big\}\big)$.

$\texttt{Weaken}(sk_{id}^{\mathbb{J}}, id, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id))$:
  Rtn $\perp$ if $\mathbb{J}' \not\subseteq \mathbb{J}$. $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{KRnd}(sk_{id}^{\mathbb{J}}, id, \mathbb{J})$.
  Parse $(sk_{id}^{\mathbb{J}})'$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
  $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  Rtn $sk_{id}^{\mathbb{J}'} := \big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
  $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}' \bigcup \mathbb{K}\big\}\big)$.

$\texttt{KRnd}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:
  Parse $sk_{id}^{\mathbb{J}}$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
  $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$.
  $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$,
  $[W']_2 := [WS']_2$, $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$,
  $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
  For $i \in \mathbb{J} \bigcup \mathbb{K}$:
    $[\boldsymbol{e}_i']_2 := [\boldsymbol{e}_i S']_2$, $[E_i']_2 := [E_i S']_2$,
    $[d_i']_2 := [d_i + \boldsymbol{e}_i' \boldsymbol{s}']_2$, $[\boldsymbol{d}_i']_2 := [\boldsymbol{d}_i + E_i' \boldsymbol{s}']_2$.
  Rtn $(sk_{id}^{\mathbb{J}})' :=$
  $\big([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2$
  $\big\{[d_i']_2, [\boldsymbol{d}_i']_2, [\boldsymbol{e}_i']_2, [E_i']_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
```

Fig. 1. Our DIBS scheme DAMAC`to`DIBS (interchangeably $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}$) with {`Setup`, `KGen`, `Weaken`, `Down`, `Sig`, `Ver`} (and a sub-routine key-randomizing algorithm `KRnd`) based on a DAMAC scheme $\Sigma_{\mathrm{DAMAC}} = \{\texttt{Gen}_{\mathrm{MAC}}, \texttt{Tag}, \texttt{Weaken}, \texttt{Down}, \texttt{Ver}\}$. Note that $\mathbb{K}$ denotes a set $[l+1, l+m]$ of successive integers.

any wildcarded $wid \in \mathcal{I}_{wwk}$ s.t. $1 \leftarrow \mathcal{R}_{wwk}(id, wid)$ by firstly generating a *secret-key* for wid based on $\texttt{Down}'$ (note: this correctly works since $dwid \preceq_{\mathbb{I}_1(did)} did$, where $did := \phi_{wwk}(id)$ and $dwid := \phi_{wwk}(wid)$), then secondly generating a signature based on $\texttt{Sig}'$. The transformation is formally described below.

```
WWkIBS.Setup$(1^\lambda, l, m, n)$:
  $(mpk, msk) \leftarrow \texttt{Setup}'(1^\lambda, 2ln, m)$.
  $sk_{\#^n} := sk_{1^{2ln}}^{\mathbb{I}_1(1^{2ln})} \leftarrow \texttt{KGen}'(msk, 1^{2ln})$. Rtn $(mpk, sk_{\#^n})$.
WWkIBS.KGen$(sk_{id}, id \in \mathcal{I}_{wk}, id' \in \mathcal{I}_{wk})$:
  $did \leftarrow \phi_{wwk}(id)$. $did' \leftarrow \phi_{wwk}(id')$. Let $sk_{did}^{\mathbb{I}_1(did)}$ denote $sk_{id}$.
  Rtn $sk_{did'}^{\mathbb{I}_1(did')} \leftarrow \texttt{Down}'(sk_{did}^{\mathbb{I}_1(did)}, did, \mathbb{I}_1(did), did')$.
WWkIBS.Sig$(sk_{id}, id \in \mathcal{I}_{wk}, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
  $did \leftarrow \phi_{wwk}(id)$. $dwid \leftarrow \phi_{wwk}(wid)$. Let $sk_{did}^{\mathbb{I}_1(did)}$ denote $sk_{id}$.
  $sk_{dwid}^{\mathbb{I}_1(dwid)} \leftarrow \texttt{Down}'(sk_{did}^{\mathbb{I}_1(did)}, did, \mathbb{I}_1(did), dwid)$.
  Rtn $\sigma \leftarrow \texttt{Sig}'(sk_{dwid}^{\mathbb{I}_1(dwid)}, dwid, \mathbb{I}_1(dwid), msg)$.
WWkIBS.Ver$(\sigma, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
  $dwid \leftarrow \phi_{wwk}(wid)$. Rtn $1$ / $0 \leftarrow \texttt{Ver}'(\sigma, dwid, msg)$.
```

Its security is guaranteed by Theorem 3. It is proven in Subsect. B.3.

Theorem 3. DIBS*to*WWkIBS1 *is* EUF-CMA *if the underlying DIBS scheme* Σ_{DIBS} *is* EUF-CMA*.* DIBS*to*WWkIBS1 *is signer-private if* Σ_{DIBS} *is signer-private.*

The Second-Type Transformations. The transformations work for only the non-wildcarded IBS-primitives. They effectively use Weaken of the DIBS. We explain the details of the one for WkIBS, denoted by DIBStoWkIBS2. The ones for IBS and HIBS are obtained from it.

Assume that DIBStoWkIBS2 has identity space $(\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n$. It uses a DIBS scheme with identity-length ln. A secret-key for an $id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n$ is a DIBS secret-key for $did \in \{0,1\}^{ln}$ partially-losing its downgradability. We parse did as $||_{i=1}^n did_i$ (where $did_i \in \{0,1\}^l$). Each id_i is transformed into did_i. Precisely, if $id_i = \#$, then it is transformed into $did_i := 1^l$ equipped with the full downgradability. Else if $id_i \in \{0,1\}^l \setminus \{1^l\}$, then it is transformed into $did_i = id_i$ with no downgradability. The details can be seen in Sect. C.

Instantiation and Efficiency Analysis. We instantiate the transformations by our DIBS scheme. In this paper, we mainly focus on the instantiations of wildcarded IBS primitives, i.e., the ones of DIBStoWIBS1, DIBStoWHIBS1 and DIBStoWWkIBS1, since their contribution is clear. Their features are summarized as in Table 1. WIBS$_{\text{SAH}}$ [27] is attractive because of the constant size of secret-keys and perfect privacy. The instantiation of DIBStoWIBS1 is attractive because of size of signatures which is constant (in other words, independent of l) and security loss which is asymptotically-smaller than WIBS$_{\text{SAH}}$. To the best of our knowledge, the instantiations of DIBStoWHIBS1 and DIBStoWWkIBS are the first WHIBS and WWkIBS schemes.

There is a transformation from any n-level HIBE into an $(n-1)$-level HIBS [21,18]. We believe that, a transformation from n-level WkIBE into $(n-1)$-level WkIBS, based on the same technique, correctly works. For instance, the

Schemes	$\lvert mpk \rvert$	$\lvert sk \rvert$	$\lvert \sigma \rvert$	Sec. Loss	Assum.	SP
WIBS$_{\mathrm{SAH}}$ [27]	$\mathcal{O}(l)\lvert g_2 \rvert$	$\mathcal{O}(1)(\lvert g_1 \rvert + \lvert g_2 \rvert)$	$\mathcal{O}(l)(\lvert g_1 \rvert + \lvert g_2 \rvert)$	$\mathcal{O}((q_r + q_s)^2)$	SXDH	P
DIBStoWIBS1	$\mathcal{O}((l+m)k^2)\lvert g_1 \rvert$	$\mathcal{O}((l+m)k^2)\lvert g_2 \rvert$	$(2k+2)\lvert g_2 \rvert$	$\mathcal{O}(q_r + q_s)$	k-Lin	S
DIBStoWHIBS1	$\mathcal{O}((ln+m)k^2)\lvert g_1 \rvert$	$\mathcal{O}((ln+m)k^2)\lvert g_2 \rvert$	$(2k+2)\lvert g_2 \rvert$	$\mathcal{O}(q_r + q_s)$	k-Lin	S
DIBStoWWkIBS1	$\mathcal{O}((ln+m)k^2)\lvert g_1 \rvert$	$\mathcal{O}((ln+m)k^2)\lvert g_2 \rvert$	$(2k+2)\lvert g_2 \rvert$	$\mathcal{O}(q_r + q_s)$	k-Lin	S

Table 1. Comparison among existing *wildcarded* IBS schemes which are adaptively and weakly (existentially) unforgeable under standard (static) assumptions. The message space is $\{0,1\}^m$. For the WIBS, WHIBS and WWkIBS schemes, the ID space is $\{0,1\}^l$, $(\{0,1\}^l)^{\leq n}$ and $(\{0,1\}^l \bigcup \{\#\})^n$, respectively. For schemes based on asymmetric bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, $\lvert g_1 \rvert$ (resp. $\lvert g_2 \rvert$, $\lvert g_T \rvert$) denotes bit length of an element in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$, $\mathbb{G}_T$). q_r (resp. q_s) denotes total number that $\mathcal{A}$ issues a query to $\mathfrak{Reveal}$ (resp. $\mathfrak{Sign}$). For the column for signer-privacy (SP), S and P denote statistical and perfect security, respectively. WIBS$_{\mathrm{SAH}}$ is the WIBS scheme obtained as an instantiation of the ABS scheme in [27].

instantiation of DIBStoWkIBS2, the one of DIBStoWkIBS1 and the WkIBS scheme transformed from the WkIBE scheme proposed in [7] achieve asymptotically equivalent efficiency in data size and security loss. However, their actual efficiency can greatly differ. Especially, the instantiation of DIBStoWkIBS2 has a master public-key whose size is almost two thirds of either of the others. The details are explained in Subsect. C.

5 Trapdoor Sanitizable Signatures (TSS)

In the ordinary digital signature, no modification of a signed-message is allowed. Sanitizable signatures (SS) [3] allow an entity called *sanitizer* to partially modify the message while retaining validity of the signature. In SS [3,9,13,12], the signer chooses a public-key of a sanitizer. The sanitizer modifies the message using her secret-key. In trapdoor SS (TSS) [14], each signed-message is associated with a *trapdoor*. Any entity can correctly modify the message using the trapdoor.

5.1 Our TSS Model

We define syntax and security of TSS. As we explain in Subsect. 5.2, our model is different from and stronger than the original in [14,29].

Syntax. TSS consist of following 4 polynomial time algorithms, where `KGen`, `Sig` and `Sanit` are probabilistic and `Ver` are deterministic.

Key-generation `KGen`: $l \in \mathbb{N}$ denotes length of a message. It takes 1^λ and l, then outputs a key-pair (pk, sk). We write $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$.

Signing `Sig`: It takes sk, a message $msg \in \{0,1\}^l$ and a set $\mathbb{T} \subseteq [1,l]$ of its modifiable parts, then outputs a signature σ and a trapdoor td. We write $(\sigma, td) \leftarrow \mathtt{Sig}(sk, msg, \mathbb{T})$.

Sanitizing `Sanit`: It takes pk, msg, $\mathbb{T}$, σ, td, a message $\overline{msg}$ and a set $\overline{\mathbb{T}} \subseteq \mathbb{T}$, then outputs a signature $\overline{\sigma}$ and a trapdoor $\overline{td}$. We write $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$.

Verification `Ver`: It takes pk, σ and msg, then returns 1 or 0. We write $1/0 \leftarrow \mathtt{Ver}(pk, msg, \sigma)$.

We require every TSS scheme to be correct. We say that a TSS scheme Σ_{TSS} is correct, if $\forall \lambda \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall (pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$, $\forall msg_0 \in \{0,1\}^l$, $\forall \mathbb{T}_0 \subseteq [1, l]$, $\forall (\sigma_0, td_0) \leftarrow \mathtt{Sig}(pk, sk, msg_0, \mathbb{T}_0)$, $\forall msg_1 \in \{0,1\}^l$ s.t. $\bigwedge_{i \in [1,l] \text{ s.t. } msg_1[i] \neq msg_0[i]} i \in \mathbb{T}_0$, $\forall \mathbb{T}_1 \subseteq \mathbb{T}_0$, $\forall (\sigma_1, td_1) \leftarrow \mathtt{Sanit}(pk, msg_0, \mathbb{T}_0, \sigma_0, td_0, msg_1, \mathbb{T}_1)$, $\cdots$, $\forall msg_n \in \{0,1\}^l$ s.t. $\bigwedge_{i \in [1,l] \text{ s.t. } msg_n[i] \neq msg_{n-1}[i]} i \in \mathbb{T}_{n-1}$, $\forall \mathbb{T}_n \subseteq \mathbb{T}_{n-1}$, $\forall (\sigma_n, td_n) \leftarrow \mathtt{Sanit}(pk, msg_{n-1}, \mathbb{T}_{n-1}, \sigma_{n-1}, td_{n-1}, msg_n, \mathbb{T}_n)$, $\bigwedge_{i=0}^{n} 1 \leftarrow \mathtt{Ver}(pk, \sigma_i, msg_i)$.

Security. We mainly consider the following 5 security requirements. *Unforgeability* (`UNF`) guarantees that any entity except for the signer, even if he can arbitrarily acquire any signature with or without its trapdoor, cannot forge an original correct signature. *Transparency* (`TRN`) guarantees that any entity, given a pair of signature and trapdoor, cannot correctly guess whether the signature has been sanitized. *(Weak) privacy* (`wPRV`) guarantees that any entity, given a pair of sanitized signature and trapdoor, cannot get any information about the original message. *Unlinkability* (`UNL`) guarantees that any entity, given a pair of sanitized signature and trapdoor, cannot get any information about the original signature. *Invisibility* (`INV`) guarantees that any entity, given a signature without its trapdoor, cannot get any information about its modifiable parts $\mathbb{T}$.

We introduce the sixth security notion, *strong privacy* (`sPRV`). It informally means that any sanitized signature and its trapdoor distribute identically to a fresh pair of signature and trapdoor generated by `Sig`.

They are defined by Def. 9, 10 using the experiments for the first 5 notions depicted in Fig. 2 and the following experiment for `sPRV`. Theorem 4 (proven in Subsect. B.4) says that 5 implications hold between the 6 notions.

```
$\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\text{TSS}},\mathcal{A},b}(1^\lambda, l)$:   // $b \in \{0, 1\}$.
  $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign}, \mathfrak{San}/\mathfrak{Sig}}(pk, sk)$, where
  ..........................................................................
  $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1, l])$:
    $(\sigma, td) \leftarrow \mathtt{Sig}(pk, sk, msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}\ (\sigma, td)$.
  $-\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1, l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1, l])$:
    $\mathbf{Rtn} \perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee (msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigvee_{i \in [1,l] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
    $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(pk, sk, \overline{msg}, \overline{\mathbb{T}})$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
```

Definition 9. *A TSS scheme Σ_{TSS} is EUF-CMA, if $\forall \lambda \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ s.t. $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\text{TSS}},\mathcal{A},l}(\lambda) := \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\text{TSS}},\mathcal{A}}(1^\lambda, l)] < \epsilon$.*

Definition 10. *Let $Z \in \{\mathtt{TRN}, \mathtt{wPRV}, \mathtt{UNL}, \mathtt{INV}, \mathtt{sPRV}\}$. A scheme Σ_{TSS} is statistically (resp. perfectly) Z, if $\forall \lambda, l \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PA}$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ s.t. $\mathtt{Adv}^{Z}_{\Sigma_{\text{TSS}},\mathcal{A},l}(\lambda) := |\sum_{b=0}^{1} (-1)^b \Pr[1 \leftarrow \boldsymbol{Expt}^{Z}_{\Sigma_{\text{TSS}},\mathcal{A},b}(1^\lambda, l)]| < \epsilon$ (resp. $\mathtt{Adv}^{Z}_{\Sigma_{\text{TSS}},\mathcal{A},l}(\lambda) = 0$).*[6]

[6] If we say *a TSS scheme is Z secure*, that means *the scheme is statistically Z secure.*

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}}(1^\lambda, l)$:
    $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, l)$. $(\sigma^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanitizeTd}}(pk)$, where
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
        $(\sigma, td) \leftarrow \texttt{Sig}(pk, sk, msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}\ \sigma$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigvee \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ \overline{\sigma}$.
    $-\mathfrak{SanitizeTd}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigvee \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q}_{td} := \mathbb{Q}_{td} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma})\}$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
    $\mathbf{Rtn}\ 0$ if $0 \leftarrow \texttt{Ver}(\sigma^*, msg^*) \bigvee_{(msg, \mathbb{T}, \sigma) \in \mathbb{Q}_{td}} \bigwedge_{i \in [1,l] \text{ s.t. } msg^*[i] \neq msg[i]} i \in \mathbb{T}$.
    $\mathbf{Rtn}\ 1$ if $\bigwedge_{(msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}} msg \neq msg^*$. $\mathbf{Rtn}\ 0$.
```

```
$\boldsymbol{Expt}^{\texttt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},b}(1^\lambda, l)$:   // $b \in \{0, 1\}$.
    $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{San}/\mathfrak{Sig}}(pk, sk)$, where
    $-\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
        $(\sigma, td) \leftarrow \texttt{Sig}(pk, sk, msg, \mathbb{T})$. $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sig}(pk, sk, \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
```

```
$\boldsymbol{Expt}^{\texttt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},b}(1^\lambda, l)$:   // $b \in \{0, 1\}$.
    $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigSanLR}}(pk, sk)$, where
    $-\mathfrak{SigSanLR}(msg_0, msg_1 \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{\beta \in \{0,1\}} \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
        $(\sigma, td) \leftarrow \texttt{Sig}(pk, sk, msg_b, \mathbb{T})$. $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg_b, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
```

```
$\boldsymbol{Expt}^{\texttt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},b}(1^\lambda, l)$:   // $b \in \{0, 1\}$.
    $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}(pk, sk)$, where
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
        $(\sigma, td) \leftarrow \texttt{Sig}(pk, sk, msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}\ (\sigma, td)$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
        $\mathbf{Rtn}\ \bot$ if $(msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
    $-\mathfrak{SanLR}(msg_0 \in \{0,1\}^l, \mathbb{T}_0 \subseteq [1,l], \sigma_0, td_0, msg_1 \in \{0,1\}^l, \mathbb{T}_1 \subseteq [1,l], \sigma_1, td_1,$
                                                        $\overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $\bigvee_{\beta \in \{0,1\}} \left[\overline{\mathbb{T}} \not\subseteq \mathbb{T}_\beta \bigvee (msg_\beta, \mathbb{T}_\beta, \sigma_\beta, td_\beta) \notin \mathbb{Q} \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}_\beta\right]$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg_b, \mathbb{T}_b, \sigma_b, td_b, \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
```

```
$\boldsymbol{Expt}^{\texttt{INV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},b}(1^\lambda, l)$:   // $b \in \{0, 1\}$.
    $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigLR},\mathfrak{SanLR}}(pk, sk)$, where
    $-\mathfrak{SigLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l])$:
        $(\sigma, td) \leftarrow \texttt{Sig}(pk, sk, msg, \mathbb{T}_b)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td)\}$. $\mathbf{Rtn}\ \sigma$.
    $-\mathfrak{SanLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1 \subseteq [1,l])$:
        $\mathbf{Rtn}\ \bot$ if $\bigvee_{\beta \in \{0,1\}} \left[\overline{\mathbb{T}}_\beta \not\subseteq \mathbb{T}_\beta \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}_\beta\right] \bigvee (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, \cdot) \notin \mathbb{Q}$.
        $\exists (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(pk, msg, \mathbb{T}_b, \sigma, td, \overline{msg}, \overline{\mathbb{T}}_b)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ \overline{\sigma}$.
```

Fig. 2. Experiments for (weak) existential unforgeability, transparency, weak privacy, unlinkability and invisibility w.r.t. a TSS scheme $\Sigma_{\mathrm{TSS}} = \{\texttt{KGen}, \texttt{Sig}, \texttt{Sanit}, \texttt{Ver}\}$.

Theorem 4. *For any TSS scheme, (1)* `TRN` *implies* `wPRV`*, (2)* `UNL` *implies* `wPRV`*, (3)* `sPRV` *implies* `TRN`*, (4)* `sPRV` *implies* `UNL`*, and (5)* `TRN` $\bigwedge$ `UNL` *implies* `sPRV`*. The implications holds even if the security notions are perfect ones.*

5.2 Difference from the Existing TSS Models [14,29]

They differ in how to generate a trapdoor associated with a signature. In the existing models, they are simultaneously generated by `Sig`. In the original model, the trapdoor is generated from the signature by a trapdoor-generation algorithm using the secret-key. Practical significance of the algorithm is limited. In a situation where someone demands the trapdoor associated with a previously-generated signature, the signer would (ignore the signature and) newly generate a signature and its trapdoor on the same message and $\mathbb{T}$.

Furthermore, our model differs in the following 3 respects. Firstly, `Sanit` is *fully-probabilistic*. The property is necessary to achieve either of `sPRV` and `UNL`. Note that the `Sanit` of the scheme in [14] is fully-deterministic, and the one of the scheme in [29] is semi-probabilistic. Actually, their schemes can achieve neither `UNL` nor `sPRV`. Secondly, both of a signature and its trapdoor can be rerandomized. This is done by executing `Sanit` with $(\overline{msg}, \overline{\mathbb{T}}) = (msg, \mathbb{T})$. Thirdly, the modifiable parts for a signature can be *downsizable*. This is done by running `Sanit` with $\overline{msg} = msg$ and $\overline{\mathbb{T}} \subset \mathbb{T}$. The original model assumes that the trapdoor and modifiable parts are permanently fixed.

5.3 Generic TSS Construction from DIBS

In this subsection, we propose a generic TSS construction from DIBS. We require the underlying DIBS scheme to be *key-invariant* (`KI`). Informally, the property means that each secret-key generated by `Weaken` or `Down` distributes identically to fresh one generated by `KGen` and `Weaken`. Formally, we define it by Def. 11 using the following experiment.

```
$\boldsymbol{Expt}^{\texttt{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},b}(1^\lambda, l, m)$:   // $b \in \{0, 1\}$.
  $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$. Rtn $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down}}(mpk, msk)$, where
..................................................................................
  $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
    $sk \leftarrow \texttt{KGen}(msk, id \in \{0,1\}^l)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. Rtn $sk$.
  $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], \mathbb{J}' \subseteq [1,l])$:
    Rtn $\bot$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
    $sk' \leftarrow \texttt{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$. $sk \leftarrow \texttt{KGen}(msk, id)$. $sk' \leftarrow \texttt{Weaken}(sk, id, \mathbb{I}_1(id), \mathbb{J}')$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id, \mathbb{J})\}$. Rtn $sk'$.
  $-\mathfrak{Down}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l)$:
    Rtn $\bot$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. $sk' \leftarrow \texttt{Down}(sk, id, \mathbb{J}, id')$.
    $sk \leftarrow \texttt{KGen}(msk, id')$. $sk' \leftarrow \texttt{Weaken}(sk, id', \mathbb{I}_1(id'), \mathbb{J} \setminus \mathbb{I}_0(id'))$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id', \mathbb{J} \setminus \mathbb{I}_0(id'))\}$. Rtn $sk'$.
```

Definition 11. *A DIBS scheme Σ_{DIBS} is statistically (resp. perfectly)* `KI`*, if* $\forall \lambda, l, m \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PA}$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{Adv}^{\mathit{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) := |\sum_{b=0}^{1} (-1)^b \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathit{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},b}(1^\lambda, l, m)]| < \epsilon$ *(resp.* $\boldsymbol{Adv}^{\mathit{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) = 0$*).*

Theorem 5 is proven in Subsect. B.5.

Theorem 5. *Our DAMAC-based DIBS $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ (in Fig. 1) is statistically* `KI`.

The TSS construction DIBS**to**TSS (interchangeably $\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$) with message-length l uses a DIBS scheme with identity/message-length l. In general, a TSS signature and its trapdoor are DIBS secret-keys. Specifically, a TSS signature w.r.t. $(msg \in \{0,1\}^l, \mathbb{T} \subseteq \{0,1\}^l)$[7] is a DIBS secret-key w.r.t. $(msg, \emptyset)$[8], and its trapdoor is one w.r.t. $(\Phi_{\mathbb{T}}(msg), \mathbb{T})$. The function $\Phi_{\mathbb{T}}$ takes a message $msg \in \{0,1\}^l$ then outputs $msg' \in \{0,1\}^l$, where msg' is identical to msg except that for every $i \in [1,l]$ s.t. $i \in \mathbb{T} \wedge msg[i] = 0$, $msg'[i]$ becomes 1. In verification, we verify whether the TSS signature is a correct the DIBS secret-key for the identity msg. Specifically, we generate a signature on a random message for the identity msg using the secret-key, then verifies it. In either of signing and sanitizing, we firstly generate a TSS trapdoor (= a DIBS secret-key w.r.t. $(\Phi_{\mathbb{T}}(msg), \mathbb{T})$), then generate a TSS signature (= one w.r.t. $(msg, \emptyset)$) using the trapdoor. In signing, we generate a TSS trapdoor (= one w.r.t. $(\Phi_{\mathbb{T}}(msg), \mathbb{T})$) from the DIBS master secret-key. In sanitizing, we generate a *modified* TSS trapdoor (= one w.r.t. $(\Phi_{\overline{\mathbb{T}}}(\overline{msg}), \overline{\mathbb{T}})$) from the *original* TSS trapdoor. The TSS construction based on $\Sigma_{\mathrm{DIBS}} = \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}', \mathtt{Ver}'\}$ is described as follows.

```
$\mathtt{KGen}(1^\lambda, l)$:   $(pk, sk) := (mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$.
$\mathtt{Sig}(pk, sk, msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
  $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$. $sk^{\mathbb{I}_1(msg')}_{msg'} \leftarrow \mathtt{KGen}'(msk, msg')$.
  $td := sk^{\mathbb{T}}_{msg'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(msg')}_{msg'}, msg', \mathbb{I}_1(msg'), \mathbb{T})$.
  $sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, msg)$.
  $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset)$. $\mathbf{Rtn}$ $(\sigma, td)$.
$\mathtt{Sanit}(pk, msg, \mathbb{T}, \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
  $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
  $sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, \overline{msg}')$.
  $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}'}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}})$.
  $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{Down}'(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
  $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$. $\mathbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
$\mathtt{Ver}(pk, \sigma, msg \in \{0,1\}^l)$:
  $\sigma$ as $sk^{\emptyset}_{msg}$. $\hat{msg} \leftsquigarrow \{0,1\}^l$. $\hat{\sigma} \leftarrow \mathtt{Sig}'(sk^{\emptyset}_{msg}, msg, \emptyset, \hat{msg})$.
  $\mathbf{Rtn}$ $1/0 \leftarrow \mathtt{Ver}'(\hat{\sigma}, msg, \hat{msg})$.
```

`KI` of Σ_{DIBS} implies `sPRV` of DIBS**to**TSS, which implies its `TRN`, `wPRV` and `UNL` because of Theorem 4. A sanitized (or non-sanitized) signature $\overline{\sigma}$ w.r.t. $(\overline{msg}, \overline{\mathbb{T}})$ and its trapdoor are a DIBS secret-key w.r.t. $(\overline{msg}, \emptyset)$ and one w.r.t. $(\Phi_{\overline{\mathbb{T}}}(\overline{msg}), \overline{\mathbb{T}})$, respectively. Either one is generated from a DIBS secret-key using the `Weaken`

[7] For $msg \in \{0,1\}^l$ and $\mathbb{T} \subseteq [1,l]$, by a TSS signature w.r.t. $(msg, \mathbb{T})$, we mean a TSS signature on the message msg modifiable on $\mathbb{T}$.

[8] For $id \in \{0,1\}^l$ and $\mathbb{J} \subseteq [1,l]$, by a DIBS secret-key w.r.t. $(id, \mathbb{J})$, we mean a secret-key for the identity id with the downgradability $\mathbb{J}$.

algorithm. The KI guarantees that they distribute identically to ones generated directly from the master secret-key. Thus, a sanitized signature and its trapdoor distribute identically to fresh ones generated from the signer's TSS secret-key.

INV is also implied by the KI. A TSS signature (= a DIBS secret-key w.r.t. $(msg, \emptyset)$) is generated from a trapdoor (= a DIBS secret-key w.r.t. $(\Phi_{\mathbb{T}}(msg), \mathbb{T})$). The KI guarantees the TSS signature distributes identically to fresh one generated from the signer's TSS secret-key. Thus, it does not include any information about the modifiable parts $\mathbb{T}$.

It can achieve perfect wPRV. For any msg_0, msg_1 and $\mathbb{T}$ queried to the oracle $\mathfrak{SigSanLR}$, since it holds that $\Phi_{\mathbb{T}}(msg_0) = \Phi_{\mathbb{T}}(msg_1)$, the sanitized signature $\overline{\sigma}$ and its trapdoor $\overline{td}$ are generated from a DIBS secret-key w.r.t. $(\Phi_{\mathbb{T}}(msg_0), \mathbb{T})$ in either of the two wPRV experiments.

EUF-CMA of the TSS is reduced to EUF-CMA and KI of the DIBS. The reduction is almost straightforward.

We obtain the following theorem. We rigorously prove it in Subsect. B.6.

Theorem 6. *$\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$ is EUF-CMA if the underlying DIBS scheme Σ_{DIBS} is EUF-CMA and KI. $\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$ is sPRV and INV if Σ_{DIBS} is KI. $\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$ is sPRV and INV if Σ_{DIBS} is KI. $\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$ is perfectly wPRV.*

5.4 Equivalence between TSS and DIBS

TSS and DIBS are equivalent. We have shown that TSS can be (generically) constructed from DIBS. We show that DIBS can be constructed from TSS.

We construct DIBS with identity-length l and message-length m from TSS with message-length $l + m$. The first l bits (resp. the last m bits) of the TSS message are used for the DIBS identity (resp. message). In general, a DIBS secret-key w.r.t. $(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$ is a TSS signature w.r.t. $(id||1^m, \mathbb{J} \cup [l+1, l+m])$ and its trapdoor, and a DIBS signature on $msg \in \{0,1\}^m$ under $id \in \{0,1\}^l$ is a TSS signature w.r.t. $(id||msg, \emptyset)$ (and its trapdoor[9]). The construction TSStoDIBS (interchangeably $\Omega^{\mathrm{DIBS}}_{\mathrm{TSS}}$) based on a TSS scheme $\Sigma_{\mathrm{TSS}} = \{\mathtt{KGen}', \mathtt{Sig}', \mathtt{Sanit}', \mathtt{Ver}'\}$ is formally described as follows.

```
Setup($1^\lambda, l, m$):   Rtn $(mpk, msk) := (pk, sk) \leftarrow \mathtt{KGen}'(1^\lambda, l+m)$.
KGen($msk, id \in \{0,1\}^l$):   Rtn $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \mathtt{Sig}'(pk, sk, id||1^m, \mathbb{I}_1(id) \bigcup [l+1, l+m])$.
Weaken($sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id)$):
  Rtn $\perp$ if $\mathbb{J}' \not\subseteq \mathbb{J}$. Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$.
  Rtn $sk_{id}^{\mathbb{J}'} := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
Down($sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), id' \in \{0,1\}^l$):
  Rtn $\perp$ if $id' \not\preceq_{\mathbb{J}} id$. Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \bigcup [l+1, l+m] \setminus \mathbb{I}_0(id')$.
  Rtn $sk_{id'}^{\mathbb{J}'} := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J}')$.
Sig($sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m \setminus \{1^m\}$):
  Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$.
  $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||msg, \emptyset)$. Rtn $\overline{\sigma}$.
Ver($\sigma, id \in \{0,1\}^l, msg \in \{0,1\}^m \setminus \{1^m\}$):   Rtn $1/0 \leftarrow \mathtt{Ver}'(pk, \sigma, id||msg)$.
```

[9] The trapdoor is unnecessary since the TSS signature cannot be sanitized.

`EUF-CMA` of the DIBS is tightly reduced to `EUF-CMA` of the underlying TSS. The reduction is straightforward.

If the TSS satisfy both `UNL` and `TRN`, then the DIBS satisfy `SP`. Informally, `SP` (under Def. 8) is a property guaranteeing that a signature σ w.r.t. ($id' \preceq_{\mathbb{J}} id$, msg) generated from a secret-key sk w.r.t. $(id, \mathbb{J})$ does not include any specific info about the secret-key. Specifically, the secret-key sk generates a secret-key sk' for id' by `Down`, then sk' generates the signature σ. In TSS`to`DIBS, sk, sk' and σ are a TSS signature on a message $id||1^l$, $id'||1^l$ and $id'||msg$, respectively, and sk (resp. sk') generates sk' (resp. σ) by `Sanit`$'$. `UNL` and `TRN` of TSS guarantee that sk' distributes identically to a *flesh* TSS signature on the same message $id'||1^l$ generated by `Sig`$'$. Furthermore, `TRN` of TSS guarantees that σ distributes identically to a *flesh* TSS signature on the same message $id'||msg$ generated by `Sig`$'$. Hence, σ does not include any information about sk.

We obtain the following theorem. We rigorously prove it in Subsect. B.7.

Theorem 7. *$\Omega^{\text{DIBS}}_{\text{TSS}}$ is `EUF-CMA` if the underlying TSS scheme Σ_{TSS} is `EUF-CMA`. $\Omega^{\text{DIBS}}_{\text{TSS}}$ is `SP` if Σ_{TSS} is `UNL` and `TRN`.*

5.5 Security Analysis of Existing Generic TSS Constructions

We investigate whether existing generic TSS constructions, the IBCH-based one [14] and the digital-signature-based one [29], are secure under our definitions.

The former one (TSS$_{\text{CLM}}$) uses an IBCH and digital signature scheme. It adopts *(IB)CH-then-Sign* approach. Signer's secret-key consists of a master secret-key MSK of the IBCH and a secret-key SK of the digital signature. She signs a message $msg = ||_{i=1}^{n} msg_i \in (\{0,1\}^l)^n$ with $\mathbb{T} \subseteq [1,n]$ as follows. For every $i \in \mathbb{T}$, she computes the hash h_i of the sub-message msg_i under identity msg and a randomness r_i. Let $\hat{msg}_i := h_i$. For every $i \in [1,n] \setminus \mathbb{T}$, simply $\hat{msg}_i := msg_i$. Then, she computes the hash h of msg under identity msg and a randomness r. Then, she generates a signature $\hat{\sigma}$ on $\hat{msg}_1 || \cdots || \hat{msg}_n || h$ using SK. Finally, the signature consists of $(\hat{\sigma}, \{h_i, r_i \mid i \in \mathbb{T}\}, h, r)$. Its trapdoor is a secret-key for the identity msg generated from MSK. We have proven that TSS$_{\text{CLM}}$ is not `wPRV` (implying that it is neither `TRN`, `UNL` nor `sPRV` because of Theorem 4), and that it is not `INV`. The proofs can be seen in Sect. D.

The latter one (TSS$_{\text{YSL}}$) is simple. Signer's key-pair is (VK, SK) of the signature scheme. To sign a message $msg \in \{0,1\}^l$ for $\mathbb{T} \subseteq [1,l]$, the signer generates a new key-pair $(\hat{VK}, \hat{SK})$, then makes a message $\hat{msg} := ||_{i=1}^{l} \hat{msg}_i$, where $\hat{msg}_i$ is set to a special symbol, e.g., $\star$, (if $i \in \mathbb{T}$) or msg_i (otherwise). The signature consists of $(\hat{VK}, \sigma_0, \sigma_1)$, where σ_0 is a signature on a message $\hat{VK}||\hat{msg}$ generated by SK, and σ_1 is a signature on $\hat{VK}||\hat{msg}||msg$ by $\hat{SK}$. The trapdoor is $\hat{SK}$. We have proven that TSS$_{\text{YSL}}$ is perfectly `TRN` (implying that it is perfectly `wPRV`), that it is not `UNL` (implying that it is not `sPRV`), and that it is not `INV`. The proofs can be seen in Sect. D.

TSS$_{\text{Ours}}$ denotes the DIBS-based TSS construction in Subsect. 5.3, instantiated by the DAMAC-based DIBS construction in Subsect. 4.2. TSS$_{\text{Ours}}$ is the first one achieving `UNL` and/or `INV` (and `sPRV`). As a result, we obtain Table 2.

Gene. Const.	Building Blo.	UNF(IMM)	TRN	wPRV	UNL	INV	sPRV	Assumptions
TSS_{CLM} [14]	IBCH, DS	sEUF-CMA	✗	✗	✗	✗	✗	CR (IBCH), sEUF-CMA (DS)
TSS_{YSL} [29]	DS	EUF-CMA	P	P	✗	✗	✗	EUF-CMA (DS)
TSS_{Ours}	DAMAC	EUF-CMA	S	P	S	S	S	PR-CMA1 (DAMAC), MDDH

Table 2. Comparison among existing generic TSS constructions. ✗ means that even the statistical security cannot be achieved. P (resp. S) means perfect (resp. statistical). CR means collision-resistance. sEUF-CMA means the strong existential unforgeability.

6 Equivalence among DIBS, TSS and DIBTSS

Downgradable identity-based TSS (DIBTSS) are DIBS, where each signature can be sanitized using its trapdoor. Its syntax and security are formally defined in Subsect. E.1. A DAMAC-based generic construction is described in Subsect. E.2. Implication from DIBTSS to either of DIBS and TSS is obvious. We prove implications from either of TSS and DIBS to DIBTSS in Subsections E.3, E.4.

References

1. M. Abdalla, D. Catalano, A.W. Dent, J. Malone-Lee, G. Neven, and N.P. Smart. Identity-based encryption gone wild. In *ICALP 2006*, pp. 300–311. Springer, 2006.
2. M. Abdalla, E. Kiltz, and G. Neven. Generalized key delegation for hierarchical identity-based encryption. In *ESORICS 2007*, pp. 139–154. Springer, 2007.
3. G. Ateniese, D.H. Chou, B. De Medeiros, and G. Tsudik. Sanitizable signatures. In *ESORICS 2005*, pp. 159–177. Springer, 2005.
4. M. T. Beck, J. Camenisch, D. Derler, S. Krenn, H.C. Pöhls, K. Samelin, and D. Slamanig. Practical strongly invisible and strongly accountable sanitizable signatures. In *ACISP 2017*, pp. 437–452. Springer, 2017.
5. M. Bellare and S. Goldwasser. New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. In *CRYPTO 1989*, pp. 194–211. Springer, 1989.
6. J. Birkett, A.W. Dent, G. Neven, and J.C.N. Schuldt. Efficient chosen-ciphertext secure identity-based encryption with wildcards. In *ACISP 2007*, pp. 274–292. Springer, 2007.
7. O. Blazy, P. Germouty, and D. H. Phan. Downgradable identity-based encryption and applications. In *CT-RSA 2019*, pp. 44–61. Springer, 2019.
8. O. Blazy, E. Kiltz, and J. Pan. (hierarchical) identity-based encryption from affine message authentication. In *CRYPTO 2014*, pp. 408–425. Springer, 2014.
9. C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schröder, and F. Volk. Security of sanitizable signatures revisited. In *PKC 2009*, pp. 317–336. Springer, 2009.
10. C. Brzuska, M. Fischlin, A. Lehmann, and D. Schröder. Unlinkability of sanitizable signatures. In *PKC 2010*, pp. 444–461. Springer, 2010.
11. X. Bultel and P. Lafourcade. Unlinkable and strongly accountable sanitizable signatures from verifiable ring signatures. In *CANS 2017*, pp. 203–226. Springer, 2017.

12. X. Bultel, P. Lafourcade, R. Lai, G. Malavolta, D. Schröder, S. Aravinda, and K. Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. In *PKC 2019*, pp. 159–189. Springer, 2019.
13. J. Camenisch, D. Derler, S. Krenn, H. C. Pöhls, K. Samelin, and D. Slamanig. Chameleon-hashes with ephemeral trapdoors and applications to invisible sanitizable signatures. In *PKC 2017*, pp. 152–182. Springer, 2017.
14. S. Canard, F. Laguillaumie, and M. Milhau. Trapdoor sanitizable signatures and their application to content protection. In *ACNS 2008*, pp. 258–276. Springer, 2008.
15. S. Chatterjee and P. Sarkar. Practical hybrid (hierarchical) identity-based encryption schemes based on the decisional bilinear diffie-hellman assumption. *International Journal of Applied Cryptography (IJACT)*, 3(1):47–83, 2013.
16. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for diffie-hellman assumptions. In *CRYPTO 2013*, pp. 129–147. Springer, 2013.
17. N. Fleischhacker, J. Krupp, G. Malavolta, J. Schneider, D. Schröder, and M. Simkin. Efficient unlinkable sanitizable signatures from signatures with re-randomizable keys. In *PKC 2016*, pp. 301–330. Springer, 2016.
18. C. Gentry and A. Silverberg. Hierarchical id-based cryptography. In *ASIACRYPT 2002*, pp. 548–566. Springer, 2002.
19. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT 2008*, pp. 415–432. Springer, 2008.
20. J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In *EUROCRYPT 2002*, pp. 466–481. Springer, 2002.
21. E. Kiltz and G. Neven. Identity-based signatures. *Identity-Based Cryptography*, 2(31):75, 2009.
22. S. Krenn, K. Samelin, and D. Sommer. Stronger security for sanitizable signatures. In *DPM 2015*, pp. 100–117. Springer, 2015.
23. R. Langrehr and J. Pan. Tightly secure hierarchical identity-based encryption. In *PKC 2019*, pp. 436–465. Springer, 2019.
24. R. Langrehr and J. Pan. Hierarchical identity-based encryption with tight multi-challenge security. In *PKC 2020*, pp. 153–183. Springer, 2020.
25. H.K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. In *CT-RSA 2011*, pp. 376–392. Springer, 2011.
26. K.G. Paterson and J.C.N. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP 2006*, pp. 207–222. Springer, 2006.
27. Y. Sakai, N. Attrapadung, and G. Hanaoka. Attribute-based signatures for circuits from bilinear map. In *PKC 2016*, pp. 283–300. Springer, 2016.
28. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO 1984*, pp. 47–53. Springer, 1984.
29. D. H. Yum, J. W. Seo, and P. J. Lee. Trapdoor sanitizable signatures made easy. In *ACNS 2010*, pp. 53–68. Springer, 2010.

A Identity-Based Signatures (IBS) and Wildcarded IBS (WIBS)

Syntax. IBS (resp. WIBS) consist of following 4 polynomial time algorithms: Let $l \in \mathbb{N}$ denote length of an identity. **Setup** algorithm $\mathtt{Setup}$ takes 1^λ, l and m as input, then outputs mpk and msk. We write $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$.

Key-generation algorithm $\mathtt{KGen}$ takes msk and an identity $id \in \{0,1\}^l$, then outputs a sk_{id} for the identity. We write $sk_{id} \leftarrow \mathtt{KGen}(msk, id)$. **Signing** algorithm $\mathtt{Sig}$ takes a sk_{id}, an identity $id' \in \{0,1\}^l$ (resp. a wildcarded identity $id' \in \{0,1,*\}^l$), and a $msg \in \{0,1\}^m$, then outputs a signature σ. We write $\sigma \leftarrow \mathtt{Sig}(sk_{id}, id', msg)$. **Verifying** algorithm $\mathtt{Ver}$ takes a signature σ, an $id' \in \{0,1\}^l$ (resp. $id' \in \{0,1,*\}^l$) and a $msg \in \{0,1\}^m$, then outputs $1/0$. We write $1/0 \leftarrow \mathtt{Ver}(\sigma, id', msg)$.

Every IBS or WIBS scheme is required to be correct under the following definition.

Definition 12. *An IBS scheme (resp. A WIBS scheme) is correct, if* $\forall \lambda, l, m \in \mathbb{N}$, $\forall (mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$, $\forall id \in \{0,1\}^l$, $\forall sk_{id} \leftarrow \mathtt{KGen}(msk, id)$, $\forall id' \in \{0,1\}^l$ *s.t.* $id' = id$, *(resp.* $\forall id' \in \{0,1,*\}^l$ *s.t.* $\bigwedge_{i \in [1,l] \text{ s.t. } id'[i] \neq *} id[i] = id'[i]$*,)* $\forall msg \in \{0,1\}^m$, $\forall \sigma \leftarrow \mathtt{Sig}(sk_{id}, id', msg)$, $1 \leftarrow \mathtt{Ver}(\sigma, id', msg)$.

Existential Unforgeability for IBS and WIBS. We require an IBS or WIBS scheme to be existentially unforgeable (EUF-CMA). For a probabilistic algorithm $\mathcal{A}$, the EUF-CMA experiment w.r.t. a WIBS scheme $\boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\mathrm{WIBS}},\mathcal{A}}$ is defined as in Fig. 3. Analogously, the experiment w.r.t. an IBS scheme $\boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\mathrm{IBS}},\mathcal{A}}$ is defined. The difference is that every identity queried to the signing oracle id and the target identity wid^* must be a non-wildcarded identity.

Definition 13. *An IBS scheme* Σ_{IBS} *(resp. A WIBE scheme* Σ_{WIBS}*) is existentially unforgeable, if* $\forall \lambda, l, m \in \mathbb{N}$, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{Adv}^{\mathit{EUF\text{-}CMA}}_{\Sigma_{\mathrm{IBS}}(resp.\ \Sigma_{\mathrm{WIBS}}),\mathcal{A},l,m}(\lambda) := \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathit{EUF\text{-}CMA}}_{\Sigma_{\mathrm{IBS}}(resp.\ \Sigma_{\mathrm{WIBS}}),\mathcal{A}}(1^\lambda, l, m)] < \epsilon$.

Signer-Privacy for WIBS. We require a WIBS scheme to be signer-private. For a probabilistic algorithm $\mathcal{A}$, we consider two experiments described in Fig. 3.

Definition 14. *A WIBS scheme* Σ_{WIBS} *is statistically (resp. perfectly) signer private, if for every* $\lambda, l, m \in \mathbb{N}$ *and every probabilistic algorithm* $\mathcal{A}$*, there exist polynomial time algorithms* $\Sigma'_{\mathrm{WIBS}} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Sig}'\}$ *and a negligible function* $\epsilon \in \mathsf{NGL}_\lambda$ *such that* $\boldsymbol{Adv}^{\mathit{SP}}_{\Sigma_{\mathrm{WIBS}},\Sigma'_{\mathrm{WIBS}},\mathcal{A},l,m}(\lambda) := |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathit{SP}}_{\Sigma_{\mathrm{WIBS}},\mathcal{A},0}(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathit{SP}}_{\Sigma_{\mathrm{WIBS}},\mathcal{A},1}(1^\lambda, l, m))]|$ *is less than* ϵ *(resp. equal to* 0*).*

B Omitted Proofs

B.1 Proof of Theorem 1 (on $\mathtt{PR\text{-}CMA1}$ of Π_{DAMAC})

Let $\boldsymbol{Expt}_0$ (resp. $\boldsymbol{Expt}_1$) denote the pseudo-randomness experiment in Fig. **??** parameterized by $b = 0$ (resp. $b = 1$) w.r.t. our DAMAC scheme Π_{DAMAC}, i.e., $\boldsymbol{Expt}^{\mathtt{PR\text{-}CMA1}}_{\Pi_{\mathrm{DAMAC}},\mathcal{A},0}$ (resp. $\boldsymbol{Expt}^{\mathtt{PR\text{-}CMA1}}_{\Pi_{\mathrm{DAMAC}},\mathcal{A},1}$). To prove the indistinguishability between them, we introduce multiple experiments $(\boldsymbol{Expt}_{b.0.j}, \boldsymbol{Expt}'_{b.0.j})$ where $b \in \{0,1\}$ and $j \in [0, q_e]$, and $(\boldsymbol{Expt}_{b.1.j}, \boldsymbol{Expt}'_{b.1.j})$, where $b \in \{0,1\}$ and $j \in [0, q'_e]$. Their formal definitions are described in Fig. 4. Note that, for each

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\mathrm{WIBS}},\mathcal{A}}(1^\lambda, l, m)$:
    $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$.
    $(\sigma^*, wid^* \in \{0,1,*\}^l, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$: $sk \leftarrow \texttt{KGen}(msk, id)$. $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{id\}$. $\textbf{Rtn } sk$.
    $-\mathfrak{Sign}(id \in \{0,1\}^l, wid \in \{0,1,*\}^l, msg \in \{0,1\}^m)$:
        $\textbf{Rtn} \perp$ if $\bigvee_{i\in[1,l]}[id[i] \neq wid[i] \implies wid[i] \neq *]$.
        $\sigma \leftarrow \texttt{Sig}(\texttt{KGen}(msk, id), wid, msg)$. $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(wid, msg, \sigma)\}$. $\textbf{Rtn } \sigma$.
    $\textbf{Rtn } 1$ if $1 \leftarrow \texttt{Ver}(\sigma^*, wid^*, msg^*) \bigwedge_{id\in\mathbb{Q}_r} \bigwedge_{i\in[1,l]}[id[i] \neq wid^*[i] \implies wid^*[i] = *]$
    $\bigwedge_{(wid,msg,\cdot)\in\mathbb{Q}_s}(wid, msg) \neq (wid^*, msg^*)$. $\textbf{Rtn } 0$.
$\boldsymbol{Expt}^{\texttt{SP}}_{\Sigma_{\mathrm{WIBS}},\mathcal{A},b}(1^\lambda, l, m)$:   // $b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$. $(mpk, msk') \leftarrow \texttt{Setup}'(1^\lambda, l, m)$.
    $\textbf{Rtn } b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk, msk)$, where
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$: $sk \leftarrow \texttt{KGen}(msk, id)$. $sk \leftarrow \texttt{KGen}'(msk', id)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id)\}$. $\textbf{Rtn } sk$.
    $-\mathfrak{Sign}(sk, id \in \{0,1\}^l, wid \in \{0,1,*\}^l, msg \in \{0,1\}^m)$:
        $\textbf{Rtn} \perp$ if $(sk, id) \notin \mathbb{Q} \bigvee_{i\in[1,l]}[id[i] \neq wid[i] \implies wid[i] \neq *]$.
        $\sigma \leftarrow \texttt{Sig}(sk, id, wid, msg)$. $\sigma \leftarrow \texttt{Sig}'(msk', wid, msg)$. $\textbf{Rtn } \sigma$.
```

Fig. 3. Experiments for EUF-CMA and signer-privacy w.r.t. a WIBS scheme Σ_{WIBS}

$b \in \{0, 1\}$, $\boldsymbol{Expt}_b$ (resp. $\boldsymbol{Expt}'_{b.0.q_e}$) is identical to $\boldsymbol{Expt}'_{b.0.0}$ (resp. $\boldsymbol{Expt}'_{b.1.0}$).

Based on the definitions of the experiments and the triangle inequality, we obtain

$$\begin{aligned}
\texttt{Adv}^{\texttt{PR-CMA1}}_{\Pi_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) &= |\Pr[1 \leftarrow \boldsymbol{Expt}_0(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}_1(par)]| \\
&\leq \sum_{b=0}^{1} \Big\{ |\Pr[1 \leftarrow \boldsymbol{Expt}_b(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}'_{b.0.0}(par)]| \\
&\quad + \sum_{j=1}^{q_e} \left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.j-1}(par)\right] - \Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.q_e}(par)]\right| \\
&\quad + \sum_{j=1}^{q_e} \left|\Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.j}(par)\right]\right| \\
&\quad + \left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.q_e}(par)\right] - \Pr[1 \leftarrow \boldsymbol{Expt}'_{b.1.0}(par)]\right| \\
&\quad + \sum_{j=1}^{q'_e} \left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.1.j-1}(par)\right] - \Pr[1 \leftarrow \boldsymbol{Expt}_{b.1.q_e}(par)]\right| \\
&\quad + \sum_{j=1}^{q'_e} \left|\Pr[1 \leftarrow \boldsymbol{Expt}_{b.1.j}(par)] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.1.j}(par)\right]\right| \Bigg\} \\
&\quad + \left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{0.1.q'_e}(par)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{1.1.q'_e}(par)\right]\right|.
\end{aligned}$$

```
$\boldsymbol{Expt}_{b.0.j}(par)$:   // $\boxed{\boldsymbol{Expt}'_{b.0.j}}$
$\boldsymbol{Expt}_{b.1.j}(par)$:   // $\boxed{\boldsymbol{Expt}'_{b.1.j}}$

    $sk_{\mathrm{MAC}} := (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x)$, where $B \leftarrow\!\!\!\sim \mathcal{D}_k$, $\boldsymbol{x}_i \in \mathbb{Z}_p^{k+1}$ and $x \leftarrow\!\!\!\sim \mathbb{Z}_p$.
    $(msg^* \in \{0,1\}^l, st) \leftarrow \mathcal{A}_0^{\mathfrak{Eval}_0, \mathfrak{Eval}_1}(par)$:

    $-\mathfrak{Eval}_0(msg_\iota \in \{0,1\}^l, \mathbb{J}_\iota \subseteq \mathbb{I}_1(msg_\iota))$:
                                        $//\iota \in [1, q_e]$
        If $\iota > j$:
            $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$, $\boldsymbol{t} := B\boldsymbol{s}$.
            $u := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\iota[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x$.
            $S \leftarrow\!\!\!\sim \mathbb{Z}_p^{n' \times n'}$, $T := BS$.
            $\boldsymbol{w} := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\iota[i]\boldsymbol{x}_i^\top)T$.
            For $i \in \mathbb{J}_\iota$:   $d_i := \boldsymbol{x}_i^\top \boldsymbol{t}$, $\boldsymbol{e}_i := \boldsymbol{x}_i^\top T$.
        If $\iota < j$:
            $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $T \leftarrow\!\!\!\sim \mathbb{Z}_p^{(k+1)\times k}$.
            $u \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{w} \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$.
            For $i \in \mathbb{J}_\iota$:   $d_i \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{e}_i \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$.
        If $\iota = j$:
            $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $T \leftarrow\!\!\!\sim \mathbb{Z}_p^{(k+1)\times k}$.
            $u := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\iota[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x$. $\boxed{u \leftarrow\!\!\!\sim \mathbb{Z}_p.}$
            $\boldsymbol{w} := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\iota[i]\boldsymbol{x}_i^\top)T$. $\boxed{\boldsymbol{w} \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}.}$
            For $i \in \mathbb{J}_\iota$:   $d_i := \boldsymbol{x}_i^\top \boldsymbol{t}$, $\boldsymbol{e}_i := \boldsymbol{x}_i^\top T$.
                                $\boxed{d_i \leftarrow\!\!\!\sim \mathbb{Z}_p,\ \boldsymbol{e}_i \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}.}$
        Rtn $\tau := ([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2,$
                $\{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}_\iota\})$.
    $-\mathfrak{Eval}_1(msg_\theta \in \{0,1\}^l)$:   $//\ \theta \in [1, q'_e]$
        $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$, $\boldsymbol{t} := B\boldsymbol{s}$.
        $u := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x$.
        Rtn $\tau := ([\boldsymbol{t}]_2, [u]_2)$.

    $-\mathfrak{Eval}_0(msg_\iota \in \{0,1\}^l, \mathbb{J}_\iota \subseteq \mathbb{I}_1(msg_\iota))$:
                                        $//\ \iota \in [1, q_e]$
        $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $T \leftarrow\!\!\!\sim \mathbb{Z}_p^{(k+1)\times k}$.
        $u \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{w} \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$.
        For $i \in \mathbb{J}_\iota$: $d_i \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{e}_i \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$.
        Rtn $\tau := ([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2,$
            $\{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}_\iota\})$.

    $-\mathfrak{Eval}_1(msg_\theta \in \{0,1\}^l)$:   $//\theta \in [1, q'_e]$
        If $\theta > j$:
            $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$, $\boldsymbol{t} := B\boldsymbol{s}$.
            $u := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x$.
        If $\theta < j$: $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $u \leftarrow\!\!\!\sim \mathbb{Z}_p$.
        If $\theta = j$:
            $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$.
            $u := (\boldsymbol{x}_0^\top + \sum_{i=1}^{l} msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x$.
            $\boxed{u \leftarrow\!\!\!\sim \mathbb{Z}_p.}$
        Rtn $\tau := ([\boldsymbol{t}]_2, [u]_2)$.

    Abt if $\bigvee_{\iota=1}^{q_e} msg_\iota \succeq_{\mathbb{J}_\iota} msg^* \bigvee_{\theta=1}^{q'_e} msg_\theta = msg^*$.
    $h \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{h}_0 := (\boldsymbol{x}_0 + \sum_{i=1}^{l} msg^*[i]\boldsymbol{x}_i)h$. If $b = 0$, $h_1 := xh$. If $b = 1$, $h_1 \leftarrow\!\!\!\sim \mathbb{Z}_p$.
    Rtn $b' \leftarrow \mathcal{A}_1(st, [h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$.
```

Fig. 4. $2(q_e+q'_e+2)$ experiments to prove PR-CMA1 of $\mathit{\Pi}_{\mathrm{DAMAC}} = \{\mathtt{Gen}_{\mathrm{MAC}}, \mathtt{Tag}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Ver}\}$: $\{\boldsymbol{Expt}_{b.0.j}, \boldsymbol{Expt}'_{b.0.j} \mid b \in \{0,1\}, j \in [0, q_e]\}$, $\{\boldsymbol{Expt}_{b.1.j}, \boldsymbol{Expt}'_{b.1.j} \mid b \in \{0,1\}, j \in [0, q'_e]\}$.

We provide 7 lemmata, i.e., Lemmata 2, 3, 4, 5, 6, 7, 8, below, each of which is accompanied by a proof, except for Lemmata 2, 5. Each of the two lemmata is obviously true since (as we mentioned earlier) the two experiments (considered in the lemma) are identical. By the 7 lemmata, we conclude that for every $\mathcal{A} \in \mathsf{PPTA}_\lambda$, there exist $\mathcal{B} \in \mathsf{PPTA}_\lambda$ such that $\mathtt{Adv}^{\mathtt{PR\text{-}CMA1}}_{\Pi_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) \leq 2\{(k+1)q_e + q'_e\}(\frac{1}{p} + \frac{1}{p^{k+1}}) + \frac{4q_e}{p-1} + 2(q_e + q'_e)\mathtt{Adv}^{\mathcal{D}_k-\mathtt{MDDH}}_{\mathcal{B},\mathcal{G}_{BG},\mathbb{G}_2}(\lambda)$. □

Lemma 2. $\forall b \in \{0,1\}$, $|\Pr[1 \leftarrow \boldsymbol{Expt}_b(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}'_{b.0.0}(par)]| = 0$.

Lemma 3. $\forall b \in \{0,1\}, \forall j \in [1, q_e], \exists \mathcal{B}_1 \in \mathsf{PPTA}_\lambda, |\Pr[1 \leftarrow \boldsymbol{Expt}'_{b.0.j-1}(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)]| \leq \mathit{Adv}^{\mathcal{D}_k-\mathit{MDDH}}_{\mathcal{B}_1,\mathcal{G}_{BG},\mathbb{G}_2}(\lambda) + \frac{1}{p-1}$.

Proof. $\hat{\mathcal{B}}_1$ is a PPT algorithm attempting to break $(\mathcal{D}_k, k+1)$-MDDH assumption w.r.t. $\mathcal{G}_{BG}$ and $\mathbb{G}_2$ by using $\mathcal{A}$ as a subroutine. $\hat{\mathcal{B}}_1$ behaves as described in Fig. 5. Obviously, if $V = B\hat{W}$ (resp. $V = \hat{U}$), $\hat{\mathcal{B}}_1$ perfectly simulates $\boldsymbol{Expt}'_{b.0.j-1}$ (resp. $\boldsymbol{Expt}_{b.0.j}$) to $\mathcal{A}$, and if (and only if) $\mathcal{A}$ acts in a way letting the experiment return 1, $\hat{\mathcal{B}}_1$ returns 1. Thus, $\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.j-1}(par)\right] = \Pr\left[1 \leftarrow \hat{\mathcal{B}}_1\left(gd, [B]_2, \left[B\hat{W}\right]_2\right)\right]$ (resp. $\Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)] = \Pr\left[1 \leftarrow \hat{\mathcal{B}}_1\left(gd, [B]_2, \left[\hat{U}\right]_2\right)\right]$) holds. Hence, $|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.j-1}(par)\right] - \Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)]| = \mathtt{Adv}^{(\mathcal{D}_k,k+1)-\mathtt{MDDH}}_{\hat{\mathcal{B}}_1,\mathcal{G}_{BG},\mathbb{G}_2}(\lambda)$. By Lemma 1, $\forall \hat{\mathcal{B}}_1 \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B}_1$ s.t. $\mathtt{Adv}^{(\mathcal{D}_k,k+1)-\mathtt{MDDH}}_{\hat{\mathcal{B}}_1,\mathcal{G}_{BG},\mathbb{G}_2}(\lambda) \leq \mathtt{Adv}^{\mathcal{D}_k-\mathtt{MDDH}}_{\mathcal{B}_1,\mathcal{G}_{BG},\mathbb{G}_2}(\lambda) + \frac{1}{p-1}$. □

Lemma 4. $\forall b \in \{0,1\}, \forall j \in [1, q_e], \left|\Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.j}(par)\right]\right| \leq (k+1)(\frac{1}{p} + \frac{1}{p^{k+1}}) + \frac{1}{p-1}$.

Proof. Let $\mathbf{E}_1$ denote the event where $\boldsymbol{t}^\top \leftsquigarrow \mathbb{Z}_p^{1\times(k+1)}$ is not the zero vector. Let $\mathbf{E}_2$ denote the event where any row vector in $T^\top \leftsquigarrow \mathbb{Z}_p^{k\times(k+1)}$ is not the zero vector. Let $\mathbf{E}_3$ denote the event where $\boldsymbol{t}^\top \leftsquigarrow \mathbb{Z}_p^{1\times(k+1)}$ is not in the span of $B^\top \in \mathbb{Z}_p^{k\times(k+1)}$ (where $B \leftsquigarrow \mathcal{D}_k$). Let $\mathbf{E}_4$ denote the event where any row vector in $T^\top \leftsquigarrow \mathbb{Z}_p^{k\times(k+1)}$ is not in the span of $B^\top \in \mathbb{Z}_p^{k\times(k+1)}$ (where $B \leftsquigarrow \mathcal{D}_k$). Let $\mathbf{E}_5$ denote the event where $\boldsymbol{t}^\top \leftsquigarrow \mathbb{Z}_p^{1\times(k+1)}$ and $T^\top \leftsquigarrow \mathbb{Z}_p^{k\times(k+1)}$ are linearly independent. The proof proceeds under the assumption that all of the events have occurred. Later we rigorously prove that the probability that at least one of the events does not occur is negligibly small, which implies that the assumption is reasonably valid.

Obviously, $\bigwedge_{\iota\in[1,q_e]} msg^* \not\preceq_{\mathbb{J}_\iota} msg_\iota$ implies that $[\exists \hat{i} \in \mathbb{I}_0(msg_\iota)$ s.t. $msg^*[\hat{i}] = 1] \bigvee [\exists \hat{i} \in \mathbb{I}_1(msg_\iota) \setminus \mathbb{J}_\iota$ s.t. $msg^*[\hat{i}] = 0]$.

To make the proof simpler, we assume that the adversary $\mathcal{A}$ knows $x \in \mathbb{Z}_p$ and $\{\boldsymbol{x}_i \in \mathbb{Z}_p^{k+1} \mid i \in [1, l] \backslash \{\hat{i}\} \backslash \mathbb{I}_1(msg_j)\}$. We parse $\mathbb{I}_1(msg_j)$ as $\{\kappa_1, \cdots, \kappa_n\}$, where $n := |\mathbb{I}_1(msg_j)|$. Note that some information about $\boldsymbol{x}_0$, $\boldsymbol{x}_{\hat{i}}$, $\boldsymbol{x}_{\kappa_1}$, $\cdots$, $\boldsymbol{x}_{\kappa_n}$ are leaked through the DAMAC $([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2 \mid i \in \mathbb{I}_1(msg_{\iota'})\})$ on

```
$\hat{\mathcal{B}}_1(gd, [B]_2, [V]_2)$:   // $gd = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2) \leftarrow \mathcal{G}_{BG}(1^\lambda)$. $B \leftsquigarrow \mathcal{D}_k$.
                    // $V = A\hat{W}$ or $\hat{U}$ (where $\hat{W} \leftsquigarrow \mathbb{Z}_p^{k\times(k+1)}$, $\hat{U} \leftsquigarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$).
    For $i \in [0, l]$, $\boldsymbol{x}_i \in \mathbb{Z}_p^{k+1}$. $x \leftsquigarrow \mathbb{Z}_p$.
    $(msg^* \in \{0,1\}^l, st) \leftarrow \mathcal{A}_0^{\mathfrak{Eval}_0, \mathfrak{Eval}_1}(par)$:
    $-\mathfrak{Eval}_0(msg_\iota \in \{0,1\}^l, \mathbb{J}_\iota \subseteq \mathbb{I}_1(msg_\iota))$:
        If $\iota > j$:
            $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^k$, $[\boldsymbol{t}]_2 := [B\boldsymbol{s}]_2$. $[u]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\iota[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$.
            $S \leftsquigarrow \mathbb{Z}_p^{n'\times n'}$, $[T]_2 := [BS]_2$.
            $[\boldsymbol{w}]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\iota[i]\boldsymbol{x}_i^\top)T\right]_2$.
            For $i \in \mathbb{J}_\iota$, $[d_i]_2 := \left[\boldsymbol{x}_i^\top \boldsymbol{t}\right]_2$ and $[\boldsymbol{e}_i]_2 := \left[\boldsymbol{x}_i^\top T\right]_2$.
        If $\iota < j$:
            $\boldsymbol{t} \leftsquigarrow \mathbb{Z}_p^{k+1}$, $T \leftsquigarrow \mathbb{Z}_p^{(k+1)\times k}$. $u \leftsquigarrow \mathbb{Z}_p$, $\boldsymbol{w} \leftsquigarrow \mathbb{Z}_p^{1\times k}$.
            For $i \in \mathbb{J}_\iota$, $d_i \leftsquigarrow \mathbb{Z}_p$ and $\boldsymbol{e}_i \leftsquigarrow \mathbb{Z}_p^{1\times k}$.
        If $\iota = j$:
            For $V \in \mathbb{Z}_p^{(k+1)\times(k+1)}$ in $[V]_2 \in \mathbb{G}^{(k+1)\times(k+1)}$,
              parse $V = (\boldsymbol{v}|V')$, where $\boldsymbol{v} \in \mathbb{Z}_p^{k+1}$ and $V' \in \mathbb{Z}_p^{(k+1)\times k}$.
            $[\boldsymbol{t}]_2 := [\boldsymbol{v}]_2$, $[T]_2 := [V']_2$. $[u]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\iota[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$.
            $[\boldsymbol{w}]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\iota[i]\boldsymbol{x}_i^\top)T\right]_2$.
            For $i \in \mathbb{J}_\iota$, $[d_i]_2 := \left[\boldsymbol{x}_i^\top \boldsymbol{t}\right]_2$ and $[\boldsymbol{e}_i]_2 := \left[\boldsymbol{x}_i^\top T\right]_2$.
        **Rtn** $\tau := ([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2, \{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}_\iota\})$.
    $-\mathfrak{Eval}_1(msg_\theta \in \{0,1\}^l)$:
        $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^k$, $[\boldsymbol{t}]_2 := [B\boldsymbol{s}]_2$. $[u]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$.
        **Rtn** $\tau := ([\boldsymbol{t}]_2, [u]_2)$.
    **Abt** if $\bigvee_{\iota=1}^{q_e} msg_\iota \succeq_{\mathbb{J}_\iota} msg^* \bigvee_{\theta=1}^{q_e'} msg_\theta = msg^*$.
    $h \leftsquigarrow \mathbb{Z}_p$, $\boldsymbol{h}_0 := (\boldsymbol{x}_0 + \sum_{i=1}^l msg^*[i]\boldsymbol{x}_i)h$. If $b = 0$, $h_1 := xh$. If $b = 1$, $h_1 \leftsquigarrow \mathbb{Z}_p$.
    **Rtn** $b' \leftarrow \mathcal{A}_1(st, [h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$.
```

Fig. 5. Simulator $\hat{\mathcal{B}}_1$ introduced to prove Lemma 3

the $\iota'(> j)$-th query to $\mathfrak{Eval}_0$ and the MAC $([\boldsymbol{t}]_2, [u]_2)$ on every query to $\mathfrak{Eval}_1$ in the form of $B^\top \boldsymbol{x}_0$, $B^\top \boldsymbol{x}_{\hat{i}}$, $B^\top \boldsymbol{x}_{\kappa_1}, \cdots, B^\top \boldsymbol{x}_{\kappa_n}$. Thus, $\mathcal{A}$ information-theoretically obtains the following information.

$$\begin{array}{r}
k \\ 2k \\ 3k \\ (n+1)k \\ (n+2)k \\ (n+3)k+1 \\ (n+3)k+2 \\ (n+4)k+2 \\ (n+4)k+3 \\ (n+5)k+3 \\ (2n+4)k+n+2 \\ (2n+4)k+n+3 \\ (2n+5)k+n+3
\end{array}
\begin{pmatrix}
B^\top \boldsymbol{x}_0 \\ B^\top \boldsymbol{x}_{\hat{i}} \\ B^\top \boldsymbol{x}_{\kappa_1} \\ \vdots \\ B^\top \boldsymbol{x}_{\kappa_n} \\ \boldsymbol{h}_0 \\ u - x \\ \boldsymbol{w}^\top \\ d_{\kappa_1} \\ \boldsymbol{d}_{\kappa_1} \\ \vdots \\ d_{\kappa_n} \\ \boldsymbol{d}_{\kappa_n}
\end{pmatrix}
=
\begin{pmatrix}
B^\top & 0 & 0 & \cdots & 0 \\
0 & B^\top & 0 & \cdots & 0 \\
0 & 0 & B^\top & \cdots & 0 \\
 & \vdots & & \vdots & \\
0 & 0 & 0 & \cdots & B^\top \\
hI_{k+1} & hI_{k+1} & msg^*[\kappa_1]hI_{k+1} & \cdots & msg^*[\kappa_n]hI_{k+1} \\
\boldsymbol{t}^\top & 0 & \boldsymbol{t}^\top & \cdots & \boldsymbol{t}^\top \\
T^\top & 0 & T^\top & \cdots & T^\top \\
0 & 0 & \boldsymbol{t}^\top & \cdots & 0 \\
0 & 0 & T^\top & \cdots & 0 \\
 & \vdots & & \vdots & \\
0 & 0 & 0 & \cdots & \boldsymbol{t}^\top \\
0 & 0 & 0 & \cdots & T^\top
\end{pmatrix}
\begin{pmatrix}
\boldsymbol{x}_0 \\ \boldsymbol{x}_{\hat{i}} \\ \boldsymbol{x}_{\kappa_1} \\ \vdots \\ \boldsymbol{x}_{\kappa_n}
\end{pmatrix}
=: M
\begin{pmatrix}
\boldsymbol{x}_0 \\ \boldsymbol{x}_{\hat{i}} \\ \boldsymbol{x}_{\kappa_1} \\ \vdots \\ \boldsymbol{x}_{\kappa_n}
\end{pmatrix},$$

where the introduced matrix M is in $\mathbb{Z}_p^{\{(2n+5)k+n+3\}\times\{(k+1)(n+2)\}}$.

We prove that, under the assumption that $\bigwedge_{i=1}^{5} \mathbf{E}_i$, every row vector which is in from the $\{(n+3)k+2\}$-th row to the $\{(2n+5)k+n+3\}$-th row in M is linearly independent from every one of the other row vectors.

Firstly, we prove the linear independence of $\left(\boldsymbol{t}^\top\ 0\ \boldsymbol{t}^\top \cdots \boldsymbol{t}^\top\right)$. Because of $\mathbf{E}_1 \bigwedge \mathbf{E}_3$, the vector $\boldsymbol{t}^\top$ is linearly independent of $B^\top$. Hence, the vector is linearly independent of $\left(B^\top\ 0\ 0 \cdots 0\right)$, $\left(0\ 0\ B^\top \cdots 0\right)$, $\cdots$, $\left(0\ 0\ 0 \cdots B^\top\right)$. The vector is also linearly independent of

$$\begin{aligned}
\left(0\ B^\top\ 0 \cdots 0\right) &\quad (\because\ \mathbf{E}_1 \bigwedge \mathtt{rank}(B^\top) = k.), \\
\left(hI_{k+1}\ hI_{k+1}\ msg^*[\kappa_1]hI_{k+1} \cdots msg^*[\kappa_n]hI_{k+1}\right) &\quad (\because\ \mathbf{E}_1), \\
\left(T^\top\ 0\ T^\top \cdots T^\top\right) &\quad (\because\ \mathbf{E}_5), \\
\left(0\ 0\ \boldsymbol{t}^\top \cdots 0\right) &\quad (\because\ \mathbf{E}_1), \\
\vdots\quad & \\
\left(0\ 0\ 0 \cdots \boldsymbol{t}^\top\right) &\quad (\because\ \mathbf{E}_1), \\
\left(0\ 0\ T^\top \cdots 0\right) &\quad (\because\ \mathbf{E}_1 \bigwedge \mathbf{E}_2), \\
\vdots\quad & \\
\left(0\ 0\ 0 \cdots T^\top\right) &\quad (\because\ \mathbf{E}_1 \bigwedge \mathbf{E}_2).
\end{aligned}$$

Secondly, we prove the linear independence of every row vector in the matrix $\left(T^\top\ 0\ T^\top \cdots T^\top\right)$. Because of $\mathbf{E}_2 \bigwedge \mathbf{E}_4$, every row vector in $T^\top$ is linearly independent of $B^\top$. Hence, every row vector in the matrix is linearly independent of $\left(B^\top\ 0\ 0 \cdots 0\right)$, $\left(0\ 0\ B^\top \cdots 0\right)$, $\cdots$, $\left(0\ 0\ 0 \cdots B^\top\right)$. Every row vector in the matrix is also linearly independent of

$$\begin{array}{rl}
\big(0\ B^{\top}\ 0 \cdots 0\big) & (\because\ \mathbf{E}_2 \bigwedge \mathtt{rank}(B^{\top}) = k.), \\
\big(hI_{k+1}\ hI_{k+1}\ msg^*[\kappa_1]hI_{k+1} \cdots msg^*[\kappa_n]hI_{k+1}\big) & (\because\ \mathbf{E}_2), \\
\big(\boldsymbol{t}^{\top}\ 0\ \boldsymbol{t}^{\top} \cdots \boldsymbol{t}^{\top}\big) & (\because\ \mathbf{E}_5), \\
\big(0\ 0\ \boldsymbol{t}^{\top} \cdots 0\big) & (\because\ \mathbf{E}_1 \bigwedge \mathbf{E}_2), \\
\vdots & \\
\big(0\ 0\ 0 \cdots \boldsymbol{t}^{\top}\big) & (\because\ \mathbf{E}_1 \bigwedge \mathbf{E}_2), \\
\big(0\ 0\ T^{\top} \cdots 0\big) & (\because\ \mathbf{E}_2), \\
\vdots & \\
\big(0\ 0\ 0 \cdots T^{\top}\big) & (\because\ \mathbf{E}_2).
\end{array}$$

Analogously, we can prove the linear independence of every row vector which is in from the $\{(n+4)k+3\}$-th row to the $\{(2n+5)k+n+3\}$-th row in M.

Lastly, we prove the probability that at least one of $\{\mathbf{E}_1, \cdots, \mathbf{E}_5\}$ does not occur is negligibly small as follows. Since $\Pr[\neg\mathbf{E}_1] = 1/p^{k+1}$, $\Pr[\neg\mathbf{E}_2] \leq k/p^{k+1}$, $\Pr[\neg\mathbf{E}_3] = 1/p$, $\Pr[\neg\mathbf{E}_4] \leq k/p$ and $\Pr[\neg\mathbf{E}_5] \leq 1/(p-1)$ because of Corollary 1, $\Pr[\bigvee_{i=1}^{5} \neg\mathbf{E}_i] \leq \sum_{i=1}^{5} \Pr[\neg\mathbf{E}_i] \leq \frac{1}{p^{k+1}} + \frac{k}{p^{k+1}} + \frac{1}{p} + \frac{k}{p} + \frac{1}{p-1}$.

In conclusion, $|\Pr[1 \leftarrow \boldsymbol{Expt}_{b.0.j}(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}'_{b.0.j}(par)]| \leq (k+1)(\frac{1}{p} + \frac{1}{p^{k+1}}) + \frac{1}{p-1}$. □

Lemma 5. $\forall b \in \{0,1\}$, $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.0.q_e}(par)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.1.0}(par)\right]\right| = 0$.

Lemma 6. $\forall b \in \{0,1\}$, $\forall j \in [1, q'_e]$, $\exists \mathcal{B}_2 \in \mathsf{PPTA}_\lambda$, $|\Pr[1 \leftarrow \boldsymbol{Expt}'_{b.1.j-1}(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{b.1.j}(par)]| = \mathit{Adv}^{\mathcal{D}_k\text{-}\mathit{MDDH}}_{\mathcal{B}_2, \mathcal{G}_{BG}, \mathbb{G}_2}(\lambda)$.

Proof. $\mathcal{B}_2$ is a PPT algorithm attempting to break $\mathcal{D}_k$-MDDH assumption w.r.t. $\mathcal{G}_{BG}$ and $\mathbb{G}_2$ by using $\mathcal{A}$ as a subroutine. $\mathcal{B}_2$ behaves as described in Fig. 6. Obviously, if $\boldsymbol{v} = B\hat{\boldsymbol{w}}$ (resp. $\boldsymbol{v} = \hat{\boldsymbol{u}}$), $\mathcal{B}_2$ perfectly simulates $\boldsymbol{Expt}'_{b.1.j-1}$ (resp. $\boldsymbol{Expt}_{b.1.j}$) to $\mathcal{A}$, and if (and only if) $\mathcal{A}$ acts in a way letting the experiment return 1, $\mathcal{B}_2$ returns 1. Thus, $\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.1.j-1}(par)\right] = \Pr\left[1 \leftarrow \mathcal{B}_2\left(gd, [B]_2, [B\hat{\boldsymbol{w}}]_2\right)\right]$ (resp. $\Pr\left[1 \leftarrow \boldsymbol{Expt}_{b.1.j}(par)\right] = \Pr\left[1 \leftarrow \mathcal{B}_2\left(gd, [B]_2, [\hat{\boldsymbol{u}}]_2\right)\right]$) holds. □

Lemma 7. $\forall b \in \{0,1\}$, $\forall j \in [1, q'_e]$, $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_{b.1.j}(par)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{b.1.j}(par)\right]\right| \leq 1/p + 1/p^{k+1}$.

Proof. Let $\mathbf{E}_1$ denote the event where $\boldsymbol{t}^{\top} \leftsquigarrow \mathbb{Z}_p^{1\times(k+1)}$ is not the zero vector. Let $\mathbf{E}_2$ denote the event where $\boldsymbol{t}^{\top} \leftsquigarrow \mathbb{Z}_p^{1\times(k+1)}$ is not in the span of $B^{\top} \in \mathbb{Z}_p^{k\times(k+1)}$ (where $B \leftsquigarrow \mathcal{D}_k$). The proof proceeds under the assumption that both of the

```
$\mathcal{B}_2(gd, [B]_2, [\boldsymbol{v}]_2)$:   // $gd = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2) \leftarrow \mathcal{G}_{BG}(1^\lambda)$. $B \leftarrow\!\!\!\sim \mathcal{D}_k$.
                    // $\boldsymbol{v} = A\hat{\boldsymbol{w}}$ or $\hat{\boldsymbol{u}}$ (where $\hat{\boldsymbol{w}} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$, $\hat{\boldsymbol{u}} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$).
    $sk_{\mathrm{MAC}} := (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_l, x)$, where $\boldsymbol{x}_i \in \mathbb{Z}_p^{k+1}$ and $x \leftarrow\!\!\!\sim \mathbb{Z}_p$.
    $(msg^* \in \{0,1\}^l, st) \leftarrow \mathcal{A}_0^{\mathfrak{Eval}_0, \mathfrak{Eval}_1}(par)$:
-----------------------------------------------------------------------
    $-\mathfrak{Eval}_0(msg_\iota \in \{0,1\}^l, \mathbb{J}_\iota \subseteq \mathbb{I}_1(msg_\iota))$:
        $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $T \leftarrow\!\!\!\sim \mathbb{Z}_p^{(k+1)\times k}$. $u \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{w} \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$. For $i \in \mathbb{J}_\iota$: $d_i \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{e}_i \leftarrow\!\!\!\sim \mathbb{Z}_p^{1\times k}$.
        $\mathbf{Rtn}\ \tau := ([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2, \{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}_\iota\})$.
    $-\mathfrak{Eval}_1(msg_\theta \in \{0,1\}^l)$:
        If $\theta > j$: $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p^k$, $[\boldsymbol{t}]_2 := [B\boldsymbol{s}]_2$. $[u]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$.
        If $\theta < j$: $\boldsymbol{t} \leftarrow\!\!\!\sim \mathbb{Z}_p^{k+1}$, $u \leftarrow\!\!\!\sim \mathbb{Z}_p$.
        If $\theta = j$: $[\boldsymbol{t}]_2 := [\boldsymbol{v}]_2$. $[u]_2 := \left[(\boldsymbol{x}_0^\top + \sum_{i=1}^l msg_\theta[i]\boldsymbol{x}_i^\top)\boldsymbol{t} + x\right]_2$.
        $\mathbf{Rtn}\ \tau := ([\boldsymbol{t}]_2, [u]_2)$.
-----------------------------------------------------------------------
    $\mathbf{Abt}$ if $\bigvee_{\iota=1}^{q_e} msg_\iota \succeq_{\mathbb{J}_\iota} msg^* \bigvee_{\theta=1}^{q'_e} msg_\theta = msg^*$.
    $h \leftarrow\!\!\!\sim \mathbb{Z}_p$, $\boldsymbol{h}_0 := (\boldsymbol{x}_0 + \sum_{i=1}^l msg^*[i]\boldsymbol{x}_i)h$. If $b = 0$, $h_1 := xh$. If $b = 1$, $h_1 \leftarrow\!\!\!\sim \mathbb{Z}_p$.
    $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}_1(st, [h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$.
```

Fig. 6. Simulator $\mathcal{B}_2$ introduced to prove Lemma 6

events have occurred. Later we will prove that the probability that at least one of the two events does not occur is negligibly small, which implies that the assumption is reasonably valid.

Obviously, $\bigwedge_{\theta \in [1, q'_e]} msg_\theta \neq msg^*$ implies that $\exists \hat{i} \in [1, l]$ s.t. $msg_\theta[\hat{i}] \neq msg^*[\hat{i}]$. To make the proof simpler, we assume that the adversary $\mathcal{A}$ knows $x \in \mathbb{Z}_p$ and $\{\boldsymbol{x}_i \in \mathbb{Z}_p^{k+1} \mid i \in [1, l] \setminus \{\hat{i}\}\}$. Note that some information about $\boldsymbol{x}_0 \in \mathbb{Z}_p^{k+1}$ and $\boldsymbol{x}_{\hat{i}} \in \mathbb{Z}_p^{k+1}$ are leaked through the MAC $([\boldsymbol{t}]_2, [u]_2)$ on the $\theta'(> j)$-th query to $\mathfrak{Eval}_1$ in the form of $B^\top \boldsymbol{x}_0$ and $B^\top \boldsymbol{x}_{\hat{i}}$. Thus, $\mathcal{A}$ information-theoretically obtains the following information.

$$\begin{pmatrix} B^\top \boldsymbol{x}_0 \\ B^\top \boldsymbol{x}_{\hat{i}} \\ \boldsymbol{h}_0 \\ u - x \end{pmatrix} = \begin{pmatrix} B^\top & 0 \\ 0 & B^\top \\ msg^*[\kappa_1]hI_{k+1} & msg^*[\kappa_1]hI_{k+1} \\ \boldsymbol{t}^\top & msg_\theta[\hat{i}] \cdot \boldsymbol{t}^\top \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_0 \\ \boldsymbol{x}_{\hat{i}} \end{pmatrix}$$

Since we have assumed that $\mathbf{E}_1 \bigwedge \mathbf{E}_2$, the vector $\boldsymbol{t}^\top$ is linearly independent of $B^\top$. Thus, the row vector $\begin{pmatrix}\boldsymbol{t}^\top & msg_\theta[\hat{i}] \cdot \boldsymbol{t}^\top\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$ is linearly independent of both of $\begin{pmatrix}B^\top & 0\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$ and $\begin{pmatrix}0 & B^\top\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$. If $msg_\theta[\hat{i}] = 0 \bigwedge msg^*[\hat{i}] = 1$, because of $\mathbf{E}_1$, the row vector $\begin{pmatrix}\boldsymbol{t}^\top & 0\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$ is (linearly) independent of $\begin{pmatrix}msg^*[\kappa_1]hI_{k+1} & msg^*[\kappa_1]hI_{k+1}\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$. Likewise, if $msg_\theta[\hat{i}] = 1 \bigwedge msg^*[\hat{i}] = 1$, because of $\mathbf{E}_1$, $\begin{pmatrix}\boldsymbol{t}^\top & \boldsymbol{t}^\top\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$ is (linearly) independent of $\begin{pmatrix}msg^*[\kappa_1]hI_{k+1} & 0\end{pmatrix} \in \mathbb{Z}_p^{1\times\{2(k+1)\}}$.

Lastly, we prove the probability that at least one of $\mathbf{E}_1$ and $\mathbf{E}_2$ does not occur is negligibly small as follows. $\Pr[\neg\mathbf{E}_1 \bigvee \neg\mathbf{E}_2] \leq \Pr[\neg\mathbf{E}_1] + \Pr[\neg\mathbf{E}_2] = 1/p + 1/p^{k+1}$.

In conclusion, $\| \Pr[1 \leftarrow \boldsymbol{Expt}_{b.1.j}(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}'_{b.1.j}(par)]| \leq 1/p + 1/p^{k+1}$. □

Lemma 8. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}'_{0.1.q'_e}(par)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}'_{1.1.q'_e}(par)\right]\right| = 0.$

Proof. In $\boldsymbol{Expt}_{0.1.q'_e}$, $x \in \mathbb{Z}_p$ is used only once to compute $h_1 := xh \in \mathbb{Z}_p$. Hence, h_1 is uniformly at random in $\mathbb{Z}_p$ because of the uniform randomness of $x \leftarrow\!\!\!\!\sim \mathbb{Z}_p$. □

B.2 Proof of Theorem 2 (on the Security of DAMACtoDIBS)

The theorem consists of the following three thereoms, namely Theorem 8, Theorem 9 and Theorem 10.

Theorem 8. *$\Omega^{\text{DIBS}}_{\text{DAMAC}}$ is correct.*

Proof. If we say that a secret-key $sk^{\mathbb{J}}_{id} = ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \cup [l+1, l+m]\})$ w.r.t. $(id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l])$ is correct (under an honestly-generated (mpk, msk)) if it satisfies that

$$\begin{cases} \boldsymbol{t} \in \mathbb{Z}_p^n, \quad T \in \mathbb{Z}_p^{n \times n'}, \\ u = \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^{\top}\boldsymbol{t} + x, \quad \boldsymbol{u} = \sum_{i=0}^{l+m} f_i(id||1^m)Y_i^{\top}\boldsymbol{t} + \boldsymbol{y}^{\top}, \\ \boldsymbol{w} = \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^{\top}T, \quad W = \sum_{i=0}^{l+m} f_i(id||1^m)Y_i^{\top}T, \\ (\text{For } i \in \mathbb{J} \bigcup [l+1, l+m] :) \quad d_i = h_i(id||1^m)\boldsymbol{x}_i^{\top}\boldsymbol{t}, \quad \boldsymbol{d}_i = h_i(id||1^m)Y_i^{\top}\boldsymbol{t}, \\ \qquad \boldsymbol{e}_i = h_i(id||1^m)\boldsymbol{x}_i^{\top}T, \quad E_i = h_i(id||1^m)Y_i^{\top}T. \end{cases} \tag{2}$$

The theorem is proven by the following 5 lemmata. □

Lemma 9. *For any $\lambda, l, m \in \mathbb{N}$, any $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$, any $id \in \{0,1\}^l$, $sk^{\mathbb{I}_1(id)}_{id} \leftarrow \texttt{KGen}(msk, id)$ is correct.*

Proof. Obviously true from the definition of the KGen algorithm. □

Lemma 10. *Assume that $sk^{\mathbb{J}}_{id}$ w.r.t. $id \in \{0,1\}^l$ and $\mathbb{J} \subseteq \mathbb{I}_1(id)$ is correct. $(sk^{\mathbb{J}}_{id})' \leftarrow \texttt{KRnd}(sk^{\mathbb{J}}_{id}, id, \mathbb{J})$ is correct.*

Proof. We parse $sk^{\mathbb{J}}_{id}$ as $([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \cup [l+1, l+m]\})$. It satisfies (2).

We parse $(sk^{\mathbb{J}}_{id})'$ as $([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d'_i]_2, [\boldsymbol{d}'_i]_2, [\boldsymbol{e}'_i]_2, [E'_i]_2 \mid i \in \mathbb{J} \cup [l+1, l+m]\})$. It is generated as follows.

- $S' \leftarrow\!\!\!\!\sim \mathbb{Z}_p^{n' \times n'}$.
- $[T']_2 := [TS']_2$.
- $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^{\top}TS']_2$.
- $[W']_2 := [WS']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)Y_i^{\top}TS']_2$.

- $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$.
- $[\boldsymbol{t}']_2 \coloneqq [\boldsymbol{t} + T'\boldsymbol{s}']_2 = [\boldsymbol{t} + TS'\boldsymbol{s}']_2$.
- $[u']_2 \coloneqq [u + \boldsymbol{w}'\boldsymbol{s}']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top(\boldsymbol{t} + TS'\boldsymbol{s}') + x]_2$.
- $[\boldsymbol{u}']_2 \coloneqq [\boldsymbol{u} + W'\boldsymbol{s}']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)Y_i^\top(\boldsymbol{t} + TS'\boldsymbol{s}') + \boldsymbol{y}^\top]_2$.
- For $i \in \mathbb{J} \bigcup [l+1, l+m]$:
  - $[\boldsymbol{e}_i']_2 \coloneqq [\boldsymbol{e}_i S']_2 = [h_i(id||1^m)\boldsymbol{x}_i^\top TS']_2$.
  - $[E_i']_2 \coloneqq [E_i S']_2 = [h_i(id||1^m)Y_i^\top TS']_2$.
  - $[d_i']_2 \coloneqq [d_i + \boldsymbol{e}_i'\boldsymbol{s}']_2 = [h_i(id||1^m)\boldsymbol{x}_i^\top(\boldsymbol{t} + TS'\boldsymbol{s}')]_2$.
  - $[\boldsymbol{d}_i']_2 \coloneqq [\boldsymbol{d}_i + E_i'\boldsymbol{s}']_2 = [h_i(id||1^m)Y_i^\top(\boldsymbol{t} + TS'\boldsymbol{s}')]_2$.

It satisfies (2). Thus, it is correct. □

Lemma 11. *Assume that $sk_{id}^{\mathbb{J}}$ w.r.t. $id \in \{0,1\}^l$ and $\mathbb{J} \subseteq \mathbb{I}_1(id)$ is correct. For any $\mathbb{J}' \subseteq \mathbb{J}$, $sk_{id}^{\mathbb{J}'} \leftarrow \mathtt{Weaken}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, \mathbb{J}')$ is correct.*

Proof. The algorithm `Weaken` firstly re-randomizes $sk_{id}^{\mathbb{J}}$ to get $(sk_{id}^{\mathbb{J}})'$. Because of Lemma 10, $(sk_{id}^{\mathbb{J}})'$ satisfies (2). `Weaken` secondly generates $sk_{id}^{\mathbb{J}'}$ from $(sk_{id}^{\mathbb{J}})'$. It is obvious that if $(sk_{id}^{\mathbb{J}})'$ satisfies (2), then $sk_{id}^{\mathbb{J}'}$ also satisfies it. □

Lemma 12. *Assume that $sk_{id}^{\mathbb{J}}$ w.r.t. $id \in \{0,1\}^l$ and $\mathbb{J} \subseteq \mathbb{I}_1(id)$ is correct. For any $id' \preceq_{\mathbb{J}} id$, $sk_{id}^{\mathbb{J}\setminus\mathbb{I}_0(id')} \leftarrow \mathtt{Down}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, id')$ is correct.*

Proof. The algorithm `Down` firstly re-randomizes $sk_{id}^{\mathbb{J}}$ to get $(sk_{id}^{\mathbb{J}})'$. Because of Lemma 10, $(sk_{id}^{\mathbb{J}})'$ satisfies (2). `Down` secondly generates $sk_{id'}^{\mathbb{J}\setminus\mathbb{I}_0(id')}$ from $(sk_{id}^{\mathbb{J}})'$. It is obvious that if $(sk_{id}^{\mathbb{J}})'$ satisfies (2), then $sk_{id'}^{\mathbb{J}\setminus\mathbb{I}_0(id')}$ also satisfies it. □

Lemma 13. *Assume that $sk_{id}^{\mathbb{J}}$ w.r.t. $id \in \{0,1\}^l$ and $\mathbb{J} \subseteq \mathbb{I}_1(id)$ is correct. For any $msg \in \{0,1\}^m$, any $\sigma \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, msg)$, it holds that $1 \leftarrow \mathtt{Ver}(\sigma, id, msg)$.*

Proof. The algorithm `Sig` firstly re-randomizes $sk_{id}^{\mathbb{J}}$ to get $(sk_{id}^{\mathbb{J}})'$. Because of Lemma 10, $(sk_{id}^{\mathbb{J}})'$ satisfies (2). We parse $(sk_{id}^{\mathbb{J}})'$ as $([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d_i']_2, [\boldsymbol{d}_i']_2, [\boldsymbol{e}_i']_2, [E_i']_2 \mid i \in \mathbb{J} \cup [l+1, l+m]\})$. We generate a signature $\sigma \coloneqq ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$, where $[u'']_2 \coloneqq [u' - \sum_{i \in \mathbb{I}_0(1^l||msg)} d_i']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}' + x]_2$ and $[\boldsymbol{u}'']_2 \coloneqq [\boldsymbol{u}' - \sum_{i \in \mathbb{I}_0(1^l||msg)} \boldsymbol{d}_i']_2 = [\sum_{i=0}^{l+m} f_i(id||1^m)Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top]_2$.

`Ver` verifies the signature as follows.

`Ver` firstly choose $\boldsymbol{r} \leftsquigarrow \mathbb{Z}_p^k$. Then, `Ver` computes the following variables.

$$[\boldsymbol{v}_0]_1 \coloneqq [A\boldsymbol{r}]_1, \quad [v]_1 \coloneqq [\boldsymbol{z}\boldsymbol{r}]_1, \quad [\boldsymbol{v}_1]_1 \coloneqq \left[\sum_{i=0}^{l+m} f_i(id||msg) Z_i \boldsymbol{r}\right]_1.$$

`Ver` outputs 1 if the following condition holds.

$$e([v]_1, [1]_2) = e\left([\boldsymbol{v}_0]_1, \begin{bmatrix} \boldsymbol{u}'' \\ u'' \end{bmatrix}_2\right) \cdot e([\boldsymbol{v}_1]_1, [\boldsymbol{t}']_2)^{-1} \qquad (3)$$

The following three equations hold.

$$
\begin{aligned}
v &= \boldsymbol{z}\boldsymbol{r} = \boldsymbol{r}^\top \boldsymbol{z}^\top = \boldsymbol{r}^\top \left((\boldsymbol{y} \mid x)\, A \right)^\top = \boldsymbol{r}^\top A^\top (\boldsymbol{y} \mid x)^\top = \boldsymbol{r}^\top \left(\bar{A}^\top \mid \underline{A}^\top \right) \begin{pmatrix} \boldsymbol{y}^\top \\ x \end{pmatrix} \\
&= \boldsymbol{r}^\top \left(\bar{A}^\top \boldsymbol{y}^\top + \underline{A}^\top x \right) \qquad (4)
\end{aligned}
$$

$$
\boldsymbol{v}_0 \begin{pmatrix} \boldsymbol{u}'' \\ u'' \end{pmatrix} = \boldsymbol{r}^\top A^\top \begin{pmatrix} \boldsymbol{u}'' \\ u'' \end{pmatrix} = \boldsymbol{r}^\top \left(\bar{A}^\top \mid \underline{A}^\top \right) \begin{pmatrix} \boldsymbol{u}'' \\ u'' \end{pmatrix} = \boldsymbol{r}^\top \left(\bar{A}^\top \boldsymbol{u}'' + \underline{A}^\top u'' \right) \qquad (5)
$$

$$
\begin{aligned}
\boldsymbol{v}_1^\top \boldsymbol{t}' &= \left(\sum_{i=0}^{l+m} f_i(id||msg) Z_i \boldsymbol{r} \right)^\top \boldsymbol{t}' = \boldsymbol{r}^\top \sum_{i=0}^{l+m} f_i(id||msg) Z_i^\top \boldsymbol{t}' \\
&= \boldsymbol{r}^\top \sum_{i=0}^{l+m} f_i(id||msg) \left\{ (Y_i \mid \boldsymbol{x}_i)\, A \right\}^\top \boldsymbol{t}' \\
&= \boldsymbol{r}^\top \sum_{i=0}^{l+m} f_i(id||msg) \left(Y_i \bar{A} + \boldsymbol{x}_i \underline{A} \right)^\top \boldsymbol{t}' \\
&= \boldsymbol{r}^\top \sum_{i=0}^{l+m} f_i(id||msg) \left(\bar{A}^\top Y_i^\top + \underline{A}^\top \boldsymbol{x}_i^\top \right) \boldsymbol{t}' \\
&= \boldsymbol{r}^\top \left\{ \bar{A}^\top \left(\sum_{i=0}^{l+m} f_i(id||msg) Y_i^\top \boldsymbol{t}' \right) + \underline{A}^\top \left(\sum_{i=0}^{l+m} f_i(id||msg) \boldsymbol{x}_i^\top \boldsymbol{t}' \right) \right\} \\
&= \boldsymbol{r}^\top \left\{ \bar{A}^\top \left(\boldsymbol{u}'' - \boldsymbol{y}^\top \right) + \underline{A}^\top \left(u'' - x \right) \right\} \qquad (6)
\end{aligned}
$$

From (4), the left side of (3) is $\left[\boldsymbol{r}^\top \left(\bar{A}^\top \boldsymbol{y}^\top + \underline{A}^\top x \right) \right]_T$. From (5) and (6), the right side of (3) is

$$
\left[\boldsymbol{r}^\top \left(\bar{A}^\top \boldsymbol{u}'' + \underline{A}^\top u'' \right) - \boldsymbol{r}^\top \left\{ \bar{A}^\top \left(\boldsymbol{u}'' - \boldsymbol{y}^\top \right) + \underline{A}^\top \left(u'' - x \right) \right\} \right]_T = \left[\boldsymbol{r}^\top \left(\bar{A}^\top \boldsymbol{y}^\top + \underline{A}^\top x \right) \right]_T .
$$

Thus, the equation (3) holds. □

Theorem 9. *$\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ is $\texttt{EUF-CMA}$ if the $\mathcal{D}_k$-MDDH assumption on $\mathbb{G}_1$ holds (under Def. 2) and the underlying Σ_{DAMAC} is $\texttt{PR-CMA1}$ (under Def. 6). Formally, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B}_1, \mathcal{B}_2 \in \mathsf{PPTA}_\lambda$ s.t. $\boldsymbol{Adv}^{\texttt{EUF-CMA}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) \le \boldsymbol{Adv}^{\mathcal{D}_k\texttt{-MDDH}}_{\mathcal{B}_1,\mathcal{G}_{BG},\mathbb{G}_1}(\lambda) + \boldsymbol{Adv}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2}(\lambda) + 1/p$.*

Proof. For the proof, we introduce 7 experiments. Their formal definitions are described in Fig. 7. The first one $\boldsymbol{Expt}_0$ is identical to the standard experiment for the DIBS scheme, i.e., $\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A}}$. The other ones are associated with different types of rectangles, i.e., □, ▢, ⧈, ⬚, ⛶ and ▒. For every $i \in [1, 6]$, the experiment $\boldsymbol{Expt}_i$ is identical to the previous experiment $\boldsymbol{Expt}_{i-1}$ except for each command surrounded by the rectangle with whom the experiment $\boldsymbol{Expt}_i$ is associated. In $\boldsymbol{Expt}_i$, all such commands are recognized. On the other hand, in $\boldsymbol{Expt}_{i-1}$, they are ignored. We obtain $\mathtt{Adv}^{\texttt{EUF-CMA}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) = \Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)] \le \sum_{i=1}^{6} |\Pr[1 \leftarrow \boldsymbol{Expt}_{i-1}(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_i(1^\lambda, l, m)]| +$

$\Pr[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)]$, where the first transformation is simply because of the definition of $\boldsymbol{Expt}_0$, and the second transformation is because of the triangle inequality. By the inequality and seven lemmata given below with proofs, i.e., Lemmata 14-20, we conclude that for every $\mathcal{A} \in \mathsf{PPTA}_\lambda$, there exist $\mathcal{B}_1 \in \mathsf{PPTA}_\lambda$ and $\mathcal{B}_2 \in \mathsf{PPTA}_\lambda$ s.t. $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A}}(\lambda) \leq \mathtt{Adv}^{\mathcal{D}_k-\mathtt{MDDH}(\mathbb{G}_1)}_{\mathcal{B}_1}(\lambda) + \mathtt{Adv}^{\mathtt{PR\text{-}CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2}(\lambda) + 1/p$. □

Lemma 14. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right]\right| = 0$.

Proof. In $\boldsymbol{Expt}_0$, each element in a returned signature $\sigma = ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$ is described as follows: $\boldsymbol{t}' = \boldsymbol{t} + TS'\boldsymbol{s}' = B(\boldsymbol{s} + SS'\boldsymbol{s}')$, $u'' = \sum_{i=0}^{l+m} f_i(id||msg)\boldsymbol{x}_i^\top \boldsymbol{t}' + x$ and $\boldsymbol{u}'' = \sum_{i=0}^{l+m} f_i(id||msg)Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top$, where $\boldsymbol{s}, \boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$ and $S, S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$.

On the other hand, in $\boldsymbol{Expt}_1$, each element in a returned signature $\sigma = ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$ is described as follows: $\boldsymbol{t}' = B\boldsymbol{s}$, $u'' = \sum_{i=0}^{l+m} f_i(id||msg)\boldsymbol{x}_i^\top \boldsymbol{t}' + x$ and $\boldsymbol{u}'' = \sum_{i=0}^{l+m} f_i(id||msg)Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top$, where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p$.

Obviously, $\boldsymbol{t}'$ in $\boldsymbol{Expt}_0$ distributes identically to $B\hat{\boldsymbol{s}}$ for $\hat{\boldsymbol{s}} \leftsquigarrow \mathbb{Z}_p^{n'}$, because of the uniform randomness of $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$. Thus, $\boldsymbol{t}'$ in $\boldsymbol{Expt}_0$ distributes identically to $\boldsymbol{t}'$ in $\boldsymbol{Expt}_1$, which implies that the signature in $\boldsymbol{Expt}_0$ distribute identically to one in $\boldsymbol{Expt}_1$. □

Lemma 15. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right]\right| = 0$.

Proof. In $\boldsymbol{Expt}_1$, since $\boldsymbol{z} = (\boldsymbol{y}|x)A$ and $\boldsymbol{v}_0 = A\boldsymbol{r}$, we obtain $\boldsymbol{z}\boldsymbol{r} = \{(\boldsymbol{y}|x)A\}\boldsymbol{r} = (\boldsymbol{y}|x)\boldsymbol{v}_0$. Since, for every $i \in [0, l+m]$, $Z_i = (Y_i|\boldsymbol{x}_i)A$, and $\boldsymbol{v}_0 = A\boldsymbol{r}$, we obtain $\boldsymbol{v}_1 = (\sum_{i=0}^{l+m} f_i(id^*||msg^*)Z_i)\boldsymbol{r} = \{\sum_{i=0}^{l+m} f_i(id^*||msg^*)(Y_i|\boldsymbol{x}_i)A\}\boldsymbol{r} = \sum_{i=0}^{l+m} f_i(id^*||msg^*)(Y_i|\boldsymbol{x}_i)\boldsymbol{v}_0$. □

Lemma 16. *$\exists \mathcal{B}_1 \in \mathsf{PPTA}_\lambda$, $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right]\right| = \boldsymbol{Adv}^{\mathcal{D}_k-MDDH}_{\mathcal{B}_1,\mathcal{G}_{BG},\mathbb{G}_1}(\lambda)$.*

Proof. $\mathcal{B}_1$ is a PPT algorithm attempting to break $\mathcal{D}_k$-MDDH assumption w.r.t. $\mathcal{G}_{BG}$ and $\mathbb{G}_1$ by using $\mathcal{A}$ as a black-box. $\mathcal{B}_1$ behaves as follows.

```
$\mathcal{B}_1(gd = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2), [A]_1, [\boldsymbol{v}]_1)$:   $//gd \leftarrow \mathcal{G}_{BG}(1^\lambda)$. $A \leftsquigarrow \mathcal{D}_k$.
// $\boldsymbol{v} = A\boldsymbol{r}$ or $\boldsymbol{u}$ (where $\boldsymbol{r} \leftsquigarrow \mathbb{Z}_p^k$, $\boldsymbol{u} \leftsquigarrow \mathbb{Z}_p^{k+1}$).
  $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$.
  For $i \in [0, l+m]$, $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$ and $[Z_i]_1 := [(Y_i \mid \boldsymbol{x}_i)\, A]_2$.
  $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $[\boldsymbol{z}]_2 := [(\boldsymbol{y} \mid x)\, A]_1$. $mpk := ([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1)$.
  $msk := (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
  $(\sigma^*, id^* \in \{0,1\}^l, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
.............................................................................................
    $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id)), \mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      $\mathcal{B}$ correctly replies by using $msk$.
.............................................................................................
  Parse $\sigma^*$ as $([\boldsymbol{t}^*]_2, [u^*]_2, [\boldsymbol{u}^*]_2)$.
  $[\boldsymbol{v}_0]_1 := [\boldsymbol{v}]_1$. $[v]_1 := [(\boldsymbol{y} \mid x)\, \boldsymbol{v}_0]_1$. $[\boldsymbol{v}_1]_1 := \left[\sum_{i=0}^{l+m} f_i(id^*||msg^*)\,(Y_i \mid \boldsymbol{x}_i)\, \boldsymbol{v}_0\right]_1$.
```

```
$\boldsymbol{Expt}_0(1^\lambda, l, m)(:= \boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A}}(1^\lambda, l, m))$:      // $\boxed{\boldsymbol{Expt}_1}$, $\boxed{\boldsymbol{Expt}_2}$, $\boxed{\boxed{\boldsymbol{Expt}_3}}$, $\boxed{\boldsymbol{Expt}_4}$, $\boxed{\boldsymbol{Expt}_5}$,
                                                    // $\colorbox{lightgray}{$\boldsymbol{Expt}_6$}$.
  $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$.
  For $i \in [0, l+m]$: $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $Z_i := (Y_i \mid \boldsymbol{x}_i)\, A$. $\boxed{Z_i \leftsquigarrow \mathbb{Z}_p^{n \times k}.}$
  $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A$. $\boxed{\boldsymbol{z} \leftsquigarrow \mathbb{Z}_p^{1 \times k}.}$ $mpk := ([A]_1, \{[Z_i]_1 \mid i \in [0, l+m]\}, [\boldsymbol{z}]_1)$.
  $(\sigma^*, id^* \in \{0,1\}^l, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
  $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:
      $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
      $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $\boxed{\boldsymbol{u}^\top := \{\boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m) Z_i + \boldsymbol{z} - u\underline{A}\}\bar{A}^{-1}.}$
      $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $T := BS$. $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$.
      $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$. $\boxed{W := (\bar{A}^{-1})^\top \{\sum_{i=0}^{l+m} f_i(id||1^m) Z_i^\top T - \underline{A}^\top \boldsymbol{w}\}.}$
      For $i \in \mathbb{J} \bigcup [l+1, l+m]$:
          $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boxed{\boldsymbol{d}_i^\top := (h_i(id||1^m)\boldsymbol{t}^\top Z_i - d_i \underline{A})\bar{A}^{-1}.}$
          $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$. $\boxed{E_i := \bar{A}^{-1}(h_i(id||1^m) Z_i^\top T - \underline{A}^\top \boldsymbol{e}_i).}$
      $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$.
      $\mathbf{Rtn}$ $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup [l+1, l+m]\})$.
  $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
      $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$.
      $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $T := BS$. $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$
      For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$, $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
      $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$, $[W']_2 := [WS']_2$,
      $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$, $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
      For $i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}$:
          $[\boldsymbol{e}_i']_2 := [\boldsymbol{e}_i S']_2$, $[E_i']_2 := [E_i S']_2$, $[d_i']_2 := [d_i + \boldsymbol{e}_i'\boldsymbol{s}']_2$, $[\boldsymbol{d}_i']_2 := [\boldsymbol{d}_i + E_i'\boldsymbol{s}']_2$.
      $[u'']_2 := \left[u' - \sum_{i \in \mathbb{I}_0(1^l||msg)} d_i'\right]_2$. $[\boldsymbol{u}'']_2 := \left[\boldsymbol{u}' - \sum_{i \in \mathbb{I}_0(1^l||msg)} \boldsymbol{d}_i'\right]_2$.
      $\boxed{([\boldsymbol{t}']_2, [u'']_2, \perp) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||msg)\text{, where } \boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'},\ \boldsymbol{t}' := B\boldsymbol{s} \text{ and}}$
      $\boxed{\quad u'' := \sum_{i=0}^{l+m} f_i(id||msg)\boldsymbol{x}_i^\top \boldsymbol{t}' + x. \quad \boldsymbol{u}'' := \sum_{i=0}^{l+m} f_i(id||msg) Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top.}$
      $\boxed{(\boldsymbol{u}'')^\top := \{(\boldsymbol{t}')^\top \sum_{i=0}^{l+m} f_i(id||msg) Z_i + \boldsymbol{z} - u''\underline{A}\}\bar{A}^{-1}.}$
      $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \sigma)\}$. $\mathbf{Rtn}$ $\sigma := ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$.
  Parse $\sigma^*$ as $([\boldsymbol{t}^*]_2, [u^*]_2, [\boldsymbol{u}^*]_2)$.
  $\boldsymbol{r} \leftsquigarrow \mathbb{Z}_p^k$. $\boldsymbol{v}_0 := A\boldsymbol{r}$. $\boxed{\boxed{\boldsymbol{v}_0 \leftsquigarrow \mathbb{Z}_p^{k+1}.}}$ $\boxed{h \leftsquigarrow \mathbb{Z}_p,\ \bar{\boldsymbol{v}}_0 \leftsquigarrow \mathbb{Z}_p^k,\ \underline{\boldsymbol{v}}_0 := h + \underline{A}\bar{A}^{-1}\bar{\boldsymbol{v}}_0.}$
  $v := \boldsymbol{z}\boldsymbol{r}$. $\boxed{v := (\boldsymbol{y} \mid x)\, \boldsymbol{v}_0.}$ $\boxed{v := \boldsymbol{z}\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + xh.}$ $\colorbox{lightgray}{$v \leftsquigarrow \mathbb{Z}_p$}$.
  $\boldsymbol{v}_1 := (\sum_{i=0}^{l+m} f_i(id^*||msg^*) Z_i)\boldsymbol{r}$. $\boxed{\boldsymbol{v}_1 := \sum_{i=0}^{l+m} f_i(id^*||msg^*)\, (Y_i \mid \boldsymbol{x}_i)\, \boldsymbol{v}_0.}$
  $\boxed{\boldsymbol{v}_1 := \sum_{i=0}^{l+m} f_i(id^*||msg^*)(Z_i \bar{A}^{-1}\bar{\boldsymbol{v}}_0 + \boldsymbol{x}_i h).}$
  If $\left[\begin{array}{c} e\left([v]_1, [1]_2\right) = e\left([\boldsymbol{v}_0]_1, \begin{bmatrix} \boldsymbol{u}^* \\ u^* \end{bmatrix}_2\right) \cdot e\left([\boldsymbol{v}_1]_1, [\boldsymbol{t}^*]_2\right)^{-1} \\ \bigwedge_{(id,\mathbb{J}) \in \mathbb{Q}_r} id^* \not\preceq_{\mathbb{J}} id \quad \bigwedge_{(id,msg,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*) \end{array}\right]$, then $\mathbf{Rtn}$ 1.
  Else, then $\mathbf{Rtn}$ 0.
```

Fig. 7. Seven experiments introduced to prove `EUF-CMA` of $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$

If $\left[\begin{array}{c} e\left([v]_1, [1]_2\right) = e\left([\boldsymbol{v}_0]_1, \begin{bmatrix}\boldsymbol{u}^* \\ u^*\end{bmatrix}_2\right) \cdot e\left([\boldsymbol{v}_1]_1, [\boldsymbol{t}^*]_2\right)^{-1} \\ \bigwedge_{(id,\mathbb{J})\in\mathbb{Q}_r} id^* \not\preceq_{\mathbb{J}} id \quad \bigwedge_{(id,msg,\cdot)\in\mathbb{Q}_s} (id, msg) \neq (id^*, msg^*) \end{array}\right]$, **Rtn** 1.
Else, **Rtn** 0.

Obviously, if $\boldsymbol{v} = A\boldsymbol{r}$ (resp. $\boldsymbol{v} = \boldsymbol{u}$), $\mathcal{B}_1$ perfectly simulates $\boldsymbol{Expt}_2$ (resp. $\boldsymbol{Expt}_3$) to $\mathcal{A}$, and if (and only if) $\mathcal{A}$ makes the experiment return 1, $\mathcal{B}_1$ returns 1. Thus, $\Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right] = \Pr\left[1 \leftarrow \mathcal{B}_1\left(gd, [A]_1, [A\boldsymbol{r}]_1\right)\right]$ (resp. $\Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right] = \Pr\left[1 \leftarrow \mathcal{B}_1\left(gd, [A]_1, [\boldsymbol{u}]_1\right)\right]$) holds. □

Lemma 17. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, l, m)\right]\right| = 0.$

Proof. There are 8 variables surrounded by a dashed rectangle, i.e., 4 variables $\boldsymbol{u}$, W, $\boldsymbol{d}_i$ and E_i on $\mathfrak{Reveal}$, 1 variable $\boldsymbol{u}''$ on $\mathfrak{Sign}$, and 3 variables $\boldsymbol{v}_0$, v and $\boldsymbol{v}_1$. Each variable in $\boldsymbol{Expt}_4$ is information-theoretically equivalent to the one in $\boldsymbol{Expt}_3$. For the 6 variables other than $\boldsymbol{u}''$ and $\boldsymbol{v}_0$, it holds that

$$
\begin{aligned}
\boldsymbol{u}^\top &= \boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m) Y_i + \boldsymbol{y} \quad (\because\ \boldsymbol{u} = \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top) \\
&= \boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m)(Z_i - \boldsymbol{x}_i \underline{A})\bar{A}^{-1} + (\boldsymbol{z} - x\underline{A})\bar{A}^{-1} \quad (\because\ Z_i = Y_i\bar{A} + \boldsymbol{x}_i\underline{A},\ \boldsymbol{z} = \boldsymbol{y}\bar{A} + x\underline{A}) \\
&= \left[\boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m) Z_i + \boldsymbol{z} - \left\{\boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i + x\right\}\underline{A}\right]\bar{A}^{-1} \\
&= \left\{\boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||1^m) Z_i + \boldsymbol{z} - u\underline{A}\right\}\bar{A}^{-1} \quad (\because\ u = \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x), \\
W &= \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T = (\bar{A}^{-1})^\top \sum_{i=0}^{l+m} (id||1^m)(Z_i^\top - \underline{A}^\top \boldsymbol{x}_i^\top) T \quad (\because\ Z_i = Y_i\bar{A} + \boldsymbol{x}_i\underline{A}) \\
&= (\bar{A}^{-1})^\top \left(\sum_{i=0}^{l+m} (id||1^m) Z_i^\top T - \underline{A}^\top \boldsymbol{w}\right) \quad (\because\ \boldsymbol{w} = \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T), \\
\boldsymbol{d}_i^\top &= h_i(id||1^m)\boldsymbol{t}^\top Y_i \quad (\because\ \boldsymbol{d}_i = h_i(id||1^m) Y_i^\top \boldsymbol{t}) \\
&= h_i(id||1^m)\boldsymbol{t}^\top (Z_i - \boldsymbol{x}_i\underline{A})\bar{A}^{-1} = \left(h_i(id||1^m)\boldsymbol{t}^\top Z_i - d_i\underline{A}\right)\bar{A}^{-1} \quad (\because\ d_i = h_i(id||1^m)\boldsymbol{t}^\top \boldsymbol{x}_i), \\
E_i &= h_i(id||1^m) Y_i^\top T = h_i(id||1^m)(\bar{A}^{-1})^\top (Z_i^\top - \underline{A}^\top \boldsymbol{x}_i^\top) T \\
&= (\bar{A}^{-1})^\top \left(h_i(id||1^m) Z_i^\top T - \underline{A}^\top \boldsymbol{e}_i\right) \quad (\because\ \boldsymbol{e}_i = h_i(id||1^m)\boldsymbol{x}_i^\top T), \\
v &= (\boldsymbol{y}|x)\boldsymbol{v}_0 = \boldsymbol{y}\bar{\boldsymbol{v}}_0 + x\underline{\boldsymbol{v}}_0 = (\boldsymbol{z} - x\underline{A})\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + x(h + \underline{A}\bar{A}^{-1}\bar{\boldsymbol{v}}_0) \\
&\qquad\qquad\qquad\qquad (\because\ \boldsymbol{z} = \boldsymbol{y}\bar{A} + \boldsymbol{x}\underline{A},\ \underline{\boldsymbol{v}}_0 = h + \underline{A}\bar{A}^{-1}\bar{\boldsymbol{v}}_0) \\
&= \boldsymbol{z}\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + xh, \\
\boldsymbol{v}_1 &= \sum_{i=0}^{l+m} f_i(id^*||msg^*)(Y_i|\boldsymbol{x}_i)\boldsymbol{v}_0 = \sum_{i=0}^{l+m} f_i(id^*||msg^*)(Y_i\bar{\boldsymbol{v}}_0 + \boldsymbol{x}_i\underline{\boldsymbol{v}}_0)
\end{aligned}
$$

$$= \sum_{i=0}^{l+m} f_i(id^*||msg^*) \left\{(Z_i - \boldsymbol{x}_i\underline{A})\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + \boldsymbol{x}_i(h + \underline{A}\bar{A}^{-1}\bar{\boldsymbol{v}}_0)\right\} \quad (\because\ Z_i = Y_i\bar{A} + \boldsymbol{x}_i\underline{A})$$
$$= \sum_{i=0}^{l+m} f_i(id^*||msg^*)(Z_i\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + \boldsymbol{x}_i h).$$

Based on the same argument as $\boldsymbol{u}^{\mathsf{T}}$ on $\mathfrak{Reveal}$, $(\boldsymbol{u}'')^{\mathsf{T}}$ on $\mathfrak{Sign}$ is shown to be (information-theoretically) equivalent to the one in $\boldsymbol{Expt}_3$. Lastly, $\underline{\boldsymbol{v}}_0 \in \mathbb{Z}_p$ in $\boldsymbol{Expt}_4$ distributes uniformly at random in $\mathbb{Z}_p$, because of the uniform randomness of $h \leftsquigarrow \mathbb{Z}_p$, which implies that $\boldsymbol{v} \in \mathbb{Z}_p^{k+1}$ distributes uniformly at random in $\mathbb{Z}_p^{k+1}$ because of $\bar{\boldsymbol{v}}_0 \leftsquigarrow \mathbb{Z}_p^k$. □

Lemma 18. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m)\right]\right| = 0.$

Proof. The variables $(\{Z_i \mid i \in [0, l+m]\}, \boldsymbol{z})$ in $\boldsymbol{Expt}_4$ are described as $Z_i = (Y_i|\boldsymbol{x})A = Y_i\bar{A} + \boldsymbol{x}\underline{A}$ and $\boldsymbol{z} = (\boldsymbol{y}|x)A = \boldsymbol{y}\bar{A} + x\underline{A}$, respectively. We remind us that we have assumed (without loss of generality) that the square matrix composed of the first k rows of $A \in \mathbb{Z}_p^{(k+1)\times k}$, i.e., $\bar{A} \in \mathbb{Z}_p^{k\times k}$, has full rank k. Hence, $\boldsymbol{y}\bar{A}$ distributes uniformly at random in $\mathbb{Z}_p^{1\times k}$, because of the uniform randomness of $\boldsymbol{y} \in \mathbb{Z}_p^{1\times k}$, which implies that $\boldsymbol{z}$ in $\boldsymbol{Expt}_4$ distributes uniformly at random in $\mathbb{Z}_p^{1\times k}$. Likewise, $Y_i\bar{A} \in \mathbb{Z}_p^{n\times k}$ distributes uniformly at random in $\mathbb{Z}_p^{n\times k}$, because of the uniform randomness of $Y_i \in \mathbb{Z}_p^{n\times k}$, which implies that Z_i in $\boldsymbol{Expt}_4$ distributes uniformly at random in $\mathbb{Z}_p^{n\times k}$. □

Lemma 19. $\exists\mathcal{B}_2 \in \mathsf{PPTA}_\lambda$, $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)\right]\right| = \boldsymbol{Adv}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2}(\lambda)$.

Proof. Let $\mathcal{B}_2 = (\mathcal{B}_{2,0}, \mathcal{B}_{2,1})$ denote the PPT adversary in one of the two `PR-CMA1` experiments w.r.t. Σ_{DAMAC}, i.e., $\boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,b}$ for $b \in \{0,1\}$. $\mathcal{B}_2$ uses $\mathcal{A}$ as a black-box to break the `PR-CMA1`. $\mathcal{B}$ behaves as follows.

```
$\mathcal{B}_{2,0}^{\mathfrak{Eval}_0,\mathfrak{Eval}_1}(par)$:
  $A \leftsquigarrow \mathcal{D}_k$. For $i \in [0, l+m]$, $Z_i \leftsquigarrow \mathbb{Z}_p^{n\times k}$. $\boldsymbol{z} \leftsquigarrow \mathbb{Z}_p^{1\times k}$.
  $mpk := ([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1)$.
  $(\sigma^*, id^* \in \{0,1\}^l, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
................................................................................
    $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:
      $\mathbb{J}' := \mathbb{J} \bigcup [l+1, l+m]$
      $\tau = ([\boldsymbol{t}]_2, [u]_2, [T]_2, [\boldsymbol{w}]_2, \{[d_i]_2, [\boldsymbol{e}_i]_2 \mid i \in \mathbb{J}'\}) \leftarrow \mathfrak{Eval}_0(id||1^m, \mathbb{J}')$.
      $\left[\boldsymbol{u}^{\mathsf{T}}\right]_2 := \left[\{\boldsymbol{t}^{\mathsf{T}} \sum_{i=0}^{l+m} f_i(id||1^m)Z_i + \boldsymbol{z} - u\underline{A}\}\bar{A}^{-1}\right]_2$.
      $[W]_2 := \left[(\bar{A}^{-1})^{\mathsf{T}}\{\sum_{i=0}^{l+m} f_i(id||1^m)Z_i^{\mathsf{T}}T - \underline{A}^{\mathsf{T}}\boldsymbol{w}\}\right]_2$.
      For $i \in \mathbb{J}'$:
        $\left[\boldsymbol{d}_i^{\mathsf{T}}\right]_2 := \left[(h_i(id||1^m)\boldsymbol{t}^{\mathsf{T}}Z_i - d_i\underline{A})\bar{A}^{-1}\right]_2$.
        $[E_i]_2 := \left[\bar{A}^{-1}(h_i(id||1^m)Z_i^{\mathsf{T}}T - \underline{A}^{\mathsf{T}}\boldsymbol{e}_i)\right]_2$.
      $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$. $\mathbf{Rtn}$ $sk := \begin{pmatrix} [\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \\ \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}'\} \end{pmatrix}$.
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      $\tau = ([\boldsymbol{t}]_2, [u]_2) \leftarrow \mathfrak{Eval}_1(id||msg)$. $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \sigma)\}$.
      $[\boldsymbol{u}^\top]_2 := \left[\{\boldsymbol{t}^\top \sum_{i=0}^{l+m} f_i(id||msg) Z_i + \boldsymbol{z} - u\underline{A}\}\bar{A}^{-1}\right]_2$. $\mathbf{Rtn}$ $\sigma := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2)$.
......................................................................................................
  Let $st$ include all information $\mathcal{B}_{2,0}$ has acquired.
  If $F(id^*, msg^*) = 1$, $\mathbf{Rtn}$ $(id^*, msg^*, st)$.
  Else, arbitrarily choose $(id, msg)$ s.t. $F(id, msg) = 1$ and $\mathbf{Rtn}$ $(id, msg, st)$.
$\mathcal{B}_{2,1}(st, [h]_1, [\boldsymbol{h}_0]_1, [h_1]_1)$:
  If $F(id^*, msg^*) = 1$, do:
    Parse $\sigma^*$ as $([\boldsymbol{t}^*]_2, [u^*]_2, [\boldsymbol{u}^*]_2)$. $\bar{\boldsymbol{v}}_0 \leftsquigarrow \mathbb{Z}_p^k$, $[\underline{\boldsymbol{v}}_0]_1 := \left[h + \underline{A}\bar{A}^{-1}\bar{\boldsymbol{v}}_0\right]_1$.
    $[v]_1 := \left[\boldsymbol{z}\bar{A}^{-1}\bar{\boldsymbol{v}}_0 + h_1\right]_1$. $[\boldsymbol{v}_1]_1 := \left[\sum_{i=0}^{l+m} f_i(id^*||msg^*) Z_i \bar{A}^{-1}\bar{\boldsymbol{v}}_0 + \boldsymbol{h}_0\right]_1$.
    If $e([v]_1, [1]_2) = e\left([\boldsymbol{v}_0]_1, \begin{bmatrix}\boldsymbol{u}^* \\ u^*\end{bmatrix}_2\right) \cdot e([\boldsymbol{v}_1]_1, [\boldsymbol{t}^*]_2)^{-1}$, $\mathbf{Rtn}$ 1. Else, $\mathbf{Rtn}$ 0.
  Else, $\mathbf{Rtn}$ 1.
```

If the experiment that $\mathcal{B}_2$ (unconsciously) plays is $\boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,0}$, the variables $h \in \mathbb{Z}_p$, $\boldsymbol{h}_0 \in \mathbb{Z}_p^n$ and $h_1 \in \mathbb{Z}_p$ are generated by $h \leftsquigarrow \mathbb{Z}_p$, $\boldsymbol{h}_0 := \sum_{i=0}^{l+m} f_i(id^*||msg^*)\boldsymbol{x}_i h$ and $h_1 := xh$. In this case, $\mathcal{B}_2$ perfectly simulates $\boldsymbol{Expt}_5$ to $\mathcal{A}$. We obtain $\Pr[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m)] = \Pr[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m) \bigwedge F(id^*, msg^*) = 1] + \Pr[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m) \bigwedge F(id^*, msg^*) = 0] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,0}(par)] + 1$.

On the other hand, if the experiment that $\mathcal{B}_2$ plays is $\boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,1}(par)$, the variable h_1 is randomly chosen, i.e., $h_1 \leftsquigarrow \mathbb{Z}_p$. In this case, $\mathcal{B}_2$ perfectly simulates $\boldsymbol{Expt}_6$ to $\mathcal{A}$. We obtain $\Pr[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)] = \Pr[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m) \bigwedge F(id^*, msg^*) = 1] + \Pr[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m) \bigwedge F(id^*, msg^*) = 0] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,1}(par)] + 1$.

Hence, we obtain $|\Pr[1 \leftarrow \boldsymbol{Expt}_5(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)]| = |\Pr[1 \leftarrow \boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,0}(par)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2,1}(par)]| = \mathtt{Adv}^{\texttt{PR-CMA1}}_{\Sigma_{\mathrm{DAMAC}},\mathcal{B}_2}(\lambda)$. □

Lemma 20. $\Pr\left[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)\right] \leq 1/p$.

Proof. In $\boldsymbol{Expt}_6$, $v \in \mathbb{Z}_p$ is chosen uniformly at random from $\mathbb{Z}_p$, which implies that it holds that $e([v]_1, [1]_2) = e\left([\boldsymbol{v}_0]_1, \begin{bmatrix}\boldsymbol{u}^* \\ u^*\end{bmatrix}_2\right) \cdot e([\boldsymbol{v}_1]_1, [\boldsymbol{t}^*]_2)^{-1}$ with probability $1/p$ at most. The condition is satisfied when the experiment returns 1. Thus, $\Pr\left[1 \leftarrow \boldsymbol{Expt}_6(1^\lambda, l, m)\right] \leq 1/p$. □

Theorem 10. $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$ *is statistically signer-private. Formally, for every probabilistic adversary* $\mathcal{A}$*, there exist four polynomial-time algorithms* $\Omega^{\mathrm{DIBS}'}_{\mathrm{DAMAC}} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$ *s.t.* $\boldsymbol{Adv}^{SP}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \Omega^{\mathrm{DIBS}'}_{\mathrm{DAMAC}}, \mathcal{A}, l, m}(\lambda) \leq \frac{q_r + q_{dd} + q_d + q_s}{p-1}$.

Proof. Four experiments introduced to prove the theorem are formally described in Fig. 9. The first one $\boldsymbol{Expt}_0$ is identical to the standard real-world experiment parameterized by 0 for $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$, namely $\boldsymbol{Expt}^{\mathsf{SP}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A},0}$. The other ones are associated with different types of rectangles, i.e., □, ⬚ and ■. Each one of them is identical to the previous one except for the commands surrounded by the associated rectangle.

We define five polynomial-time simulation algorithms $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}'} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$ as follows. The setup algorithm $\mathtt{Setup}'$ is completely the same as the original one, i.e., $\mathtt{Setup}$. $\mathtt{KGen}'$ is the same as $\mathtt{KGen}$ except that it aborts if the randomly-chosen square matrix $S \in \mathbb{Z}_p^{n' \times n'}$ does not have the full rank. $\mathtt{Weaken}'$ (resp. $\mathtt{Down}'$) is the same as $\mathtt{Weaken}$ (resp. $\mathtt{Down}$) except that it aborts if the randomly-chosen square matrix $S' \in \mathbb{Z}_p^{n' \times n'}$ does not have the full rank. $\mathtt{Sig}'$ generates a signature on msg for id directly from msk. They are formally described in Fig. 8.

We obtain $\mathtt{Adv}^{\mathsf{SP}}_{\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}, \Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}'}, \mathcal{A}, l, m}(\lambda) = |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}, \mathcal{A}, 1}(1^\lambda, l, m)]| \leq \sum_{i=1}^{3} |\Pr[1 \leftarrow \boldsymbol{Expt}_{i-1}(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_i(1^\lambda, l, m)]| + |\Pr[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}, \mathcal{A}, 1}(1^\lambda, l, m)]|$, where the first transformation is because of the definition of $\boldsymbol{Expt}_0$, and the second transformation is because of the triangle inequality. Based on the inequality and five lemmata given below with proofs[10], i.e., Lemmata 21-23, we conclude that for every probabilistic algorithm $\mathcal{A}$, there exist probabilistic polynomial time algorithms $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}'} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$ such that $\mathtt{Adv}^{\mathsf{SP}}_{\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}, \Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}'}, \mathcal{A}, l, m}(\lambda) \leq \frac{q_r + q_{dd} + q_d + q_s}{p-1}$. □

Lemma 21. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right]\right| = 0.$

Proof. In $\boldsymbol{Expt}_0$, each element in a returned signature $\sigma = ([\boldsymbol{t}'']_2, [u''']_2, [\boldsymbol{u}''']_2)$ is described as follows: $\boldsymbol{t}'' = \boldsymbol{t} + T'\boldsymbol{s}' + T''\boldsymbol{s}'' = \boldsymbol{t} + TS'\boldsymbol{s}' + TS'S''\boldsymbol{s}'' = B(\boldsymbol{s} + SS'\boldsymbol{s}' + SS'S''\boldsymbol{s}'')$, $u''' = \sum_{i=0}^{l+m} f_i(id'||msg)\boldsymbol{x}_i^\top \boldsymbol{t}'' + x$ and $\boldsymbol{u}''' = \sum_{i=0}^{l+m} f_i(id'||msg) Y_i^\top \boldsymbol{t}'' + \boldsymbol{y}^\top$.

On the other hand, in $\boldsymbol{Expt}_1$, each element in a returned signature $\sigma = ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$ is described as follows: $\boldsymbol{t}' = \boldsymbol{t} + T'\boldsymbol{s}' = B(\boldsymbol{s} + SS'\boldsymbol{s}')$, $u'' = \sum_{i=0}^{l+m} f_i(id'||msg)\boldsymbol{x}_i^\top \boldsymbol{t}' + x$ and $\boldsymbol{u}'' = \sum_{i=0}^{l+m} f_i(id'||msg) Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top$.

Thus, $\boldsymbol{t}'$ in $\boldsymbol{Expt}_0$ distributes identically to $\boldsymbol{t}'$ in $\boldsymbol{Expt}_1$, since either of them distributes identically to $B(\boldsymbol{s} + SS'\boldsymbol{s}')$, where $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$ and $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$. □

Lemma 22. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right]\right| \leq \frac{q_r + q_{dd} + q_d + q_s}{p-1}.$

Proof. To prove the lemma, we reuse Corollary 1 which was introduced to prove Lemma 4 in Subsect. 3.3. Obviously, both $\boldsymbol{Expt}_1$ and $\boldsymbol{Expt}_2$ are completely the same except for the case where $\boldsymbol{Expt}_2$ aborts, namely Abt, which implies that it holds that $|\Pr[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)]| \leq \Pr[\mathbf{Abt}]$.

In $\boldsymbol{Expt}_2$, at each query to $\mathfrak{Reveal}$, $\mathfrak{Weaken}$, $\mathfrak{Down}$ or $\mathfrak{Sign}$, the event where the experiment aborts can *independently* occur. For $i \in [1, q_r]$ (resp. $i \in [1, q_{dd}]$, $i \in [1, q_d]$, $i \in [1, q_s]$), let $AbtR_i$ (resp. $AbtDD_i$, $AbtD_i$, $AbtS_i$) denote the event where, at i-th query to $\mathfrak{Reveal}$ (resp. $\mathfrak{Weaken}$, $\mathfrak{Down}$, $\mathfrak{Sign}$), the experiment

[10] Lemma 24 is obviously true. We omit its proof.

```
$\texttt{Setup}'(1^\lambda, l, m)$:
  $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} \leftarrow \texttt{Gen}_{\mathrm{MAC}}(1^\lambda, l+m)$.
  Parse $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x)$.
    // $B \in \mathbb{Z}_p^{n \times n'}$, $\boldsymbol{x}_i \in \mathbb{Z}_p^n$, $x \in \mathbb{Z}_p$.
  For $i \in [0, l+m]$:
    $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $Z_i := (Y_i \mid \boldsymbol{x}_i)\, A \in \mathbb{Z}_p^{n \times k}$.
  $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A \in \mathbb{Z}_p^{1 \times k}$.
  $mpk := \left([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1\right)$.
  $msk := \left(sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y}\right)$.
  $\mathbf{Rtn}$ $(mpk, msk)$.

$\texttt{KGen}'(msk, id \in \{0,1\}^l)$:
  $\tau \leftarrow \texttt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$.
  Parse $\tau = ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
    // $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^n$.
    // $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
    // $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x \in \mathbb{Z}_p$.
  $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top \in \mathbb{Z}_p^k$.
  $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $T := BS \in \mathbb{Z}_p^{n \times n'}$.
  $\mathbf{Abt}$ if $\texttt{rank}(S) \neq n'$.
  $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T \in \mathbb{Z}_p^{1 \times n'}$.
  $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T \in \mathbb{Z}_p^{k \times n'}$.
  For $i \in \mathbb{I}_1(id||1^m)$:
    $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$,
    $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$,
    $E_i := h_i(id||1^m) Y_i^\top T$.
  $\mathbf{Rtn}$ $sk_{id}^{\mathbb{I}_1(id)} :=$
   $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2,$
   $\big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{I}_1(id||1^m)\big\}\big)$.

$\texttt{Sig}'(msk, id, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m)$:
  $\tau \leftarrow \texttt{Tag}(sk_{\mathrm{MAC}}, id||msg)$.
  Parse $\tau$ as $([\boldsymbol{t}]_2, [u']_2, \perp)$.
    // $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^n$.
    // $u' := \sum_{i=0}^{l+m} f_i(id||msg)\boldsymbol{x}_i^\top \boldsymbol{t} + x \in \mathbb{Z}_p$.
  $\boldsymbol{u}' := \sum_{i=0}^{l+m} f_i(id||msg) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top \in \mathbb{Z}_p^k$.
  $\mathbf{Rtn}$ $\sigma := \big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2\big)$.
```

```
$\texttt{Weaken}'(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id))$:
  $\mathbf{Rtn}$ $\perp$ if $\mathbb{J}' \not\subseteq \mathbb{J}$. $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{KRnd}(sk_{id}^{\mathbb{J}}, id, \mathbb{J})$.
  Parse $(sk_{id}^{\mathbb{J}})'$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2,$
    $[W]_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\mathbf{Rtn}$ $sk_{id}^{\mathbb{J}'} := \big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2,$
    $\big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{J}' \bigcup \mathbb{K}\big\}\big)$.

$\texttt{Down}'(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), id' \in \{0,1\}^l)$:
  $\mathbf{Rtn}$ $\perp$ if $id' \not\preceq_{\mathbb{J}} id$. $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{KRnd}(sk_{id}^{\mathbb{J}}, id, \mathbb{J})$.
  Parse $(sk_{id}^{\mathbb{J}})'$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2,$
    $\big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$. $\mathbb{I}^* := \mathbb{I}_1(id) \bigcap \mathbb{I}_0(id')$.
  $[u']_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$.
  $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
  $[\boldsymbol{w}']_2 := \left[\boldsymbol{w} - \sum_{i \in \mathbb{I}^*} \boldsymbol{e}_i\right]_2$.
  $[W']_2 := \left[W - \sum_{i \in \mathbb{I}^*} E_i\right]_2$.
  $\mathbf{Rtn}$ $sk_{id'}^{\mathbb{J}'} := \big([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2, [T]_2, [\boldsymbol{w}']_2,$
    $[W']_2, \big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{J}' \bigcup \mathbb{K}\big\}\big)$.

$\texttt{KRnd}'(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:
  Parse $sk_{id}^{\mathbb{J}}$ as $\big([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2,$
    $\big\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \bigm| i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
  $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\mathbf{Abt}$ if $\texttt{rank}(S') \neq n'$.
  $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$,
  $[W']_2 := [WS']_2$, $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$,
  $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
  For $i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}$:
    $[\boldsymbol{e}_i']_2 := [\boldsymbol{e}_i S']_2$, $[E_i']_2 := [E_i S']_2$,
    $[d_i']_2 := [d_i + \boldsymbol{e}_i'\boldsymbol{s}']_2$, $[\boldsymbol{d}_i']_2 := [\boldsymbol{d}_i + E_i'\boldsymbol{s}']_2$.
  $\mathbf{Rtn}$ $(sk_{id}^{\mathbb{J}})' := \big([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2,$
    $[W']_2, \big\{[d_i']_2, [\boldsymbol{d}_i']_2, [\boldsymbol{e}_i']_2, [E_i']_2 \bigm| i \in \mathbb{J} \bigcup \mathbb{K}\big\}\big)$.
```

Fig. 8. Five polynomial-time simulation algorithms $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}'}$ with $\{\texttt{Setup}', \texttt{KGen}', \texttt{Weaken}', \texttt{Down}', \texttt{Sig}'\}$ (and a sub-routine $\texttt{KRnd}'$) based on a DAMAC $\Sigma_{\mathrm{DAMAC}} = \{\texttt{Gen}_{\mathrm{MAC}}, \texttt{Tag}, \texttt{Weaken}, \texttt{Down}, \texttt{Ver}\}$. Each algorithm differs from each algorithm of the original $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBS}}$ in Fig. 1 in the commands with gray background. Note that $\mathbb{K}$ denotes a set $[l+1, l+m]$ of successive integers.

```
$\boldsymbol{Expt}_0(1^\lambda, l, m)(:= \boldsymbol{Expt}^{\mathsf{SP}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, 0}(1^\lambda, l, m))$:     // $\boxed{\boldsymbol{Expt}_1}$, $\boldsymbol{Expt}_2$, $\boldsymbol{Expt}_3$.
    $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$.
    For $i \in [0, l+m]$: $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $\mathtt{Z}_i := (Y_i \mid \boldsymbol{x}_i)\, A$.
    $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A$.
    $mpk := ([A]_1, \{[Z_i]_1 \mid i \in [0, l+m]\}, [\boldsymbol{z}]_1)$. $msk := (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
    $\mathbf{Rtn}\ b \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Down}, \mathfrak{Sign}}(mpk, msk)$, where
    -$\mathfrak{Reveal}(id)$:
        $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $T := BS$. $\mathbf{Abt}$ if $\mathtt{rank}(S) \neq n'$.
        $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$.
        For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
        $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}\ sk$.
    -$\mathfrak{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$:
        $\mathbf{Rtn}\ \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        Parse $sk$ as $([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        Re-randomize $sk$ for $(id, \mathbb{J})$ to obtain $sk'$ as follows.
            - $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\mathbf{Abt}$ if $\mathtt{rank}(S') \neq n'$.
            - $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$, $[W']_2 := [WS']_2$,
            - $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$, $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
            - For $i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}$:
                $[\boldsymbol{e}'_i]_2 := [\boldsymbol{e}_i S']_2$, $[E'_i]_2 := [E_i S']_2$, $[d'_i]_2 := [d_i + \boldsymbol{e}'_i \boldsymbol{s}']_2$, $[\boldsymbol{d}'_i]_2 := [\boldsymbol{d}_i + E'_i \boldsymbol{s}']_2$.
            - $sk' := ([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d'_i]_2, [\boldsymbol{d}'_i]_2, [\boldsymbol{e}'_i]_2, [E'_i]_2 \mid i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        $sk'' := ([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d'_i]_2, [\boldsymbol{d}'_i]_2, [\boldsymbol{e}'_i]_2, [E'_i]_2 \mid i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id, \mathbb{J}')\}$. $\mathbf{Rtn}\ sk''$.
    -$\mathfrak{Down}(sk, id, \mathbb{J}, id')$:
        $\mathbf{Rtn}\ \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
        In the same manner as $\mathfrak{Weaken}$, parse $sk$, re-randomize $sk$ to obtain $sk'$, and parse $sk'$.
        $[u'']_2 := [u' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id'||1^m)} d'_i]_2$. $[\boldsymbol{u}'']_2 := [\boldsymbol{u}' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id'||1^m)} \boldsymbol{d}'_i]_2$.
        $sk'' := ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d'_i]_2, [\boldsymbol{d}'_i]_2, [\boldsymbol{e}'_i]_2, [E'_i]_2 \mid i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id', \mathbb{J}'\}$. $\mathbf{Rtn}\ sk''$.
    -$\mathfrak{Sign}(sk, id, \mathbb{J}, id', msg \in \{0, 1\}^m)$:
        $\mathbf{Rtn}\ \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        $sk' \leftarrow \mathtt{Down}(sk, id, \mathbb{J}, id')$. $\sigma \leftarrow \mathtt{Sig}(sk', id', \mathbb{J} \setminus \mathbb{I}_0(id'), msg)$.
        In the same manner as $\mathfrak{Weaken}$, parse $sk$, re-randomize $sk$ to obtain $sk'$, and parse $sk'$.
        $[u'']_2 := [u' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id'||msg)} d'_i]_2$. $[\boldsymbol{u}'']_2 := [\boldsymbol{u}' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id'||msg)} \boldsymbol{d}'_i]_2$.
        $\sigma := ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2)$.
        $([\boldsymbol{t}]_2, [u]_2, \perp) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id'||msg)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id'||msg)\boldsymbol{x}_i^\top \boldsymbol{t} + x$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id'||msg) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $\sigma := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2)$.
        $\mathbf{Rtn}\ \sigma$.
```

Fig. 9. Four experiments introduced to prove the statistical signer-privacy of $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$

aborts. Based on the fact that every event is independent from all of the other events and Corollary 1, we obtain

$$\begin{aligned}\Pr[Abt] &= \Pr[\bigvee_{i=1}^{q_r} AbtR_i \bigvee_{i=1}^{q_{dd}} AbtDD_i \bigvee_{i=1}^{q_d} AbtD_i \bigvee_{i=1}^{q_s} AbtS_i] \\ &= \sum_{i=1}^{q_r} \Pr[AbtR_i] + \sum_{i=1}^{q_{dd}} \Pr[AbtDD_i] + \sum_{i=1}^{q_d} \Pr[AbtD_i] + \sum_{i=1}^{q_s} \Pr[AbtS_i] \\ &= \sum_{i=1}^{q_r+q_{dd}+q_d+q_s} \Pr[\mathtt{rank}(S) \neq n' \mid S \leftarrow\!\!\!\sim \mathbb{Z}_p^{n' \times n'}] \leq \frac{q_r + q_{dd} + q_d + q_s}{p-1}.\end{aligned}$$

□

Lemma 23. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right]\right| = 0.$

Proof. In $\boldsymbol{Expt}_2$, each element in a returned signature $\sigma = ([\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2$ is described as follows: $\boldsymbol{t}' = \boldsymbol{t}+TS'\boldsymbol{s}' = B(\boldsymbol{s}+SS'\boldsymbol{s}')$, $u' = \sum_{i=0}^{l+m} f_i(id'||msg)\boldsymbol{x}_i^\top \boldsymbol{t}' + x$ and $\boldsymbol{u}'' = \sum_{i=0}^{l+m} f_i(id'||msg)Y_i^\top \boldsymbol{t}' + \boldsymbol{y}^\top$, where $\boldsymbol{s}' \leftarrow\!\!\!\sim \mathbb{Z}_p^{n'}$ and $S' \leftarrow\!\!\!\sim \mathbb{Z}_p^{n' \times n'}$.

On the other hand, in $\boldsymbol{Expt}_3$, each element in a returned signature $\sigma = ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2)$ is described as follows: $\boldsymbol{t} = B\boldsymbol{s}$, $u = \sum_{i=0}^{l+m} f_i(id'||msg)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $\boldsymbol{u} = \sum_{i=0}^{l+m} f_i(id'||msg)Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$, where $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p$.

In $\boldsymbol{Expt}_2$, since both S and S' are square matrices with full rank n', their multiplication SS' is also a square matrix with full rank n'. Hence, the vector $SS'\boldsymbol{s}'$ (or $\boldsymbol{s} + SS'\boldsymbol{s}'$) distributes uniformly at random in $\mathbb{Z}_p^{n'}$, because of the uniform randomness of $\boldsymbol{s}' \leftarrow\!\!\!\sim \mathbb{Z}_p^{n'}$. The uniform randomness of $SS'\boldsymbol{s}'$ implies that the vector $\boldsymbol{t}'$ in $\boldsymbol{Expt}_2$ has a distribution identical to the one of $\boldsymbol{t}$ in $\boldsymbol{Expt}_3$, i.e., $B\boldsymbol{s}$, where $\boldsymbol{s} \leftarrow\!\!\!\sim \mathbb{Z}_p^{n'}$. □

Lemma 24. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}^{\boldsymbol{SP}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, 1}(1^\lambda, l, m)\right]\right| = 0.$

B.3 Proof of Theorem 3 (on Security of DIBS$\mathtt{to}$WWkIBS1)

The theorem consists of the following two theorems.

Theorem 11. DIBS$\boldsymbol{\mathtt{to}}$WWkIBS1 *is* $\boldsymbol{\mathtt{EUF\text{-}CMA}}$ *(under Def. 3) if the underlying DIBS scheme is* $\boldsymbol{\mathtt{EUF\text{-}CMA}}$ *(under Def. 7). Formally,* $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$, $\boldsymbol{\mathtt{Adv}}^{\boldsymbol{\mathtt{EUF\text{-}CMA}}}_{\Sigma_{\mathrm{WWkIBS}}, \mathcal{A}, l, m, n}(\lambda) = \boldsymbol{\mathtt{Adv}}^{\boldsymbol{\mathtt{EUF\text{-}CMA}}}_{\Sigma_{\mathrm{DIBS}}, \mathcal{B}, 2ln, m}(\lambda)$.

Proof. The simulator $\mathcal{B}$ behaves as shown in Fig. 10. It is obvious that $\mathcal{B}$ perfectly simulates $\boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\mathrm{WWkIBS}}, \mathcal{A}, l, m, n}$ to $\mathcal{A}$. It is also obvious that iff $\mathcal{A}$ outputs σ^*, wid^* and msg^* s.t. $1 \leftarrow \mathrm{WWkIBS}.\mathtt{Ver}(\sigma^*, wid^*, msg^*) \bigwedge_{id \in \mathbb{Q}_r} 0 \leftarrow \mathcal{R}_{wwk}(id, wid^*) \bigwedge_{(wid, msg, \cdot) \in \mathbb{Q}_s} (wid, msg) \neq (wid^*, msg^*)$, $\mathcal{B}$ outputs σ^*, $dwid^*$ and msg^* s.t. $1 \leftarrow \mathrm{DIBS}.\mathtt{Ver}(\sigma^*, dwid^*, msg^*)$
$\bigwedge_{(did, \mathbb{I}_1(did)) \in \mathbb{Q}_r'} dwid^* \not\preceq_{\mathbb{I}_1(did)} did \bigwedge_{(dwid, msg, \cdot) \in \mathbb{Q}_s} (dwid, msg) \neq (dwid^*, msg^*)$. Hence, $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\mathrm{WWkIBS}}, \mathcal{A}, l, m, n} = \mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\mathrm{DIBS}}, \mathcal{B}, 2ln, m}$. □

```
$\mathcal{B}^{\mathfrak{Reveal}',\mathfrak{Sign}'}(mpk)$:   // $(mpk, msk) \leftarrow$ DIBS.Setup$(1^\lambda, 2ln, m)$.
                           // $sk_{1^{2ln}}^{[1,2ln])} \leftarrow$ DIBS.KGen$(msk, 1^{2ln})$.
    $(\sigma^*, wid^* \in \mathcal{I}_{wwkibs}^{l,n}, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
    $-\mathfrak{Reveal}(id \in \mathcal{I}_{wk})$: $did \leftarrow \phi_{wk}(id)$.
        $sk \leftarrow \mathfrak{Reveal}'(did, \mathbb{I}_1(did))$. // $sk \leftarrow$ DIBS.Down$(sk_{1^{2ln}}^{[1,2ln]}, 1^{2ln}, [1, 2ln], did)$.
        $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{id\}$. **Rtn** $sk$.
    $-\mathfrak{Sign}(id \in \mathcal{I}_{wk}, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
        $dwid \leftarrow \phi_{wwk}(wid)$. $\sigma \leftarrow \mathfrak{Sign}'(dwid, msg)$.
          // $sk \leftarrow$ DIBS.Down$(sk_{1^{2ln}}^{[1,2ln]}, 1^{2ln}, [1, 2ln], dwid)$.
          // $\sigma \leftarrow$ DIBS.Sig$(sk, dwid, \mathbb{I}_1(dwid), msg)$.
        $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(wid, msg, \sigma)\}$. **Rtn** $\sigma$.
    **Rtn** $(\sigma^*, dwid^*, msg^*)$, where $dwid^* \leftarrow \phi_{wwk}(wid^*)$.
```

Fig. 10. Simulator $\mathcal{B}$ in the proof of Theorem 11

Theorem 12. DIBS***to***WWkIBS1 *is statistically private (under Def. 4) if the underlying DIBS scheme is statistically private (under Def. 8). Formally,* $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$, $\exists \Sigma'_{\text{WWkIBS}}$, $\exists \Sigma^\dagger_{\text{DIBS}}$, $\boldsymbol{Adv}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\Sigma'_{\text{WWkIBS}},\mathcal{A},l,m,n}(\lambda) = \boldsymbol{Adv}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\Sigma^\dagger_{\text{DIBS}},\mathcal{B},2ln,m}(\lambda)$.

Proof. We remind us that, what we must do to prove that the WWkIBS scheme Σ_{WWkIBS} is private under Def. 4 is to prove that for every $\lambda, l, m, n \in \mathbb{N}$ and every probabilistic algorithm $\mathcal{A}$, there exist polynomial time algorithms $\{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Sig}'\}$ and $\epsilon \in \mathsf{NGL}_\lambda$ s.t. $\mathtt{Adv}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\Sigma'_{\text{WWkIBS}},\mathcal{A},l,m,n}(\lambda) := |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},0}(1^\lambda, l, m, n)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},1}(1^\lambda, l, m, n))]| < \epsilon$.

Since we have assumed that the DIBS scheme $\Sigma_{\text{DIBS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Ver}\}$ with $l' := 2ln$ and $m' := m$ is private under Def. 8, it is true that for every $\lambda \in \mathbb{N}$ and every probabilistic algorithm $\mathcal{B}$, there exist polynomial time algorithms $\{\mathtt{Setup}^\dagger, \mathtt{KGen}^\dagger, \mathtt{Weaken}^\dagger, \mathtt{Down}^\dagger, \mathtt{Sig}^\dagger\}$ and $\epsilon \in \mathsf{NGL}_\lambda$ s.t. $\mathtt{Adv}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\Sigma^\dagger_{\text{DIBS}},\mathcal{B},2ln,m}(\lambda) :=$
$|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},0}(1^\lambda, 2ln, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},1}(1^\lambda, 2ln, m))]| < \epsilon$.

We define the algorithms $\{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Sig}'\}$ for Σ_{WWkIBS} as described in Fig. 12.

Let $\mathcal{A}$ (resp. B) denote an algorithm in the statistical privacy experiment w.r.t. Σ_{WWkIBS} (resp. Σ_{DIBS}). Let $\mathcal{B}$ run as described in Fig. 11. $\mathcal{B}$ uses $\mathcal{A}$ as a black box (or subroutine) to break the (statistical) privacy of Σ_{DIBS}.

It is obvious that if the experiment that $\mathcal{B}$ plays is $\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},0}$, $\mathcal{B}$ perfectly simulates $\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},0}$ to $\mathcal{A}$. It is also obvious that if the experiment that $\mathcal{B}$ plays is $\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},1}$ (w.r.t. $\Sigma^\dagger_{\text{DIBS}}$), $\mathcal{B}$ perfectly simulates $\boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},0}$ (w.r.t. Σ'_{WWkIBS}) to $\mathcal{A}$. Moreover, it is also obvious that iff $\mathcal{A}$ takes a behaviour which makes the experiment output 1, $\mathcal{B}$'s behaviour eventually makes the experiment output 1. Hence, $\bigwedge_{\beta \in \{0,1\}} \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathsf{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},\beta}(1^\lambda, 2ln, m)] = \Pr[1 \leftarrow$

```
$\mathcal{B}^{\mathfrak{Reveal}^\dagger,\mathfrak{Weaken}^\dagger,\mathfrak{Down}^\dagger,\mathfrak{Sign}^\dagger}(mpk, msk)$:   // $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, 2ln, m)$.
                                  // $(mpk, msk^\dagger(\ni msk)) \leftarrow \texttt{Setup}^\dagger(1^\lambda, 2ln, m)$.
    $sk_{\#^n} \leftarrow \texttt{KGen}(msk, 1^{2ln})$.
    $\mathbf{Rtn}\ b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Delegate},\mathfrak{Sign}}(mpk, sk_{\#^n})$, where
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    $-\mathfrak{Reveal}(id \in \mathcal{I}_{wk})$: $did \leftarrow \phi_{wk}(id)$. $sk \leftarrow \mathfrak{Reveal}^\dagger(did)$.
        // $sk \leftarrow \texttt{Down}(sk_{\#^n}, 1^{2ln}, [1, 2ln], did)$. $sk \leftarrow \texttt{Down}^\dagger(sk_{\#^n}, 1^{2ln}, [1, 2ln], did)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id)\}$. $\mathbf{Rtn}\ sk$.
    $-\mathfrak{Delegate}(sk, id, id' \in \mathcal{I}_{wk})$: $\mathbf{Rtn} \perp$ if $(sk, id) \notin \mathbb{Q} \bigvee 0 \leftarrow R_{wk}(id, id')$.
        $did \leftarrow \phi_{wk}(id)$. $did' \leftarrow \phi_{wk}(id')$. $sk' \leftarrow \mathfrak{Down}^\dagger(sk, did, \mathbb{I}_1(did), did')$.
        // $sk \leftarrow \texttt{Down}(sk, did, \mathbb{I}_1(did), did')$. $sk \leftarrow \texttt{Down}^\dagger(sk, did, \mathbb{I}_1(did), did')$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id')\}$. $\mathbf{Rtn}\ sk'$.
    $-\mathfrak{Sign}(sk, id \in \mathcal{I}_{wk}, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
        $\mathbf{Rtn} \perp$ if $(sk, id) \notin \mathbb{Q} \bigvee 0 \leftarrow \mathcal{R}_{wwk}(id, wid)$.
        $did \leftarrow \phi_{wk}(id)$. $dwid \leftarrow \phi_{wwk}(wid)$. $\mathbf{Rtn}\ \sigma \leftarrow \mathfrak{Sign}^\dagger(sk, did, \mathbb{I}_1(did), dwid)$.
        // $sk' \leftarrow \texttt{Down}(sk, did, \mathbb{I}_1(did), dwid)$. $\sigma \leftarrow \texttt{Sig}(sk', dwid, \mathbb{I}_1(dwid), msg)$.
        // $\sigma \leftarrow \texttt{Sig}^\dagger(msk^\dagger, dwid, msg)$.
```

Fig. 11. Simulator $\mathcal{B}$ in the proof of Theorem 12

```
$\texttt{Setup}'(1^\lambda, l, m, n)$:
    $(mpk, msk^\dagger) \leftarrow \texttt{Setup}^\dagger(1^\lambda, 2ln, m)$. $sk_{\#^n} \leftarrow \texttt{KGen}^\dagger(msk^\dagger, 1^{2ln})$. $\mathbf{Rtn}\ (mpk, sk_{\#^n})$.
$\texttt{KGen}'(sk_{id}, id \in \mathcal{I}_{wk}, id' \in \mathcal{I}_{wk})$:
    $did \leftarrow \phi_{wk}(id)$. $did' \leftarrow \phi_{wk}(id')$. $\mathbf{Rtn}\ sk_{id'} \leftarrow \texttt{Down}^\dagger(sk_{id}, did, \mathbb{I}_1(did), did')$.
$\texttt{Sig}'(msk, wid \in \mathcal{I}_{wwk}, msg \in \{0,1\}^m)$:
    $dwid \leftarrow \phi_{wwk}(wid)$. $\mathbf{Rtn}\ \sigma \leftarrow \texttt{Sig}^\dagger(msk^\dagger, dwid, msg)$.
```

Fig. 12. Three simulation algorithms $(\Sigma'_{\text{WWkIBS}} =)\{\texttt{Setup}', \texttt{KGen}', \texttt{Sig}'\}$ introduced for statistical privacy of the WWkIBS scheme Σ_{WWkIBS}, where $(\Sigma^\dagger_{\text{DIBS}} =)\{\texttt{Setup}^\dagger, \texttt{KGen}^\dagger, \texttt{Weaken}^\dagger, \texttt{Down}^\dagger, \texttt{Sig}^\dagger\}$ are the five simulation algorithms which make the DIBS scheme Σ_{DIBS} be statistically private

$\boldsymbol{Expt}^{\texttt{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},\beta}(1^\lambda, l, m, n)]$. Hence, $\texttt{Adv}^{\texttt{SP}}_{\Sigma_{\text{DIBS}},\mathcal{B},2ln,m}(\lambda) = \texttt{Adv}^{\texttt{SP}}_{\Sigma_{\text{WWkIBS}},\mathcal{A},l,n,m}(\lambda)$. □

B.4 Proof of Theorem 4 (on Five Implications among the Security Notions of TSS)

The theorem consists of the five implications. Each implication holds in any of the statistical and perfect formalization. For an instance of the first implication, statistical (resp. perfect) TRN implies statistical (resp. perfect) wPRV. We only prove the implications in the statistical formalization. The implications in the perfect formalization can be proven analogously.

(1) TRN Implies wPRV. Let $\mathcal{A}_{\texttt{wPRV}}$ denote a probabilistic algorithm in the wPRV experiments w.r.t. Σ_{TSS}, namely $\boldsymbol{Expt}^{\texttt{wPRV}}_{\Sigma_{\text{TSS}},\mathcal{A}_{\texttt{wPRV}},0}$ and $\boldsymbol{Expt}^{\texttt{wPRV}}_{\Sigma_{\text{TSS}},\mathcal{A}_{\texttt{wPRV}},1}$. We introduce an experiment $\boldsymbol{Expt}_{temp}$, defined as follows.

```
$\boldsymbol{Expt}_{temp}(1^\lambda, l)$:   // $b \in \{0,1\}$.
  $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$. **Rtn** $b' \leftarrow \mathcal{A}^{\mathfrak{SigSanLR}}(pk, sk)$, where
.................................................................................
    $-\mathfrak{SigSanLR}(msg_0, msg_1 \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      **Rtn** $\perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{\beta \in \{0,1\}} \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(pk, sk, \overline{msg}, \overline{\mathbb{T}})$. **Rtn** $(\overline{\sigma}, \overline{td})$.
```

We obtain $\mathtt{Adv}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l} = |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^\lambda, l)]| \leq |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)]| + |\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^\lambda, l)]|$.

Let $d \in \{0,1\}$. Let $\mathcal{B}_{\mathtt{TRN},d}$ denote a probabilistic algorithm in the TRN experiments w.r.t. Σ_{TSS}. $\mathcal{B}_{\mathtt{TRN},d}$ uses $\mathcal{A}_{\mathtt{wPRV}}$ which tries to distinguish $\boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},d}$ from $\boldsymbol{Expt}^{\mathtt{wPRV}}_{temp}$ as a sub-routine to distinguish the TRN experiments. $\mathcal{B}_{\mathtt{TRN},d}$ behaves as follows.

```
  $\mathcal{B}^{\mathfrak{San}/\mathfrak{Sig}}_{\mathtt{TRN},d}(pk, sk)$:   // $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$.
  **Rtn** $b' \leftarrow \mathcal{A}^{\mathfrak{SigSanLR}}_{\mathtt{wPRV}}(pk, sk)$, where
.................................................................................
    $-\mathfrak{SigSanLR}\begin{pmatrix} msg_0 \in \{0,1\}^l, msg_1 \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \\ \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l] \end{pmatrix}$:
      **Rtn** $\perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{\beta \in \{0,1\}} \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
      **Rtn** $(\overline{msg}, \overline{td}) \leftarrow \mathfrak{San}/\mathfrak{Sig}(msg_d, \mathbb{T}, \overline{msg}, \overline{\mathbb{T}})$.
```

For each $d \in \{0,1\}$, if the experiment whom $\mathcal{B}_{\mathtt{TRN},d}$ (unconsciously) does is $\boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},0}$ (resp. $\boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},1}$), $\mathcal{B}_{\mathtt{TRN},d}$ (unconsciously) perfectly simulates $\boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},d}$ (resp. $\boldsymbol{Expt}_{temp}$) to $\mathcal{A}_{\mathtt{wPRV}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},0}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},0}(1^\lambda, l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},1}(1^\lambda, l)]$. We also obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},1}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},0}(1^\lambda, l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},1}(1^\lambda, l)]$. Hence, $|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},d}(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)]| = \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},l}(\lambda)$ for each $d \in \{0,1\}$. Therefore, we obtain $\mathtt{Adv}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l}(\lambda) \leq \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},l}(\lambda) + \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},l}(\lambda)$. Let $d' := \underset{d \in \{0,1\}}{\arg\max}\{\mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},l}(\lambda)\}$. Let $\mathcal{B}_{\mathtt{TRN}}$ denote $\mathcal{B}_{\mathtt{TRN},d'}$. In conclusion, we obtain $\mathtt{Adv}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l}(\lambda) \leq 2 \cdot \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN}},l}(\lambda)$. □

(2) UNL Implies wPRV. Let $\mathcal{A}_{\mathtt{wPRV}}$ denote a probabilistic algorithm in the wPRV experiments w.r.t. Σ_{TSS}. Let $\mathcal{B}_{\mathtt{UNL}}$ denote a probabilistic algorithm in the UNL experiments w.r.t. Σ_{TSS}. $\mathcal{B}_{\mathtt{UNL}}$ uses $\mathcal{A}_{\mathtt{wPRV}}$ distinguishing the two wPRV experiments as a sub-routine to distinguish the two UNL experiments. $\mathcal{B}_{\mathtt{UNL}}$ behaves as follows.

```
$\mathcal{B}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}_{\mathtt{UNL}}(pk, sk)$:   // $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$.
  **Rtn** $b' \leftarrow \mathcal{A}^{\mathfrak{SigSanLR}}_{\mathtt{wPRV}}(pk, sk)$, where
.................................................................................
    $-\mathfrak{SigSanLR}\begin{pmatrix} msg_0 \in \{0,1\}^l, msg_1 \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \\ \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l] \end{pmatrix}$:
      **Rtn** $\perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{\beta \in \{0,1\}} \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
    $(\sigma_0, td_0) \leftarrow \mathfrak{Sign}(msg_0, \mathbb{T}_0)$, $(\sigma_1, td_1) \leftarrow \mathfrak{Sign}(msg_1, \mathbb{T}_1)$.
    **Rtn** $(\overline{msg}, \overline{td}) \leftarrow \mathfrak{SanLR}(msg_0, \mathbb{T}_0, \sigma_0, td_0, msg_1, \mathbb{T}_1, \sigma_1, td_1, \overline{msg}, \overline{\mathbb{T}})$.
```

If the experiment whom $\mathcal{B}_{\mathtt{UNL}}$ (unconsciously) does is the UNL experiment parameterized by $b \in \{0,1\}$, i.e., $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},b}$, $\mathcal{B}_{\mathtt{UNL}}$ (unconsciously) flawlessly simulates the wPRV experiment parameterized by b, i.e., $\boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},b}$, to $\mathcal{A}_{\mathtt{wPRV}}$. Additionally, $\mathcal{B}_{\mathtt{UNL}}$ directly outputs the bit outputted by $\mathcal{A}_{\mathtt{wPRV}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},b}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},b}(1^\lambda, l)]$ for each $b \in \{0,1\}$. Therefore, we obtain $\mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l}(\lambda) = \mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},l}(\lambda)$. □

(3) sPRV Implies TRN. Let $\mathcal{A}_{\mathtt{TRN}}$ denote a probabilistic algorithm in the TRN experiments w.r.t. Σ_{TSS}. Let $\mathcal{B}_{\mathtt{sPRV}}$ denote a probabilistic algorithm in the sPRV experiments w.r.t. Σ_{TSS}. $\mathcal{B}_{\mathtt{sPRV}}$ uses $\mathcal{A}_{\mathtt{TRN}}$ as a sub-routine to distinguish the two sPRV experiments. $\mathcal{B}_{\mathtt{sPRV}}$ behaves as follows.

```
$\mathcal{B}_{\mathtt{sPRV}}^{\mathfrak{Sign},\mathfrak{San/Sig}}(pk, sk)$:   // $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$.
  **Rtn** $b' \leftarrow \mathcal{A}_{\mathtt{TRN}}^{\mathfrak{San/Sig}}(pk, sk)$, where
.............................................................................
    $-\mathfrak{San/Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      **Rtn** $\perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
      $(\sigma, td) \leftarrow \mathfrak{Sign}(msg, \mathbb{T})$. $(\overline{msg}, \overline{td}) \leftarrow \mathfrak{San/Sig}(msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$.
      **Rtn** $(\overline{\sigma}, \overline{td})$.
```

If the experiment in whom $\mathcal{B}_{\mathtt{sPRV}}$ (unconsciously) engages is the sPRV-experiment with $b \in \{0,1\}$, i.e., $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV}},b}$, $\mathcal{B}_{\mathtt{sPRV}}$ (unconsciously) flawlessly simulates the transparency-experiment with b, i.e., $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV}},b}$, to $\mathcal{A}_{\mathtt{TRN}}$. Additionally, $\mathcal{B}_{\mathtt{sPRV}}$ outputs the bit outputted by $\mathcal{A}_{\mathtt{TRN}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{TRN}},b}(1^\lambda, l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV}},b}(1^\lambda, l)]$ for each $b \in \{0,1\}$. Therefore, we obtain $\mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{TRN}},l}(\lambda) = \mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV}},l}(\lambda)$. □

(4) sPRV Implies UNL. Let $\mathcal{A}_{\mathtt{UNL}}$ denote a probabilistic algorithm in the UNL experiments w.r.t. Σ_{TSS}, namely $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},0}$ and $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},1}$. We temporarily introduce an experiment $\boldsymbol{Expt}_{temp}$, defined as follows.

```
$\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},temp}(1^\lambda, l)$:   // $b \in \{0,1\}$.
  $(pk, sk) \leftarrow \mathtt{KGen}(1^\lambda, l)$. **Rtn** $b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}(pk, sk)$, where
.............................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
      $(\sigma, td) \leftarrow \mathtt{Sig}(pk, sk, msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. **Rtn** $(\sigma, td)$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
      **Rtn** $\perp$ if $(msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(pk, sk, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. **Rtn** $(\overline{\sigma}, \overline{td})$.
    $-\mathfrak{SanLR}\left(\begin{matrix} msg_0 \in \{0,1\}^l, \mathbb{T}_0 \subseteq [1,l], \sigma_0, td_0, msg_1 \in \{0,1\}^l, \mathbb{T}_1 \subseteq [1,l], \sigma_1, td_1, \\ \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l] \end{matrix}\right)$:
      **Rtn** $\perp$ if $\bigvee_{\beta \in \{0,1\}} \left[\begin{matrix} \overline{\mathbb{T}} \not\subseteq \mathbb{T}_\beta \bigvee (msg_\beta, \mathbb{T}_\beta, \sigma_\beta, td_\beta) \notin \mathbb{Q} \\ \bigvee\limits_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}} \end{matrix}\right]$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(pk, sk, \overline{msg}, \overline{\mathbb{T}})$. **Rtn** $(\overline{\sigma}, \overline{td})$.
```

We obtain $\mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},l} = |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^{\lambda},l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^{\lambda},l)]| \leq |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^{\lambda},l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)]| + |\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^{\lambda},l)]|$.

Let $d \in \{0,1\}$. Let $\mathcal{B}_{\mathtt{sPRV},d}$ denote a probabilistic algorithm in the $\mathtt{sPRV}$ experiments w.r.t. Σ_{TSS}. $\mathcal{B}_{\mathtt{sPRV},d}$ uses $\mathcal{A}_{\mathtt{UNL}}$ which tries to distinguish $\boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},d}$ from $\boldsymbol{Expt}_{temp}$ as a sub-routine to distinguish the two $\mathtt{sPRV}$ experiments. $\mathcal{B}_{\mathtt{sPRV},d}$ behaves as follows.

```
$\mathcal{B}^{\mathfrak{Sign},\mathfrak{San/Sig}}_{\mathtt{sPRV},d}(pk,sk)$:   // $(pk,sk) \leftarrow \mathtt{KGen}(1^{\lambda},l)$.
  $\textbf{Rtn } b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}_{\mathtt{UNL}}(pk,sk)$, where

    $-\mathfrak{Sign}(msg \in \{0,1\}^{l}, \mathbb{T} \subseteq [1,l])$:
      $(\sigma,td) \leftarrow \mathfrak{Sign}(msg,\mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg,\mathbb{T},\sigma,td)\}$. $\textbf{Rtn } (\sigma,td)$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^{l}, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^{l}, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
      $\textbf{Rtn } \bot \text{ if } (msg,\mathbb{T},\sigma,td) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
     $(\overline{\sigma},\overline{td}) \leftarrow \mathfrak{San/Sig}(msg,\mathbb{T},\sigma,td,\overline{msg},\overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg},\overline{\mathbb{T}},\overline{\sigma},\overline{td})\}$. $\textbf{Rtn } (\overline{\sigma},\overline{td})$.
    $-\mathfrak{SanLR}\begin{pmatrix} msg_0 \in \{0,1\}^{l}, \mathbb{T}_0 \subseteq [1,l], \sigma_0, td_0, msg_1 \in \{0,1\}^{l}, \mathbb{T}_1 \subseteq [1,l], \sigma_1, td_1, \\ \overline{msg} \in \{0,1\}^{l}, \overline{\mathbb{T}} \subseteq [1,l] \end{pmatrix}$:
      $\textbf{Rtn } \bot \text{ if } \bigvee_{\beta \in \{0,1\}} \begin{bmatrix} \overline{\mathbb{T}} \not\subseteq \mathbb{T}_{\beta} \bigvee (msg_{\beta},\mathbb{T}_{\beta},\sigma_{\beta},td_{\beta}) \notin \mathbb{Q} \\ \bigvee_{i \in [1,l] \text{ s.t. } msg_{\beta}[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}} \end{bmatrix}$.
      $(\overline{\sigma},\overline{td}) \leftarrow \mathfrak{San/Sig}(msg_d,\mathbb{T}_d,\sigma_d,td_d,\overline{msg},\overline{\mathbb{T}})$. $\textbf{Rtn } (\overline{\sigma},\overline{td})$.
```

For each $d \in \{0,1\}$, if the experiment whom $\mathcal{B}_{\mathtt{sPRV},d}$ (unconsciously) does is $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},d},0}$ (resp. $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},d},1}$), $\mathcal{B}_{\mathtt{sPRV},d}$ (unconsciously) perfectly simulates $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},d}$ (resp. $\boldsymbol{Expt}_{temp}$) to $\mathcal{A}_{\mathtt{UNL}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},0}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},0},0}(1^{\lambda},l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},0},1}(1^{\lambda},l)]$. We also obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},1}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},1},0}(1^{\lambda},l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},1},1}(1^{\lambda},l)]$. Hence, $|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},d}(1^{\lambda},l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)]| = \mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},d},l}(\lambda)$ for each $d \in \{0,1\}$. Therefore, we obtain $\mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},l}(\lambda) \leq \mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},0},l}(\lambda) + \mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},1},l}(\lambda)$. Let $d' := \underset{d \in \{0,1\}}{\arg\max}\{\mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},d},l}(\lambda)\}$. Let $\mathcal{B}_{\mathtt{sPRV}}$ denote $\mathcal{B}_{\mathtt{sPRV},d'}$. In conclusion, we obtain $\mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{UNL}},l}(\lambda) \leq 2 \cdot \mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV}},l}(\lambda)$. □

For each $d \in \{0,1\}$, if the experiment whom $\mathcal{B}_{\mathtt{sPRV},d}$ (unconsciously) does is $\boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{sPRV},d},0}$ (resp. $\boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},1}$), $\mathcal{B}_{\mathtt{TRN},d}$ (unconsciously) perfectly simulates $\boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},d}$ (resp. $\boldsymbol{Expt}_{temp}$) to $\mathcal{A}_{\mathtt{wPRV}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},0}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},0}(1^{\lambda},l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},1}(1^{\lambda},l)]$. We also obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},0}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},0}(1^{\lambda},l)]$, and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},1}(1^{\lambda},l)]$. Hence, $|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},d}(1^{\lambda},l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^{\lambda},l)]| = \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},l}(\lambda)$ for each $d \in \{0,1\}$. Therefore, we obtain $\mathtt{Adv}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l}(\lambda) \leq \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},0},l}(\lambda) +$

$\mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},1},l}(\lambda)$. Let $d' := \arg\max_{d\in\{0,1\}}\{\mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN},d},l}(\lambda)\}$. Let $\mathcal{B}_{\mathtt{TRN}}$ denote $\mathcal{B}_{\mathtt{TRN},d'}$. In conclusion, we obtain $\mathtt{Adv}^{\mathtt{wPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{wPRV}},l}(\lambda) \leq 2 \cdot \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN}},l}(\lambda)$. □

(5) Conjunction of TRN *and* UNL *Implies* sPRV*.* Let $\mathcal{A}_{\mathtt{sPRV}}$ denote a probabilistic algorithm in the sPRV experiments w.r.t. Σ_{TSS}, namely $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},0}$ and $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},1}$. We introduce an experiment $\boldsymbol{Expt}_{[(]}$. The three experiments are described as follows.

```
$\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},0}(1^\lambda,l)$:   // $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},temp}(1^\lambda,l)$, $\boxed{\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},1}(1^\lambda,l)}$.
  $(pk,sk) \leftarrow \mathtt{KGen}(1^\lambda,l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San/Sig}}_{\mathtt{sPRV}}(pk,sk)$, where
......................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
      $(\sigma,td) \leftarrow \mathtt{Sig}(pk,sk,msg,\mathbb{T})$. $\mathbb{Q} := \mathbb{Q}\bigcup\{(msg,\mathbb{T},\sigma,td)\}$. $\mathbf{Rtn}\ (\sigma,td)$.
    $-\mathfrak{San/Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      $\mathbf{Rtn}\ \bot$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee (msg,\mathbb{T},\sigma,td) \notin \mathbb{Q} \bigvee_{i\in[1,l] \text{ s.t. } msg[i]\neq\overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
      $(\overline{\sigma},\overline{td}) \leftarrow \mathtt{Sanit}(pk,msg,\mathbb{T},\sigma,td,\overline{msg},\overline{\mathbb{T}})$.
      $(\sigma',td') \leftarrow \mathtt{Sig}(pk,sk,msg,\mathbb{T})$. $(\overline{\sigma},\overline{td}) \leftarrow \mathtt{Sanit}(pk,msg,\mathbb{T},\sigma',td',\overline{msg},\overline{\mathbb{T}})$.
      $\boxed{(\overline{\sigma},\overline{td}) \leftarrow \mathtt{Sig}(pk,sk,msg,\mathbb{T}).}$ $\mathbb{Q} := \mathbb{Q}\bigcup\{(\overline{msg},\overline{\mathbb{T}},\overline{\sigma},\overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma},\overline{td})$.
```

We obtain $\mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},l} = |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^\lambda,l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^\lambda,l)]| \leq |\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^\lambda,l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda,l)]| + |\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda,l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^\lambda,l)]|$.

Let $\mathcal{B}_{\mathtt{UNL}}$ denote a probabilistic algorithm in the UNL experiments w.r.t. Σ_{TSS}. $\mathcal{B}_{\mathtt{UNL}}$ uses $\mathcal{A}_{\mathtt{sPRV}}$ which tries to distinguish $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},0}$ from $\boldsymbol{Expt}_{temp}$ as a sub-routine to distinguish the two UNL experiments. $\mathcal{B}_{\mathtt{UNL}}$ behaves as follows.

```
$\mathcal{B}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}_{\mathtt{UNL}}(pk,sk)$:   // $(pk,sk) \leftarrow \mathtt{KGen}(1^\lambda,l)$.
  $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San/Sig}}_{\mathtt{sPRV}}(pk,sk)$, where
......................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
      $(\sigma,td) \leftarrow \mathfrak{Sign}(pk,sk,msg,\mathbb{T})$. $\mathbb{Q} := \mathbb{Q}\bigcup\{(msg,\mathbb{T},\sigma,td)\}$. $\mathbf{Rtn}\ (\sigma,td)$.
    $-\mathfrak{San/Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      $\mathbf{Rtn}\ \bot$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee (msg,\mathbb{T},\sigma,td) \notin \mathbb{Q} \bigvee_{i\in[1,l] \text{ s.t. } msg[i]\neq\overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
    $(\sigma',td') \leftarrow \mathfrak{Sign}(pk,sk,msg,\mathbb{T})$. $(\overline{\sigma},\overline{td}) \leftarrow \mathfrak{SanLR}(msg,\mathbb{T},\sigma,td,msg,\mathbb{T},\sigma',td',\overline{msg},\overline{\mathbb{T}})$.
      $\mathbb{Q} := \mathbb{Q}\bigcup\{(\overline{msg},\overline{\mathbb{T}},\overline{\sigma},\overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma},\overline{td})$.
```

If the experiment whom $\mathcal{B}_{\mathtt{UNL}}$ (unconsciously) does is $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},0}$ (resp. $\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},1}$), $\mathcal{B}_{\mathtt{UNL}}$ (unconsciously) perfectly simulates $\boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},0}$ (resp. $\boldsymbol{Expt}_{temp}$) to $\mathcal{A}_{\mathtt{sPRV}}$. Hence, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A}_{\mathtt{sPRV}},0}(1^\lambda,l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},0}(1^\lambda,l)]$ and $\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda,l)] = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},1}(1^\lambda,l)]$. Hence, $|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},0}(1^\lambda,l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda,l)]| = \mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNL}},l}(\lambda)$.

In the same manner, we can prove that $|\Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}},\mathcal{A},1}(1^\lambda,l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda,l)]| = \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{TRN}},l}(\lambda)$, based on the simulator $\mathcal{B}_{\mathtt{TRN}}$ defined as follows.

```
$\mathcal{B}^{\mathfrak{San/Sig}}_{\mathtt{TRN}}(pk,sk)$:   // $(pk,sk) \leftarrow \mathtt{KGen}(1^\lambda,l)$.
  $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San/Sig}}_{\mathtt{sPRV}}(pk,sk)$, where
```

```
−$\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
    $(\sigma, td) \leftarrow \mathfrak{Sign}(pk, sk, msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}$ $(\sigma, td)$.
−$\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, td, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
    $\mathbf{Rtn}$ $\perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee (msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigvee_{i \in [1,l] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}}$.
    $(\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{San}/\mathfrak{Sig}(msg, \mathbb{T}, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
```

Therefore, we obtain $\mathtt{Adv}^{\mathtt{sPRV}}_{\Sigma_{\mathrm{TSS}}, \mathcal{A}_{\mathtt{sPRV}}, l}(\lambda) \leq \mathtt{Adv}^{\mathtt{UNL}}_{\Sigma_{\mathrm{TSS}}, \mathcal{B}_{\mathtt{UNL}}, l}(\lambda) + \mathtt{Adv}^{\mathtt{TRN}}_{\Sigma_{\mathrm{TSS}}, \mathcal{B}_{\mathtt{TRN}}, l}(\lambda)$. □

B.5 Proof of Theorem 5 (on Statistical Key-Invariance of DAMAC$\mathtt{to}$DIBS)

For the proof, we introduce 5 experiments. The first 2 (resp. The last 2) experiments are formally described in Fig. 13 (resp. Fig. 15). $\boldsymbol{Expt}_0$ (resp. $\boldsymbol{Expt}_4$) is identical to the standard experiment parameterized by 0 (resp. 1) w.r.t. $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$, i.e., $\boldsymbol{Expt}^{\mathtt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, 0}$ (resp. $\boldsymbol{Expt}^{\mathtt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, 1}$). $\boldsymbol{Expt}_1$ (resp. $\boldsymbol{Expt}_3$) is identical to $\boldsymbol{Expt}_0$ (resp. $\boldsymbol{Expt}_4$) except for the case where at least one square matrix S, uniform-randomly chosen from $\mathbb{Z}_p^{n' \times n'}$ at each oracle, does not have full-rank. A remaining intermediate experiment $\boldsymbol{Expt}_3$ is in Fig. 14. In the experiment, each secret-key at $\mathfrak{Weaken}$ or $\mathfrak{Down}$ is generated directly from msk.

We obtain $\mathtt{Adv}^{\mathtt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, l, m}(\lambda) = |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, l, m)]| \leq \sum_{i=1}^{4} |\Pr[1 \leftarrow \boldsymbol{Expt}_{i-1}(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_i(1^\lambda, l, m)]| + \Pr[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, l, m)]$, where the first transformation is because of the definition of key-invariance, and the second transformation is because of the triangle inequality. We provide 4 lemmata below. Lemma 28 can be proven in the same way as Lemma 25. Lemmata 26 and 27 can be proven easily. Based on the above inequality and the 4 lemmata we conclude that for every probabilistic algorithm $\mathcal{A}$, $\mathtt{Adv}^{\mathtt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, l, m}(\lambda) \leq \frac{2q_r + 3(q_{dd} + q_d)}{p-1}$. □

Lemma 25. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right]\right| \leq \frac{q_r + q_{dd} + q_d}{p-1}$.

Proof. To prove the lemma, we reuse Corollary 1. Obviously, both $\boldsymbol{Expt}_0$ and $\boldsymbol{Expt}_1$ are completely the same except for the case where $\boldsymbol{Expt}_1$ aborts, namely Abt, which implies that it holds that $|\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)]| \leq \Pr[Abt]$.

In $\boldsymbol{Expt}_1$, at each query to $\mathfrak{Reveal}$, $\mathfrak{Weaken}$ or $\mathfrak{Down}$, the event where the experiment aborts can *independently* occur. For $i \in [1, q_r]$ (resp. $i \in [1, q_{dd}]$, $i \in [1, q_d]$), let $AbtR_i$ (resp. $AbtDD_i$, $AbtD_i$) denote the event where, at i-th query to $\mathfrak{Reveal}$ (resp. $\mathfrak{Weaken}$, $\mathfrak{Down}$), the experiment aborts. Based on the fact that every event is independent from all of the other events and Corollary 1, we obtain

$$\Pr[Abt] = \Pr[\bigvee_{i=1}^{q_r} AbtR_i \bigvee_{i=1}^{q_{dd}} AbtDD_i \bigvee_{i=1}^{q_d} AbtD_i]$$

```
$\boldsymbol{Expt}_0(1^\lambda, l, m)(:= \boldsymbol{Expt}^{\mathtt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}},\mathcal{A},0}(1^\lambda, l, m))$:      // $\boxed{\boldsymbol{Expt}_1}$
    $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$.
    For $i \in [0, l+m]$: $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $\mathtt{Z}_i := (Y_i \mid \boldsymbol{x}_i)\, A$.
    $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A$.
    $mpk := ([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1)$. $msk := (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
    **Rtn** $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down}}(mpk, msk)$, where
    -----------------------------------------------------------------
    $-\mathfrak{Reveal}(id)$:
        $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$,
            where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $T := BS$. $\boxed{\textbf{Abt if } \mathtt{rank}(S) \neq n'.}$
        $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$.
        For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
        $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. **Rtn** $sk$.
    $-\mathfrak{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$:
        **Rtn** $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        Parse $sk$ as $([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        Re-randomize $sk$ for $(id, \mathbb{J})$ to obtain $sk'$ as follows.
            - $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\boxed{\textbf{Abt if } \mathtt{rank}(S') \neq n'.}$
            - $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$, $[W']_2 := [WS']_2$,
            - $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$, $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
            - For $i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\}$:
                $[\boldsymbol{e}'_i]_2 := [\boldsymbol{e}_i S']_2$, $[E'_i]_2 := [E_i S']_2$, $[d'_i]_2 := [d_i + \boldsymbol{e}'_i \boldsymbol{s}']_2$, $[\boldsymbol{d}'_i]_2 := [\boldsymbol{d}_i + E'_i \boldsymbol{s}']_2$.
            - $sk' := \left( [\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \left\{ \begin{matrix} [d'_i]_2, [\boldsymbol{d}'_i]_2, \\ [\boldsymbol{e}'_i]_2, [E'_i]_2 \end{matrix} \middle| i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\} \right\} \right)$.
        $sk'' := ([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d'_i]_2, [\boldsymbol{d}'_i]_2, [\boldsymbol{e}'_i]_2, [E'_i]_2 \mid i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id, \mathbb{J}')\}$. **Rtn** $sk''$.
    $-\mathfrak{Down}(sk, id, \mathbb{J}, id')$:
        **Rtn** $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        In the same manner as $\mathfrak{Weaken}$, parse $sk$, re-randomize $sk$ to obtain $sk'$, and parse $sk'$.
        $[u'']_2 := [u' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id')} d'_i]_2$. $[\boldsymbol{u}'']_2 := [\boldsymbol{u}' - \sum_{i \in \mathbb{I}_1(id||1^m) \bigcap \mathbb{I}_0(id')} \boldsymbol{d}'_i]_2$.
        $sk'' := \left( [\boldsymbol{t}']_2, [u'']_2, [\boldsymbol{u}'']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \left\{ \begin{matrix} [d'_i]_2, [\boldsymbol{d}'_i]_2, \\ [\boldsymbol{e}'_i]_2, [E'_i]_2 \end{matrix} \middle| i \in \mathbb{J} \bigcup_{j=l+1}^{l+m} \{j\} \setminus \mathbb{I}_0(id') \right\} \right)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id', \mathbb{J} \setminus \mathbb{I}_0(id')\}$. **Rtn** $sk''$.
```

Fig. 13. The first 2 experiments introduced to prove the statistical key-invariance of $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$

```
$\boldsymbol{Expt}_2(1^\lambda, l, m)$:.
    $A \leftsquigarrow \mathcal{D}_k$. $sk_{\text{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \texttt{Gen}_{\text{MAC}}(par)$.
    For $i \in [0, l+m]$: $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $\mathtt{Z}_i := (Y_i \mid \boldsymbol{x}_i)\, A$.
    $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A$.
    $mpk := ([A]_1, \{[Z_i]_1 \mid i \in [0, l+m]\}, [\boldsymbol{z}]_1)$. $msk := (sk_{\text{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
    $\mathbf{Rtn}$ $b \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Weaken}, \mathfrak{Down}}(mpk, msk)$, where
    ----------------------------------------------------------------
    $-\mathfrak{Reveal}(id)$:
        $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \texttt{Tag}(sk_{\text{MAC}}, id||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\mathbf{Abt}$ if $\texttt{rank}(S) \neq n'$. $T := BS$.
        $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$.
        For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
        $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \texttt{Tag}(sk_{\text{MAC}}, id||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\mathbf{Abt}$ if $\texttt{rank}(S) \neq n'$. $T := BS$.
        $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$.
        For $i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{i\}$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
        $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{j\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{J}')\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Down}(sk, id, \mathbb{J}, id')$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id'||1^m)\}) \leftarrow \texttt{Tag}(sk_{\text{MAC}}, id'||1^m)$,
          where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id'||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id'||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
        $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id'||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\mathbf{Abt}$ if $\texttt{rank}(S) \neq n'$. $T := BS$.
        $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id'||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id'||1^m) Y_i^\top T$.
        For $i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m} \{j\}$: $\boldsymbol{d}_i := h_i(id'||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id'||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id'||1^m) Y_i^\top T$.
        $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \setminus \mathbb{I}_0(id') \bigcup_{i=l+1}^{l+m} \{i\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id', \mathbb{J} \setminus \mathbb{I}_0(id')\}$. $\mathbf{Rtn}$ $sk''$.
```

Fig. 14. An intermediate experiment $\boldsymbol{Expt}_2$ introduced to prove the statistical key-invariance of $\Omega_{\text{DAMAC}}^{\text{DIBS}}$

```
$\boldsymbol{Expt}_4(1^\lambda, l, m)(:= \boldsymbol{Expt}^{\texttt{KI}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}, \mathcal{A}, 1}(1^\lambda, l, m))$:      // $\boxed{\boldsymbol{Expt}_3}$.
    $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x) \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(par)$.
    For $i \in [0, l+m]$: $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $\mathtt{Z}_i := (Y_i \mid \boldsymbol{x}_i)\, A$.
    $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A$.
    $mpk := ([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1)$. $msk := (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
    $\mathbf{Rtn}$ $b \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Weaken}, \mathfrak{Down}}(mpk, msk)$, where
    $-\mathfrak{Reveal}(id)$:
        Generate $sk$ for $id$ as follows.
            - $([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\}) \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$,
              where $\boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x$ and $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$.
            - $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top$. $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\boxed{\mathbf{Abt}\text{ if }\mathtt{rank}(S) \neq n'.}$ $T := BS$.
            - $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T$. $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T$.
            - For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$. $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
            - $sk := ([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        In the same manner as $\mathfrak{Reveal}$, generate $sk$ for $id$ and parse $sk$.
        Re-randomize $sk$ for $(id, \mathbb{I}_1(id))$ to obtain $sk'$ as follows.
            - $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$. $\boxed{\mathbf{Abt}\text{ if }\mathtt{rank}(S') \neq n'.}$
            - $[T']_2 := [TS']_2$, $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$, $[W']_2 := [WS']_2$,
            - $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$, $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
            - For $i \in \mathbb{I}_1(id) \bigcup_{j=l+1}^{l+m}\{j\}$:
                $[\boldsymbol{e}_i']_2 := [\boldsymbol{e}_i S']_2$, $[E_i']_2 := [E_i S']_2$, $[d_i']_2 := [d_i + \boldsymbol{e}_i'\boldsymbol{s}']_2$, $[\boldsymbol{d}_i']_2 := [\boldsymbol{d}_i + E_i'\boldsymbol{s}']_2$.
            - $sk' := \left([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \left\{\begin{matrix}[d_i']_2, [\boldsymbol{d}_i']_2, \\ [\boldsymbol{e}_i']_2, [E_i']_2\end{matrix} \middle| i \in \mathbb{I}_1(id) \bigcup_{j=l+1}^{l+m}\{j\}\right\}\right)$.
        $sk'' := ([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \{[d_i']_2, [\boldsymbol{d}_i']_2, [\boldsymbol{e}_i']_2, [E_i']_2 \mid i \in \mathbb{J}' \bigcup_{j=l+1}^{l+m}\{j\}\})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id, \mathbb{J}')\}$. $\mathbf{Rtn}$ $sk''$.
    $-\mathfrak{Down}(sk, id, \mathbb{J}, id')$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        In the same manner as $\mathfrak{Reveal}$, generate $sk$ for $id'$ and parse $sk$.
        In the same manner as $\mathfrak{Weaken}$, re-randomize $sk$ for $(id', \mathbb{I}_1(id'))$ to obtain $sk'$, and parse $sk'$.
        $sk'' := \left([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \left\{\begin{matrix}[d_i']_2, [\boldsymbol{d}_i']_2, \\ [\boldsymbol{e}_i']_2, [E_i']_2\end{matrix} \mid i \in \mathbb{J} \setminus \mathbb{I}_0(id') \bigcup_{j=l+1}^{l+m}\{j\}\right\}\right)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk'', id', \mathbb{J} \setminus \mathbb{I}_0(id')\}$. $\mathbf{Rtn}$ $sk''$.
```

Fig. 15. The last 2 experiments introduced to prove the statistical key-invariance of $\Omega^{\mathrm{DIBS}}_{\mathrm{DAMAC}}$

$$= \sum_{i=1}^{q_r} \Pr[AbtR_i] + \sum_{i=1}^{q_{dd}} \Pr[AbtDD_i] + \sum_{i=1}^{q_d} \Pr[AbtD_i]$$

$$= \sum_{i=1}^{q_r+q_{dd}+q_d} \Pr[\mathtt{rank}(S) \neq n' \mid S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}] \leq \frac{q_r + q_{dd} + q_d}{p-1}.$$

□

Lemma 26. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right]\right| = 0.$

Lemma 27. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_2(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right]\right| = 0.$

Lemma 28. $\left|\Pr\left[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)\right] - \Pr\left[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, l, m)\right]\right| \leq \frac{q_r+2(q_{dd}+q_d)}{p-1}.$

B.6 Proof of Theorem 6 (on Security of DIBStoTSS)

The theorem consists of the following three theorems.

Theorem 13. *$\Omega_{\mathrm{DIBS}}^{\mathrm{TSS}}$ is EUF-CMA if the underlying DIBS Σ_{DIBS} is EUF-CMA and KI. Formally, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B}_1 \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B}_2 \in \mathsf{PA}$, $\boldsymbol{Adv}_{\Omega_{\mathrm{DIBS}}^{\mathrm{TSS}}, \mathcal{A}, l}^{\textit{EUF-CMA}}(\lambda) \leq \boldsymbol{Adv}_{\Sigma_{\mathrm{DIBS}}, \mathcal{B}_1, l, l}^{\textit{EUF-CMA}}(\lambda) + \boldsymbol{Adv}_{\Sigma_{\mathrm{DIBS}}, \mathcal{B}_2, l, l}^{\textit{KI}}(\lambda)$.*

Proof. Let $\mathcal{A}$ denote a probabilistic algorithm in the EUF-CMA experiment w.r.t. DIBStoTSS, namely $\boldsymbol{Expt}_{\mathrm{DIBStoTSS}, \mathcal{A}}^{\mathtt{EUF-CMA}}$. Let the experiment be denoted by $\boldsymbol{Expt}_0$. We introduce a temporary experiment $\boldsymbol{Expt}_1$, which is defined in Fig. 16. We obtain $\mathtt{Adv}_{\mathrm{DIBStoTSS}, \mathcal{A}, l}^{\mathtt{EUF-CMA}}(\lambda) = \Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l)] \leq |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l)]| + \Pr[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l)]$. We define two simulators $\mathcal{B}_{\mathtt{KI}}$ and $\mathcal{B}_{\mathtt{UNF}}$ as follows.

```
$\mathcal{B}_{\mathtt{KI}}^{\mathfrak{Reveal}, \mathfrak{Weaken}, \mathfrak{Down}}(mpk, msk)$:   //   $(mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$.
  $(pk, sk) := (mpk, msk)$. $(\sigma^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Sign}, \mathfrak{Sanitize}, \mathfrak{SanitizeTd}}(pk)$, where
............................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
      $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$.
      $sk_{msg'}^{\mathbb{I}_1(msg')} \leftarrow \mathfrak{Reveal}(msg')$. $td := sk_{msg'}^{\mathbb{T}} \leftarrow \mathfrak{Weaken}(sk_{msg'}^{\mathbb{I}_1(msg')}, msg', \mathbb{I}_1(msg'), \mathbb{T})$.
      $sk_{msg}^{\mathbb{T} \setminus \mathbb{I}_0(msg)} \leftarrow \mathfrak{Down}(sk_{msg'}^{\mathbb{T}}, msg', \mathbb{T}, msg)$.
      $\sigma := sk_{msg}^{\emptyset} \leftarrow \mathfrak{Weaken}(sk_{msg}^{\mathbb{T} \setminus \mathbb{I}_0(msg)}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset)$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. Rtn $\sigma$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
      Rtn $\perp$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
      $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
      $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk_{msg'}^{\mathbb{T}}$.
      $sk_{\overline{msg}'}^{\mathbb{I}_1(\overline{msg}')} \leftarrow \mathfrak{Down}(sk_{msg'}^{\mathbb{T}}, msg', \mathbb{T}, \overline{msg}')$.
      $\overline{td} := sk_{\overline{msg}'}^{\overline{\mathbb{T}}} \leftarrow \mathfrak{Weaken}(sk_{\overline{msg}'}^{\mathbb{T} \setminus \mathbb{I}_0(\overline{msg}')}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}'), \overline{\mathbb{T}})$.
      $sk_{\overline{msg}}^{\overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg})} \leftarrow \mathfrak{Down}(sk_{\overline{msg}'}^{\overline{\mathbb{T}}}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
    $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Weaken}(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\textbf{Rtn}$ $\overline{\sigma}$.
  $-\mathfrak{SanitizeTd}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
    $\textbf{Rtn}$ $\perp$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
    $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
    $sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathfrak{Down}(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, \overline{msg}')$.
    $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathfrak{Weaken}(sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')}_{\overline{msg}'}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}'), \overline{\mathbb{T}})$.
    $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathfrak{Down}(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
    $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Weaken}(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
    $\mathbb{Q}_{td} := \mathbb{Q}_{td} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma})\}$. $\textbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
```

```
Write $\sigma^*$ as $sk^{\emptyset}_{msg^*}$. $\hat{msg} \leftsquigarrow \{0,1\}^l$. $\hat{\sigma} \leftarrow \mathtt{Sig}'(sk^{\emptyset}_{msg^*}, msg^*, \emptyset, \hat{msg})$.
$\textbf{Rtn}$ 1 if $\begin{bmatrix} 1 \leftarrow \mathtt{Ver}'(\hat{\sigma}, msg, \hat{msg}) & \bigwedge_{(msg,\mathbb{T},\sigma,td)\in\mathbb{Q}} & msg \neq msg^* \\ \bigwedge_{(msg,\mathbb{T},\sigma)\in\mathbb{Q}_{td}} & \bigvee_{i\in[1,l] \text{ s.t. } msg^*[i]\neq msg[i]} & i \notin \mathbb{T} \end{bmatrix}$.
$\textbf{Rtn}$ 0.
```

```
$\mathcal{B}^{\mathfrak{Reveal},\mathfrak{Sign}}_{\mathtt{UNF}}(mpk, msk)$:   // $(mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$.
  $(pk, sk) := (mpk, msk)$. $(\sigma^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanitizeTd}}(pk)$, where
```

```
  $-\mathfrak{Sign}(msg, \mathbb{T})$:
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$. $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathfrak{Reveal}(msg, \emptyset)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, \perp)\}$. $\textbf{Rtn}$ $\sigma$.
  $-\mathfrak{Sanitize}(msg, \mathbb{T}, \sigma, \overline{msg}, \overline{\mathbb{T}})$:
    $\textbf{Rtn}$ $\perp$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Sign}(\overline{msg}, \emptyset)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \perp)\}$. $\textbf{Rtn}$ $\overline{\sigma}$.
  $-\mathfrak{SanitizeTd}(msg, \mathbb{T}, \sigma, \overline{msg}, \overline{\mathbb{T}})$:
    $\textbf{Rtn}$ $\perp$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathfrak{Reveal}(\overline{msg}', \overline{\mathbb{T}})$.
    $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Reveal}(\overline{msg}, \emptyset)$.
    $\mathbb{Q}_{td} := \mathbb{Q}_{td} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma})\}$. $\textbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
```

```
Write $\sigma^*$ as $sk^{\emptyset}_{msg^*}$. $\hat{msg} \leftsquigarrow \{0,1\}^l$. $\hat{\sigma} \leftarrow \mathtt{Sig}'(sk^{\emptyset}_{msg^*}, msg^*, \emptyset, \hat{msg})$.
$\textbf{Rtn}$ $(\hat{\sigma}, msg^*, \hat{msg})$ if $1 \leftarrow \mathtt{Ver}'(\hat{\sigma}, msg, \hat{msg}) \bigwedge_{(msg,\mathbb{T},\sigma,td)\in\mathbb{Q}} msg \neq msg^*$
$\bigwedge_{(msg,\mathbb{T},\sigma)\in\mathbb{Q}_{td}} \bigvee_{i\in[1,l] \text{ s.t. } msg^*[i]\neq msg[i]} i \notin \mathbb{T}$.
$\textbf{Rtn}$ 0.
```

Based on the two simulators, we can easily verify that the 2 terms in the last inequality are upper-bounded by $\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_{\mathtt{KI}},l,l}(\lambda)$ and $\mathtt{Adv}^{\mathtt{UNF}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_{\mathtt{UNF}},l,l}(\lambda)$, respectively. Thus, we obtain $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\mathrm{DIBStoTSS},\mathcal{A},l}(\lambda) \leq \mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_0,l,l}(\lambda) + \mathtt{Adv}^{\mathtt{UNF}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_{\mathtt{UNF}},l,l}(\lambda)$. □

```
$\boldsymbol{Expt}_0(:= \boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\mathrm{DIBStoTSS},\mathcal{A}})(1^\lambda, l)$:   $//\boldsymbol{Expt}_1$
    $(pk, sk) := (mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$. $(\sigma^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanitizeTd}}(pk)$, where
    ------------------------------------------------------------------------------------------------
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
        $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$.
        $sk^{\mathbb{I}_1(msg')}_{msg'} \leftarrow \mathtt{KGen}'(msk, msg')$. $td := sk^{\mathbb{T}}_{msg'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(msg')}_{msg'}, msg', \mathbb{I}_1(msg'), \mathbb{T})$.
        $sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, msg)$.
        $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset)$.
        $sk^{\mathbb{I}_1(msg)}_{msg} \leftarrow \mathtt{KGen}'(msk, msg)$. $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(msg)}_{msg}, msg, \mathbb{I}_1(msg), \emptyset)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\textbf{Rtn}\ \sigma$.
    $-\mathfrak{Sanitize}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\textbf{Rtn}\ \bot$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
        $sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, \overline{msg}')$.
        $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}'}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}'), \overline{\mathbb{T}})$.
        $sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{KGen}'(msk, \overline{msg}')$. $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'}, \overline{msg}', \mathbb{I}_1(\overline{msg}'), \overline{\mathbb{T}})$.
        $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{Down}'(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
        $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
        $sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{KGen}'(msk, \overline{msg})$. $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}}, \overline{msg}, \mathbb{I}_1(\overline{msg}), \emptyset)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\textbf{Rtn}\ \overline{\sigma}$.
    $-\mathfrak{SanitizeTd}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
        $\textbf{Rtn}\ \bot$ if $(msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
        $sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, \overline{msg}')$.
        $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}'}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}'), \overline{\mathbb{T}})$.
        $sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{KGen}'(msk, \overline{msg}')$. $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'}, \overline{msg}', \mathbb{I}_1(\overline{msg}'), \overline{\mathbb{T}})$.
        $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{Down}'(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
        $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
        $sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{KGen}'(msk, \overline{msg})$. $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}}, \overline{msg}, \mathbb{I}_1(\overline{msg}), \emptyset)$.
        $\mathbb{Q}_{td} := \mathbb{Q}_{td} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma})\}$. $\textbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
    ------------------------------------------------------------------------------------------------
    Write $\sigma^*$ as $sk^{\emptyset}_{msg^*}$. $\hat{msg} \leftarrow\!\!\sim \{0,1\}^l$. $\hat{\sigma} \leftarrow \mathtt{Sig}'(sk^{\emptyset}_{msg^*}, msg^*, \emptyset, \hat{msg})$.
    $\textbf{Rtn}\ 1$ if $\begin{bmatrix} 1 \leftarrow \mathtt{Ver}'(\hat{\sigma}, msg, \hat{msg}) & \bigwedge_{(msg,\mathbb{T},\sigma,td)\in\mathbb{Q}} & msg \neq msg^* \\ \bigwedge_{(msg,\mathbb{T},\sigma)\in\mathbb{Q}_{td}} & \bigvee_{i\in[1,l] \text{ s.t. } msg^*[i]\neq msg[i]} & i \notin \mathbb{T} \end{bmatrix}$.
    $\textbf{Rtn}\ 0$.
```

Fig. 16. Experiments for `EUF-CMA` w.r.t. DIBS`to`TSS

Theorem 14. *$\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}}$ is sPRV if the underlying DIBS Σ_{DIBS} is KI. Formally, $\forall\mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists\mathcal{B}$, $\textbf{\textit{Adv}}^{\textit{sPRV}}_{\Omega^{\mathrm{TSS}}_{\mathrm{DIBS}},\mathcal{A},l}(\lambda) \leq 2 \cdot \textbf{\textit{Adv}}^{\textit{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B},l,l}(\lambda)$.*

Proof. Let $\mathcal{A}$ denote a probabilistic algorithm in the $\mathtt{sPRV}$ experiments w.r.t. DIBStoTSS, namely $\textbf{\textit{Expt}}^{\mathtt{sPRV}}_{\mathrm{DIBStoTSS},\mathcal{A},b}$ for $b \in \{0,1\}$. Let them be shortly denoted by $\textbf{\textit{Expt}}_b$. Let us introduce a temporary experiment $\textbf{\textit{Expt}}_{temp}$, which is defined in Fig. 17. We obtain $\mathtt{Adv}^{\mathtt{sPRV}}_{\mathrm{DIBStoTSS},\mathcal{A},l}(\lambda) = |\Pr[1 \leftarrow \textbf{\textit{Expt}}_0(1^\lambda,l)] - \Pr[1 \leftarrow \textbf{\textit{Expt}}_1(1^\lambda,l)]| \leq |\Pr[1 \leftarrow \textbf{\textit{Expt}}_0(1^\lambda,l)] - \Pr[1 \leftarrow \textbf{\textit{Expt}}_{temp}(1^\lambda,l)]| + |\Pr[1 \leftarrow \textbf{\textit{Expt}}_{temp}(1^\lambda,l)] - \Pr[1 \leftarrow \textbf{\textit{Expt}}^{\mathtt{wPRV}}_1(1^\lambda,l)]|$. We define two simulators $\mathcal{B}_0$ and $\mathcal{B}_1$ as follows.

```
$\mathcal{B}_0^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down}}(mpk,msk)$:   // $(mpk,msk) \leftarrow \mathtt{Setup}'(1^\lambda,l,l)$.
  $(pk,sk) := (mpk,msk)$. $\mathbf{Rtn}$ $b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San}/\mathfrak{Sig}}(pk,sk)$, where
.................................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
      $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$.
     $sk^{\mathbb{I}_1(msg')}_{msg'} \leftarrow \mathfrak{Reveal}(msg')$. $td := sk^{\mathbb{T}}_{msg'} \leftarrow \mathfrak{Weaken}(sk^{\mathbb{I}_1(msg')}_{msg'}, msg', \mathbb{I}_1(msg'), \mathbb{T})$.
      $sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg} \leftarrow \mathfrak{Down}(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, msg)$.
      $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathfrak{Weaken}(sk^{\mathbb{T}\setminus\mathbb{I}_0(msg)}_{msg}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset)$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg,\mathbb{T},\sigma,td)\}$. $\mathbf{Rtn}$ $(\sigma,td)$.
    $-\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      $\mathbf{Rtn}$ $\perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i\in[1,l] \text{ s.t. } msg[i]\neq\overline{msg}[i]} i \notin \overline{\mathbb{T}} \bigvee (msg,\mathbb{T},\sigma,\cdot) \notin \mathbb{Q}$.
      $\exists(msg,\mathbb{T},\sigma,td) \in \mathbb{Q}$ for some $td$.
      $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
      $sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathfrak{Down}(sk^{\mathbb{T}}_{msg'}, msg', \mathbb{T}, \overline{msg}')$.
      $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathfrak{Weaken}(sk^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}'}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}})$.
      $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathfrak{Down}(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
      $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Weaken}(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg},\overline{\mathbb{T}},\overline{\sigma},\overline{td})\}$. $\mathbf{Rtn}$ $(\overline{\sigma},\overline{td})$.
$\mathcal{B}_1^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down}}(mpk,msk)$:   // $(mpk,msk) \leftarrow \mathtt{Setup}'(1^\lambda,l,l)$.
  $(pk,sk) := (mpk,msk)$. $\mathbf{Rtn}$ $b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San}/\mathfrak{Sig}}(pk,sk)$, where
.................................................................................
    $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:   The same as $\mathcal{B}_0$.
    $-\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
      $\mathbf{Rtn}$ $\perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i\in[1,l] \text{ s.t. } msg[i]\neq\overline{msg}[i]} i \notin \overline{\mathbb{T}} \bigvee (msg,\mathbb{T},\sigma,\cdot) \notin \mathbb{Q}$.
      $\exists(msg,\mathbb{T},\sigma,td) \in \mathbb{Q}$ for some $td$.
      $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}}_{msg'}$.
      $sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathfrak{Reveal}(\overline{msg}')$.
      $\overline{td} := sk^{\overline{\mathbb{T}}}_{\overline{msg}'} \leftarrow \mathfrak{Weaken}(sk^{\mathbb{I}_1(\overline{msg}')}_{\overline{msg}'}, \overline{msg}', \mathbb{I}_1(\overline{msg}'), \overline{\mathbb{T}})$.
      $sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathfrak{Down}(sk^{\overline{\mathbb{T}}}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
      $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathfrak{Weaken}(sk^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg},\overline{\mathbb{T}},\overline{\sigma},\overline{td})\}$. $\mathbf{Rtn}$ $(\overline{\sigma},\overline{td})$.
```

Based on the two simulators, we can easily verify that the 2 terms in the last inequality are upper-bounded by $\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_0,l,l}(\lambda)$ and $\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\mathrm{DIBS}},\mathcal{B}_1,l,l}(\lambda)$,

```
$\boldsymbol{Expt}_0(:= \boldsymbol{Expt}^{\mathtt{sPRV}}_{\text{DIBStoTSS},\mathcal{A},0})(1^\lambda, l)$:   // $\boldsymbol{Expt}_{temp}$, $\boxed{\boldsymbol{Expt}_1(:= \boldsymbol{Expt}^{\mathtt{sPRV}}_{\text{DIBStoTSS},\mathcal{A},1})}$.
  $(pk, sk) := (mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{San}/\mathfrak{Sig}}(pk, sk)$, where
  ------------------------------------------------------------------------------------------------
  $-\mathfrak{Sign}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l])$:
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$.
    $sk_{msg'}^{\mathbb{I}_1(msg')} \leftarrow \mathtt{KGen}'(msk, msg')$. $td := sk_{msg'}^{\mathbb{T}} \leftarrow \mathtt{Weaken}'(sk_{msg'}^{\mathbb{I}_1(msg')}, msg', \mathbb{I}_1(msg'), \mathbb{T})$.
    $sk_{msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)} \leftarrow \mathtt{Down}'(sk_{msg'}^{\mathbb{T}}, msg', \mathbb{T}, msg)$.
    $\sigma := sk_{msg}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset)$.
    $sk_{msg}^{\mathbb{I}_1(msg)} \leftarrow \mathtt{KGen}'(msk, msg)$. $\sigma := sk_{msg}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{msg}^{\mathbb{I}_1(msg)}, msg, \mathbb{I}_1(msg), \emptyset)$.
    $\boxed{sk_{msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)} \leftarrow \mathtt{Down}'(sk_{msg'}^{\mathbb{T}}, msg', \mathbb{T}, msg).}$
    $\boxed{\sigma := sk_{msg}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)}, msg, \mathbb{T} \setminus \mathbb{I}_0(msg), \emptyset).}$
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}\ (\sigma, td)$.
  $-\mathfrak{San}/\mathfrak{Sig}(msg \in \{0,1\}^l, \mathbb{T} \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}} \subseteq [1,l])$:
    $\mathbf{Rtn}\ \perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i \in [1,l] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}} \bigvee (msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q}$.
    $\exists (msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}$ for some $td$.
    $msg' \leftarrow \Phi_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk_{msg'}^{\mathbb{T}}$.
    $sk_{\overline{msg}'}^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')} \leftarrow \mathtt{Down}'(sk_{msg'}^{\mathbb{T}}, msg', \mathbb{T}, \overline{msg}')$.
    $\overline{td} := sk_{\overline{msg}'}^{\overline{\mathbb{T}}} \leftarrow \mathtt{Weaken}'(sk_{\overline{msg}'}^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}, \overline{msg}', \mathbb{T} \setminus \mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}})$.
    $sk_{\overline{msg}'}^{\mathbb{I}_1(\overline{msg}')} \leftarrow \mathtt{KGen}'(msk, \overline{msg}')$. $\overline{td} := sk_{\overline{msg}'}^{\overline{\mathbb{T}}} \leftarrow \mathtt{Weaken}'(sk_{\overline{msg}'}^{\mathbb{I}_1(\overline{msg}')}, \overline{msg}', \mathbb{I}_1(\overline{msg}'), \overline{\mathbb{T}})$.
    $sk_{\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})} \leftarrow \mathtt{Down}'(sk_{\overline{msg}'}^{\overline{\mathbb{T}}}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg})$.
    $\overline{\sigma} := sk_{\overline{msg}}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
    $sk_{\overline{msg}}^{\mathbb{I}_1(\overline{msg})} \leftarrow \mathtt{KGen}'(msk, \overline{msg})$. $\overline{\sigma} := sk_{\overline{msg}}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{\overline{msg}}^{\mathbb{I}_1(\overline{msg})}, \overline{msg}, \mathbb{I}_1(\overline{msg}), \emptyset)$.
    $\boxed{sk_{\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})} \leftarrow \mathtt{Down}'(sk_{\overline{msg}'}^{\overline{\mathbb{T}}}, \overline{msg}', \overline{\mathbb{T}}, \overline{msg}).}$
    $\boxed{\overline{\sigma} := sk_{\overline{msg}}^{\emptyset} \leftarrow \mathtt{Weaken}'(sk_{\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}, \overline{msg}, \overline{\mathbb{T}} \setminus \mathbb{I}_0(\overline{msg}), \emptyset).}$
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
```

Fig. 17. Three experiments used in the proof of Theorem 14

respectively. Thus, we obtain $\mathtt{Adv}^{\mathtt{INV}}_{\text{DIBStoTSS},\mathcal{A},l}(\lambda) \leq 2 \cdot \max\{\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}},\mathcal{B}_0,l,l}(\lambda), \mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}},\mathcal{B}_1,l,l}(\lambda)\}$. □

Theorem 15. *$\Omega^{\text{TSS}}_{\text{DIBS}}$ is INV if the underlying DIBS Σ_{DIBS} is KI. Formally, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B}$, $\boldsymbol{Adv}^{\boldsymbol{INV}}_{\Omega^{\text{TSS}}_{\text{DIBS}},\mathcal{A},l}(\lambda) \leq 2 \cdot \boldsymbol{Adv}^{\boldsymbol{KI}}_{\Sigma_{\text{DIBS}},\mathcal{B},l,l}(\lambda)$.*

Proof. Let $\mathcal{A}$ denote a probabilistic algorithm in the INV experiments w.r.t. DIBStoTSS, namely $\boldsymbol{Expt}^{\mathtt{INV}}_{\text{DIBStoTSS},\mathcal{A},b}$ for $b \in \{0,1\}$. Let them be shortly denoted by $\boldsymbol{Expt}_b$. Let us introduce a temporary experiment $\boldsymbol{Expt}_{temp}$, which is defined in Fig. 18. We obtain $\mathtt{Adv}^{\mathtt{INV}}_{\text{DIBStoTSS},\mathcal{A},l}(\lambda) = |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_1(1^\lambda, l)]| \leq |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)]| + |\Pr[1 \leftarrow \boldsymbol{Expt}_{temp}(1^\lambda, l)] - \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{wPRV}}_1(1^\lambda, l)]|$. We define two simulators $\mathcal{B}_0$ and $\mathcal{B}_1$ as follows.

```
$\mathcal{B}_b^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down}}(mpk, msk)$:   // $(mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$.
  $(pk, sk) := (mpk, msk)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigLR},\mathfrak{SanLR}}(pk, sk)$, where
```

```
$-\mathfrak{SigLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l])$:
    $msg' \leftarrow \Phi_{\mathbb{T}_b}(msg)$.
$sk_{msg'}^{\mathbb{I}_1(msg')} \leftarrow \mathfrak{Reveal}(msg')$. $td := sk_{msg'}^{\mathbb{T}_b} \leftarrow \mathfrak{Weaken}(sk_{msg'}^{\mathbb{I}_1(msg')}, msg', \mathbb{I}_1(msg'), \mathbb{T}_b)$.
    $sk_{msg}^{\mathbb{T}_b \setminus \mathbb{I}_0(msg)} \leftarrow \mathfrak{Down}(sk_{msg'}^{\mathbb{T}_b}, msg', \mathbb{T}_b, msg)$.
    $\sigma := sk_{msg}^{\emptyset} \leftarrow \mathfrak{Weaken}(sk_{msg}^{\mathbb{T}_b \setminus \mathbb{I}_0(msg)}, msg, \mathbb{T}_b \setminus \mathbb{I}_0(msg), \emptyset)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td)\}$. $\mathbf{Rtn}$ $\sigma$.
$-\mathfrak{SanLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1 \subseteq [1,l])$:
    $\mathbf{Rtn}\ \bot$ if $\bigvee_{\beta \in \{0,1\}} \begin{bmatrix} \overline{\mathbb{T}}_\beta \nsubseteq \mathbb{T}_\beta \\ \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} \quad i \notin \overline{\mathbb{T}}_\beta \end{bmatrix} \bigvee (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, \cdot) \notin \mathbb{Q}$.
    $\exists (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td) \in \mathbb{Q}$ for some $td$.
    $msg' \leftarrow \Phi_{\mathbb{T}_b}(msg)$, $\overline{msg}' \leftarrow \Phi_{\overline{\mathbb{T}}_b}(\overline{msg})$. Write $td$ as $sk_{msg'}^{\mathbb{T}_b}$.
    $sk_{\overline{msg}'}^{\mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg}')} \leftarrow \mathfrak{Down}(sk_{msg'}^{\mathbb{T}_b}, msg', \mathbb{T}_b, \overline{msg}')$.
    $\overline{td} := sk_{\overline{msg}'}^{\overline{\mathbb{T}}_b} \leftarrow \mathfrak{Weaken}(sk_{\overline{msg}'}^{\mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg})}, \overline{msg}', \mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}}_b)$.
    $sk_{\overline{msg}}^{\overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg})} \leftarrow \mathfrak{Down}(sk_{\overline{msg}'}^{\overline{\mathbb{T}}_b}, \overline{msg}', \overline{\mathbb{T}}_b, \overline{msg})$.
    $\overline{\sigma} := sk_{\overline{msg}}^{\emptyset} \leftarrow \mathfrak{Weaken}(sk_{\overline{msg}}^{\overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg})}, \overline{msg}, \overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
    $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}$ $\overline{\sigma}$.
```

Based on the two simulators, we can easily verify that the 2 terms in the last inequality are upper-bounded by $\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}}, \mathcal{B}_0, l, l}(\lambda)$ and $\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}}, \mathcal{B}_1, l, l}(\lambda)$, respectively. Thus, we obtain $\mathtt{Adv}^{\mathtt{INV}}_{\text{DIBStoTSS}, \mathcal{A}, l}(\lambda) \leq 2 \cdot \max\{\mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}}, \mathcal{B}_0, l, l}(\lambda), \mathtt{Adv}^{\mathtt{KI}}_{\Sigma_{\text{DIBS}}, \mathcal{B}_1, l, l}(\lambda)\}$. □

B.7 Proof of Theorem 7 (on Security of TSStoDIBS)

The theorem consists of the following two theorems.

Theorem 16. *$\Omega^{\text{DIBS}}_{\text{TSS}}$ is EUF-CMA (under Def. 7) if the underlying TSS Σ_{TSS} is EUF-CMA (under Def. 9). Formally, $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$ s.t. $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Omega^{\text{DIBS}}_{\text{TSS}}, \mathcal{A}, l, m}(\lambda) = \mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\text{TSS}}, \mathcal{B}, l+m}(\lambda)$.*

Proof. Let $\mathcal{A}$ denote a probabilistic algorithm in the EUF-CMA experiment w.r.t. TSStoDIBS, namely $\boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\text{TSStoDIBS}, \mathcal{A}}$. Because of the definition, $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\text{TSStoDIBS}, \mathcal{A}, l, m}(\lambda) = \Pr[1 \leftarrow \boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\text{TSStoDIBS}, \mathcal{A}}(1^\lambda, l, m)]$. We define a PPT simulator $\mathcal{B}_{\mathtt{UNF}}$ as follows.

```
$\mathcal{B}_{\mathtt{UNF}}^{\mathfrak{Sign}, \mathfrak{Sanitize}, \mathfrak{SanitizeTd}}(pk, sk)$:   // $(pk, sk) \leftarrow \mathtt{KGen}'(1^\lambda, l+m)$.
  $(mpk, msk) := (pk, sk)$. $(\sigma^*, id^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Sign}}(mpk)$, where

    $-\mathfrak{Reveal}(id, \mathbb{J})$:   $\sigma \leftarrow \mathfrak{Sign}(id || 1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\})$.
      $sk := (\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{SanitizeTd}(id || 1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}, \sigma, id || 1^m, \mathbb{J} \bigcup_{i=l+1}^{l+m} \{i\}))$.
      $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Sign}(id, msg)$:   $\sigma \leftarrow \mathfrak{Sign}(id || 1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}))$.
    $(\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{Sanitize}(id || 1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}, \sigma, id || msg, \emptyset)$. $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \overline{\sigma})\}$.
$\mathbf{Rtn}$ $\overline{\sigma}$.
```

```
$\boldsymbol{Expt}_b(:= \boldsymbol{Expt}^{\mathtt{INV}}_{\mathrm{DIBS}\mathtt{to}\mathrm{TSS},\mathcal{A},b})(1^\lambda, l)$:    // $\boldsymbol{Expt}_{temp}$.
    $(pk, sk) := (mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, l, l)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigLR},\mathfrak{SanLR}}(pk, sk)$, where
    $-\mathfrak{SigLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l])$:
        $msg' \leftarrow \varPhi_{\mathbb{T}_b}(msg)$.
        $sk^{\mathbb{I}_1(msg')}_{msg'} \leftarrow \mathtt{KGen}'(msk, msg')$. $td := sk^{\mathbb{T}_b}_{msg'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(msg')}_{msg'}, msg', \mathbb{I}_1(msg'), \mathbb{T}_b)$.
        $sk^{\mathbb{T}_b \setminus \mathbb{I}_0(msg)}_{msg} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}_b}_{msg'}, msg', \mathbb{T}_b, msg)$.
        $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}_b \setminus \mathbb{I}_0(msg)}_{msg}, msg, \mathbb{T}_b \setminus \mathbb{I}_0(msg), \emptyset)$.
        $sk^{\mathbb{I}_1(msg)}_{msg} \leftarrow \mathtt{KGen}'(msk, msg)$. $\sigma := sk^{\emptyset}_{msg} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(msg)}_{msg}, msg, \mathbb{I}_1(msg), \emptyset)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td)\}$. $\mathbf{Rtn}\ \sigma$.
    $-\mathfrak{SanLR}(msg \in \{0,1\}^l, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,l], \sigma, \overline{msg} \in \{0,1\}^l, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1 \subseteq [1,l])$:
        $\mathbf{Rtn} \perp$ if $\bigvee_{\beta \in \{0,1\}} \left[ \overline{\mathbb{T}}_\beta \not\subseteq \mathbb{T}_\beta \bigvee_{i \in [1,l] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \overline{\mathbb{T}}_\beta \right] \bigvee (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, \cdot) \notin \mathbb{Q}$.
        $\exists (msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $msg' \leftarrow \varPhi_{\mathbb{T}_b}(msg)$, $\overline{msg}' \leftarrow \varPhi_{\overline{\mathbb{T}}_b}(\overline{msg})$. Write $td$ as $sk^{\mathbb{T}_b}_{msg'}$.
        $sk^{\mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg}')}_{\overline{msg}'} \leftarrow \mathtt{Down}'(sk^{\mathbb{T}_b}_{msg'}, msg', \mathbb{T}_b, \overline{msg}')$.
        $\overline{td} := sk^{\overline{\mathbb{T}}_b}_{\overline{msg}'} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg})}_{\overline{msg}'}, \overline{msg}', \mathbb{T}_b \setminus \mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}}_b)$.
        $sk^{\overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{Down}'(sk^{\overline{\mathbb{T}}_b}_{\overline{msg}'}, \overline{msg}', \overline{\mathbb{T}}_b, \overline{msg})$.
        $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg})}_{\overline{msg}}, \overline{msg}, \overline{\mathbb{T}}_b \setminus \mathbb{I}_0(\overline{msg}), \emptyset)$.
        $sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}} \leftarrow \mathtt{KGen}'(msk, \overline{msg})$. $\overline{\sigma} := sk^{\emptyset}_{\overline{msg}} \leftarrow \mathtt{Weaken}'(sk^{\mathbb{I}_1(\overline{msg})}_{\overline{msg}}, \overline{msg}, \mathbb{I}_1(\overline{msg}), \emptyset)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(\overline{msg}, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ \overline{\sigma}$.
```

Fig. 18. Three experiments used in the proof of Theorem 15

```
$\boldsymbol{Expt}^{\mathtt{EUF\text{-}CMA}}_{\mathrm{TSS}\mathtt{to}\mathrm{DIBS},\mathcal{A}}(1^\lambda, l, m)$:
    $(mpk, msk) := (pk, sk) \leftarrow \mathtt{KGen}'(1^\lambda, l + m)$. $(\sigma^*, id^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(mpk)$, where
    $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$:    $(\sigma, td) \leftarrow \mathtt{Sig}'(sk, id||1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\})$.
        $sk := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}, \sigma, td, id||1^m, \mathbb{J} \bigcup_{i=l+1}^{l+m} \{i\})$.
        $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$. $\mathbf{Rtn}\ sk$.
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$:    $(\sigma, td) \leftarrow \mathtt{Sig}'(sk, id||1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}))$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{I}_1(id) \bigcup_{i=l+1}^{l+m} \{i\}, \sigma, td, id||msg, \emptyset)$.
        $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \overline{\sigma})\}$. $\mathbf{Rtn}\ \overline{\sigma}$.
    $\mathbf{Rtn}\ 1$ if $1 \leftarrow \mathtt{Ver}'(pk, \sigma^*, id^*||msg^*) \bigwedge_{(id,\mathbb{J}) \in \mathbb{Q}_r} id^* \not\preceq_{\mathbb{J}} id$
        $\bigwedge_{(id,msg,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*)$.
    $\mathbf{Rtn}\ 0$.
```

Fig. 19. Experiment for unforgeability w.r.t. TSS`to`DIBS

```
    Rtn 1 if $\left[\begin{array}{c} 1 \leftarrow \mathtt{Ver}'(pk, \sigma^*, id^*||msg^*) \bigwedge_{(id,\mathbb{J}) \in \mathbb{Q}_r} id^* \not\preceq_{\mathbb{J}} id \\ \bigwedge_{(id,msg,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*) \end{array}\right]$.
    Rtn 0.
```

We obtain $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\mathrm{TSStoDIBS},\mathcal{A},l,m}(\lambda) = \mathtt{Adv}^{\mathtt{UNF}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_{\mathtt{UNF}},l+m}(\lambda)$. □

Theorem 17. *$\Omega^{\mathrm{DIBS}}_{\mathrm{TSS}}$ is statistically signer private (under Def. 8) if the underlying TSS Σ_{TSS} is statistically TRN and UNL (under Def. 10). Formally, for every probabilistic algorithm $\mathcal{A}$, there exist probabilistic algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$ and four polynomial-time algorithms $\Pi'_{\mathrm{DIBS}} = \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Down}', \mathtt{Sig}'\}$ such that $\boldsymbol{Adv}^{\boldsymbol{SP}}_{\Omega^{\mathrm{DIBS}}_{\mathrm{TSS}},\Pi'_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) \leq \boldsymbol{Adv}^{\boldsymbol{UNL}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_1,l+m}(\lambda) + 2 \cdot \boldsymbol{Adv}^{\boldsymbol{TRN}}_{\Sigma_{\mathrm{TSS}},\mathcal{B}_2,l+m}(\lambda)$.*

Proof. Let $\mathcal{A}$ denote a probabilistic algorithm in the statistical signer-privacy experiments, namely $\boldsymbol{Expt}^{\mathtt{SP}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},0}$ and $\boldsymbol{Expt}^{\mathtt{SP}}_{\Sigma_{\mathrm{DIBS}},\mathcal{A},1}$. The latter experiment is associated with simulation algorithms $\{\mathtt{SimSetup}, \mathtt{SimKGen}, \mathtt{SimDisD}, \mathtt{SimDown}, \mathtt{SimSig}\}$, defined as follows.

```
$\mathtt{SimSetup}$, $\mathtt{SimKGen}$, $\mathtt{SimDisD}$, $\mathtt{SimDown}$:   The same as the original ones of TSStoDIBS.
$\mathtt{SimSig}(msk, id \in \{0,1\}^l, msg \in \{0,1\}^m)$:  Write $msk$ as $sk$. $(\sigma, td) \leftarrow \mathtt{Sig}(sk, id||msg, \emptyset)$.
```

The two experiments are shortly denoted by $\boldsymbol{Expt}_0$ and $\boldsymbol{Expt}_3$, respectively. We introduce two experiments, namely $\boldsymbol{Expt}_1$ and $\boldsymbol{Expt}_2$. The four experiments are described in Fig. 20.

We obtain $\mathtt{Adv}^{\mathtt{SP}}_{\Pi_{\mathrm{DIBS}},\Pi'_{\mathrm{DIBS}},\mathcal{A},l,m}(\lambda) = |\Pr[1 \leftarrow \boldsymbol{Expt}_0(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_3(1^\lambda, l, m)]| \leq \sum_{i=1}^{3} |\Pr[1 \leftarrow \boldsymbol{Expt}_{i-1}(1^\lambda, l, m)] - \Pr[1 \leftarrow \boldsymbol{Expt}_i(1^\lambda, l, m)]|$. We define three simulators $\mathcal{B}_{\mathtt{UNL}}$, $\mathcal{B}_{\mathtt{TRN}}$ and $\mathcal{B}'_{\mathtt{TRN}}$ as follows.

```
$\mathcal{B}_{\mathtt{UNL}}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}(mpk, msk)$:   // $(mpk, msk) \leftarrow \mathtt{KGen}(1^\lambda, l+m)$.
  Rtn $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where

    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
      $sk := (\sigma, td) \leftarrow \mathfrak{Sign}(id||1^m, \mathbb{I}_1(id) \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. Rtn $sk$.
    $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], \mathbb{J}' \subseteq [1,l])$:
      Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \nsubseteq \mathbb{J}$. Parse $sk$ as $(\sigma, td)$.
      $sk' := (\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{Sanitize}(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{J}')\}$. Rtn $sk'$.
    $-\mathfrak{Down}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l)$:
      Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
      $sk' := (\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{Sanitize}(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id', \mathbb{J}')\}$. Rtn $sk'$.
    $-\mathfrak{Sign}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      Rtn $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
      $(\sigma', td') \leftarrow \mathfrak{Sign}(id||1^m, \mathbb{J} \bigcup [l+1, l+m])$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{SanLR}(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td,$
                          $id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma', td', id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $(\overline{\overline{\sigma}}, \overline{\overline{td}}) \leftarrow \mathfrak{Sanitize}(id'||1^m, \mathbb{J}' \bigcup [l+1, l+m], \overline{\sigma}, \overline{td}, id'||msg, \emptyset)$. Rtn $\overline{\overline{\sigma}}$.
```

```
$\boldsymbol{Expt}_0(:= \boldsymbol{Expt}^{\mathsf{SP}}_{\mathrm{TSStoDIBS},\mathcal{A},0})(1^\lambda, l, m)$:   // $\boxed{\boldsymbol{Expt}_1}$, $\boxed{\boldsymbol{Expt}_2}$, $\boldsymbol{Expt}_3(:= \boldsymbol{Expt}^{\mathsf{SP}}_{\mathrm{TSStoDIBS},\mathrm{TSStoDIBS}',\mathcal{A},1})$.
    $(mpk, msk) \leftarrow \mathtt{KGen}'(1^\lambda, l+m)$.
    $\mathbf{Rtn}\ b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where
    ------------------------------------------------------------------------
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
        $sk := (\sigma, td) \leftarrow \mathtt{Sig}'(msk, id||1^m, \mathbb{I}_1(id) \bigcup [l+1, l+m])$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}\ sk$.
    $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], \mathbb{J}' \subseteq [1,l])$:
        $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$. Parse $sk$ as $(\sigma, td)$.
        $sk' := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id, \mathbb{J}')\}$. $\mathbf{Rtn}\ sk'$.
    $-\mathfrak{Down}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l)$:
        $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
        $sk' := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id', \mathbb{J}' \bigcup [l+1, l+m])\}$. $\mathbf{Rtn}\ sk'$.
    $-\mathfrak{Sign}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l, msg \in \{0,1\}^m)$:
        $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$.
        $\boxed{(\sigma, td) \leftarrow \mathtt{Sig}'(msk, id||1^m, \mathbb{J} \bigcup [l+1, l+m]).}$
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J} \setminus \mathbb{I}_0(id') \bigcup [l+1, l+m])$.
        $\boxed{(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}'(msk, id'||1^m, \mathbb{J} \setminus \mathbb{I}_0(id') \bigcup [l+1, l+m])}$.
        $(\overline{\overline{\sigma}}, \overline{\overline{td}}) \leftarrow \mathtt{Sanit}'(id'||1^m, \mathbb{J} \setminus \mathbb{I}_0(id') \bigcup [l+1, l+m], \overline{\sigma}, \overline{td}, id'||msg, \emptyset)$.
        $(\overline{\overline{\sigma}}, \overline{\overline{td}}) \leftarrow \mathtt{Sig}'(msk, id'||msg, \emptyset)$. $\mathbf{Rtn}\ \overline{\overline{\sigma}}$.
```

Fig. 20. Four experiments used in the proof of Theorem 17

```
$\mathcal{B}^{\mathfrak{San}/\mathfrak{Sig}}_{\mathtt{TRN}}(mpk, msk)$:   // $(mpk, msk) \leftarrow \mathtt{KGen}(1^\lambda, l+m)$.
  $\mathbf{Rtn}\ b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where
..........................................................................
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
      $sk := (\sigma, td) \leftarrow \mathtt{Sig}'(msk, id||1^m, \mathbb{I}_1(id) \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}\ sk$.
    $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], \mathbb{J}' \subseteq [1,l])$:
      $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$. Parse $sk$ as $(\sigma, td)$.
      $sk := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||1^m, \mathbb{J} \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{J}')\}$. $\mathbf{Rtn}\ sk$.
    $-\mathfrak{Down}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l)$:
      $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
      $sk' := (\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}'(id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id', \mathbb{J}')\}$. $\mathbf{Rtn}\ sk'$.
    $-\mathfrak{Sign}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      $\mathbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
      $(\sigma, td) \leftarrow \mathtt{Sig}'(msk, id||1^m, \mathbb{J} \bigcup [l+1, l+m])$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \mathfrak{San}/\mathfrak{Sig}(id||1^m, \mathbb{J} \bigcup [l+1, l+m], id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $(\overline{\overline{\sigma}}, \overline{\overline{td}}) \leftarrow \mathtt{Sanit}'(id'||1^m, \mathbb{J}' \bigcup [l+1, l+m], \overline{\sigma}, \overline{td}, id'||msg, \emptyset)$. $\mathbf{Rtn}\ \overline{\overline{\sigma}}$.
```

```
${\mathcal{B}'_{\mathtt{TRN}}}^{\mathfrak{San}/\mathfrak{Sig}}(mpk, msk)$:   // $(mpk, msk) \leftarrow \mathtt{KGen}(1^\lambda, l+m)$.
  $\mathbf{Rtn}\ b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where
..........................................................................
```

```
    $-\mathfrak{Reveal}, \mathfrak{Weaken}, \mathfrak{Down}$:   Same as $\mathcal{B}_{\texttt{TRN}}$.
    $-\mathfrak{Sign}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], id' \in \{0,1\}^l, msg \in \{0,1\}^m)$:
      $\textbf{Rtn} \perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \npreceq_{\mathbb{J}} id$. Parse $sk$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
      $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sig}'(msk, id'||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
      $(\overline{\overline{\sigma}}, \overline{\overline{td}}) \leftarrow \mathfrak{San}/\mathfrak{Sig}(id'||1^m, \mathbb{J}' \bigcup [l+1, l+m], id'||msg, \emptyset)$. $\textbf{Rtn}\ \overline{\overline{\sigma}}$.
```

We can easily verify that the 3 terms in the last inequality are upper-bounded by $\texttt{Adv}^{\texttt{UNL}}_{\Sigma_{\text{TSS}}, \mathcal{B}_{\texttt{UNL}}, l+m}(\lambda)$, $\texttt{Adv}^{\texttt{TRN}}_{\Sigma_{\text{TSS}}, \mathcal{B}_{\texttt{TRN}}, l+m}(\lambda)$, $\texttt{Adv}^{\texttt{TRN}}_{\Sigma_{\text{TSS}}, \mathcal{B}'_{\texttt{TRN}}, l+m}(\lambda)$, respectively. Thus, we obtain $\texttt{Adv}^{\texttt{SP}}_{\Pi_{\text{DIBS}}, \Pi'_{\text{DIBS}}, \mathcal{A}, l, m}(\lambda) \leq \texttt{Adv}^{\texttt{UNL}}_{\Sigma_{\text{TSS}}, \mathcal{B}_{\texttt{UNL}}, l+m}(\lambda) + 2 \cdot \max\{\texttt{Adv}^{\texttt{TRN}}_{\Sigma_{\text{TSS}}, \mathcal{B}_{\texttt{TRN}}, l+m}(\lambda), \texttt{Adv}^{\texttt{TRN}}_{\Sigma_{\text{TSS}}, \mathcal{B}'_{\texttt{TRN}}, l+m}(\lambda)\}$. □

C The Second Transformations from DIBS into Non-Wildcarded IBS Primitives

*Transforming DIBS into IBS (*DIBS*to*IBS2*).* An IBS scheme (w. identity length $l \in \mathbb{N}$) can be generically transformed from a DIBS scheme (w. the same identity length l) $\Sigma_{\text{DIBS}} = \{\texttt{Setup}', \texttt{KGen}', \texttt{Weaken}', \texttt{Down}', \texttt{Sig}', \texttt{Ver}'\}$ as follows.

```
IBS.$\texttt{Setup}(1^\lambda, l, m)$: $\textbf{Rtn}\ (mpk, msk) \leftarrow \texttt{Setup}'(1^\lambda, l, m)$.
IBS.$\texttt{KGen}(msk, id \in \{0,1\}^l)$:
  $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \texttt{KGen}'(msk, id)$. $\textbf{Rtn}\ sk_{id}^{\emptyset} \leftarrow \texttt{Weaken}'(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), \emptyset)$.
IBS.$\texttt{Sig}(sk_{id}(= sk_{id}^{\emptyset}), id \in \{0,1\}^l, msg \in \{0,1\}^m)$: $\textbf{Rtn}\ \sigma_{id} \leftarrow \texttt{Sig}'(sk_{id}^{\emptyset}, id, msg)$.
IBS.$\texttt{Ver}(\sigma_{id}, id \in \{0,1\}^l, msg \in \{0,1\}^m)$: $\textbf{Rtn}\ 1\ /\ 0 \leftarrow \texttt{Ver}'(\sigma_{id}, id, msg)$.
```

Its correctness and security are reduced to those of the underlying DIBS scheme. Theorem 19 is proven below.

Theorem 18. DIBS*to*IBS2 *is correct if the underlying DIBS scheme is correct.*

Theorem 19. DIBS*to*IBS2 *is existentially unforgeable (under Def. 13) if the underlying DIBS scheme is existentially unforgeable (under Def. 7). Formally,* $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$, $\textit{\textbf{Adv}}^{\textit{EUF-CMA}}_{\text{DIBS}\,to\text{IBS2}, \mathcal{A}, l, m}(\lambda) = \textit{\textbf{Adv}}^{\textit{EUF-CMA}}_{\Sigma_{\text{DIBS}}, \mathcal{B}, l, m}(\lambda)$.

Proof. The simulator $\mathcal{B}$ behaves as follows.

```
$\mathcal{B}^{\mathfrak{Reveal}', \mathfrak{Sign}'}(mpk)$:   // $(msk, mpk) \leftarrow \texttt{Setup}'(1^\lambda, l, m)$.
  $\textbf{Rtn}\ (\sigma^*, id^* \in \{0,1\}^l, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Sign}}(mpk)$, where
........................................................................
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$: $sk' \leftarrow \mathfrak{Reveal}'(id, \emptyset)$.
      // $sk \leftarrow \texttt{KGen}'(msk, id)$. $sk' \leftarrow \texttt{Weaken}'(sk, id, \mathbb{I}_1(id), \emptyset)$.
      $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{id\}$. $\textbf{Rtn}\ sk$.
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m)$: $\sigma \leftarrow \mathfrak{Sign}'(id, msg)$.
      // $sk \leftarrow \texttt{KGen}'(msk, id)$. $\sigma \leftarrow \texttt{Sig}'(sk, id, \mathbb{I}_1(id), msg)$.
      $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \sigma)\}$. $\textbf{Rtn}\ \sigma$.
```

It is obvious that $\mathcal{B}$ perfectly simulates $\textit{\textbf{Expt}}^{\texttt{EUF-CMA}}_{\text{DIBStoIBS2}, \mathcal{A}, l, m}$ to $\mathcal{A}$. It is also obvious that iff $\mathcal{A}$ outputs σ^*, id^* and msg^* s.t. $1 \leftarrow$ IBS.$\texttt{Ver}(\sigma^*, id^*, msg^*) \bigwedge_{id \in \mathbb{Q}_r} id \neq id^* \bigwedge_{(id, msg, \cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*)$, $\mathcal{B}$ outputs the ones s.t. $1 \leftarrow \texttt{Ver}'(\sigma^*, id^*, msg^*) \bigwedge_{(id, \emptyset) \in \mathbb{Q}'_r} id^* \npreceq_{\emptyset} id \bigwedge_{(id, msg, \cdot) \in \mathbb{Q}'_s} (id, msg) \neq (id^*, msg^*)$ (note: $id^* \npreceq_{\emptyset} id$ is logically equivalent to $id^* \neq id$). Hence, $\texttt{Adv}^{\texttt{EUF-CMA}}_{\text{DIBStoIBS2}, \mathcal{A}, l, m}(\lambda) = \texttt{Adv}^{\texttt{EUF-CMA}}_{\Sigma_{\text{DIBS}}, \mathcal{B}, l, m}(\lambda)$. □

*Transforming DIBS into Wicked IBS (*DIBS$\mathtt{\textit{to}}$WkIBS2*).* A WkIBS scheme parameterized by l, n can be generically transformed from a DIBS scheme $\Sigma_{\text{DIBS}} = \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}', \mathtt{Ver}'\}$ with identity length $l' := ln$ as follows.

```
WkIBS.$\mathtt{Setup}(1^\lambda, l, m, n)$:
  $(mpk, msk) \leftarrow \mathtt{Setup}'(1^\lambda, ln, m)$. $sk_{\#^n} := sk_{1^{ln}}^{\mathbb{I}_1(1^{ln})} \leftarrow \mathtt{KGen}'(msk, 1^{ln})$.
  Rtn $(mpk, sk_{\#^n})$.
WkIBS.$\mathtt{KGen}(sk_{id}, id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n, id' \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n)$:
  Write $sk_{id}$ as $sk_{did}^{\mathbb{J}}$, where $did := \phi_{wk}(id)$ and $\mathbb{J} := \bigcup_{i \in [1,n] \text{ s.t. } id_i = \#} [l \cdot (i-1)+1, l \cdot i]$.
  $sk_{did'}^{\mathbb{J} \setminus \mathbb{I}_0(did')} \leftarrow \mathtt{Down}'(sk_{did}^{\mathbb{J}}, did, \mathbb{J}, did')$, where $did' := \phi_{wk}(id')$.
  Rtn $sk_{id'} := sk_{did'}^{\mathbb{J}'} \leftarrow \mathtt{Weaken}'(sk_{did'}^{\mathbb{J} \setminus \mathbb{I}_0(did)}, did', \mathbb{J} \setminus \mathbb{I}_0(did'), \mathbb{J}')$,
    where $\mathbb{J}' := \bigcup_{i \in [1,n] \text{ s.t. } id'_i = \#} [l \cdot (i-1)+1, l \cdot i]$.
WkIBS.$\mathtt{Sig}(sk_{id}, id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n, msg \in \{0,1\}^m)$:
  Write $sk_{id}$ as $sk_{did}^{\mathbb{J}}$, where $did := \phi_{wk}(id)$ and $\mathbb{J} := \bigcup_{i \in [1,n] \text{ s.t. } id_i = \#} [l \cdot (i-1)+1, l \cdot i]$.
  Rtn $\sigma_{id} := \sigma_{did} \leftarrow \mathtt{Sig}'(sk_{did}^{\mathbb{J}}, did, \mathbb{J}, msg)$.
WkIBS.$\mathtt{Ver}(\sigma_{id}, id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n, msg \in \{0,1\}^m)$:
  Write $\sigma_{id}$ as $\sigma_{did}$, where $did \leftarrow \phi_{wk}(id)$. Rtn $1 \,/\, 0 \leftarrow \mathtt{Ver}'(\sigma_{did}, did, msg)$.
```

Its correctness and security are reduced to those of the underlying DIBS scheme.

Theorem 20. DIBS$\mathtt{\textit{to}}$WkIBS2 *is correct if the underlying DIBS scheme is correct.*

Theorem 21. DIBS$\mathtt{\textit{to}}$WkIBS2 *is existentially unforgeable (under Def. 3) if the underlying DIBS scheme is existentially unforgeable (under Def. 7). Formally,* $\forall \mathcal{A} \in \mathsf{PPTA}_\lambda$, $\exists \mathcal{B} \in \mathsf{PPTA}_\lambda$, $\boldsymbol{\mathit{Adv}}^{\textit{EUF-CMA}}_{\text{DIBS}\textit{to}\text{WkIBS2},\mathcal{A},l,m,n}(\lambda) = \boldsymbol{\mathit{Adv}}^{\textit{EUF-CMA}}_{\Sigma_{\text{DIBS}},\mathcal{B},ln,m}(\lambda)$.

Proof. The simulator $\mathcal{B}$ behaves as follows.

```
$\mathcal{B}^{\mathfrak{Reveal}', \mathfrak{Sign}'}(mpk)$:    // $(msk, mpk) \leftarrow \mathtt{Setup}'(1^\lambda, ln, m)$.
  $(\sigma^*, id^* \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n, msg^* \in \{0,1\}^m) \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Sign}}(mpk)$, where
.......................................................................
    $-\mathfrak{Reveal}(id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n)$:
      $sk' \leftarrow \mathfrak{Reveal}'(did, \mathbb{J})$,
        where $did \leftarrow \phi_{wk}(id)$ and $\mathbb{J} := \bigcup_{i \in [1,n] \text{ s.t. } id_i = \#} [l \cdot (i-1)+1, l \cdot i]$
      // $sk \leftarrow \mathtt{KGen}'(msk, did)$. $sk' \leftarrow \mathtt{Weaken}'(sk, did, \mathbb{I}_1(did), \mathbb{J})$.
      $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{id\}$. Rtn $sk$.
    $-\mathfrak{Sign}(id \in (\{0,1\}^l \setminus \{1^l\} \bigcup \{\#\})^n, msg \in \{0,1\}^m)$:
      $\sigma \leftarrow \mathfrak{Sign}'(did, msg)$, where $did \leftarrow \phi_{wk}(id)$.
      // $sk \leftarrow \mathtt{KGen}'(msk, did)$. $\sigma \leftarrow \mathtt{Sig}'(sk, did, \mathbb{I}_1(did), msg)$.
      $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \sigma)\}$. Rtn $\sigma$.
.......................................................................
      Rtn $(\sigma^*, did^*, msg^*)$, where $did^* := \phi_{wk}(id^*)$.
```

It is obvious that $\mathcal{B}$ perfectly simulates $\boldsymbol{\mathit{Expt}}^{\mathtt{EUF\text{-}CMA}}_{\text{DIBS}\mathtt{to}\text{WkIBS2},\mathcal{A},l,m}$ to $\mathcal{A}$. It is also obvious that iff $\mathcal{A}$ outputs σ^*, id^* and msg^* s.t. $1 \leftarrow$ WkIBS.$\mathtt{Ver}(\sigma^*, id^*, msg^*) \bigwedge_{id \in \mathbb{Q}_r} 0 \leftarrow R_w(id, id^*) \bigwedge_{(id,msg,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*)$, $\mathcal{B}$ outputs the ones s.t. $1 \leftarrow \mathtt{Ver}'(\sigma^*, did^*, msg^*) \bigwedge_{(did,\emptyset) \in \mathbb{Q}'_r} did^* \not\preceq_{\mathbb{J}} did \bigwedge_{(did,msg,\cdot) \in \mathbb{Q}'_s} (did, msg) \neq (did^*, msg^*)$ (note: $did^* \not\preceq_{\mathbb{J}} did$ is logically equivalent to $0 \leftarrow R_{wk}(id, id^*)$). Hence, $\mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\text{DIBS}\mathtt{to}\text{WkIBS2},\mathcal{A},l,n,m}(\lambda) = \mathtt{Adv}^{\mathtt{EUF\text{-}CMA}}_{\Sigma_{\text{DIBS}},\mathcal{B},ln,m}(\lambda)$. □

Instantiations and Efficiency Analysis. Existing and our non-wildcarded IBS schemes are compared in Table 3. Although we present a discussion on WkIBS schemes, basically the same discussion can be applied to IBS and HIBS schemes. Firstly note that DIBS`to`WkIBS1 instantiated by our DIBS scheme $\mathrm{DIBS}_{\mathrm{Ours}}$ (which is the one obtained by instantiating our DAMAC-based DIBS in Sect. 4 by our DAMAC scheme in Sect. 3) and WkIBE`to`WkIBS instantiated by $\mathrm{WkIBE}_{\mathrm{BGP}}$ are basically the same WkIBS scheme. Thus, their efficiency are identical. DIBS`to`WkIBS2 instantiated by $\mathrm{DIBS}_{\mathrm{Ours}}$ and either of them achieve asymptotically the equivalent efficiency. However, their actual efficiency greatly differ, in terms of size of master public/secret-key and (user) secret-key. The WkIBS scheme via DIBS`to`WkIBS2 has

$$\begin{aligned} mpk &= ([A]_1, \{[Z_i]_1 \mid i \in [0, l+m], [\boldsymbol{z}]_1\}), \\ msk &= (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y}), \end{aligned}$$

where $sk_{\mathrm{MAC}} = (B, \{\boldsymbol{x}_i \mid i \in [0, l+m]\}, x)$. On the other hand, the WiIBS scheme via DIBS`to`WkIBS1 has

$$\begin{aligned} mpk &= ([A]_1, \{[Z_i]_1 \mid i \in [0, 2l+m], [\boldsymbol{z}]_1\}), \\ msk &= (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, 2l+m]\}, \boldsymbol{y}), \end{aligned}$$

where $sk_{\mathrm{MAC}} = (B, \{\boldsymbol{x}_i \mid i \in [0, 2l+m]\}, x)$. In the WkIBS scheme via DIBS`to`WkIBS2, a secret-key for a (wicked) identity id is

$$sk_{id} = \left(\begin{array}{c} [\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \\ \left\{ [d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \middle| i \in \bigcup_{j \in [1,l] \text{ s.t. } id[j] = \#} \{j\} \bigcup_{j=l+1}^{l+m} \{j\} \right\} \end{array} \right).$$

On the other hand, in the WkIBS scheme via DIBS`to`WkIBS1, it is

$$sk_{id} = \left(\begin{array}{c} [\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \\ \left\{ [d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \middle| i \in \bigcup_{j \in [1,l] \text{ s.t. } id[j] = \#} \{2j-1, 2j\} \bigcup_{j=2l+1}^{2l+m} \{j\} \right\} \end{array} \right).$$

Thus, for master-public/secret-key and (user) secret-key, size of the former becomes approximately two thirds of the size of the latter if $l \approx m$. Note that for signature, there is no difference between them.

Schemes	Building Blo.	$\lvert mpk\rvert$	$\lvert sk\rvert$	$\lvert\sigma\rvert$	Sec. Loss	Assump.
$\mathrm{IBS}_{\mathrm{PS}}$ [26]	–	$(l+m+5)\lvert g\rvert$	$2\lvert g\rvert$	$3\lvert g\rvert$	$\mathcal{O}((q_r+q_s)q_s lm)$	CDH
HIBEtoIBS	$\mathrm{HIBE}_{\mathrm{BGP}}$ [7]	$\mathcal{O}(lk^2)\lvert g_1\rvert$	$\mathcal{O}(lk^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin
DIBStoIBS1(2)	$\mathrm{DIBS}_{\mathrm{Ours}}$	$\mathcal{O}((l+m)k^2)\lvert g_1\rvert$	$\mathcal{O}(mk^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin
$\mathrm{HIBS}_{\mathrm{CS1}}$ [15]	–	$\mathcal{O}(l+n)\lvert g_1\rvert+\lvert g_T\rvert$	$\lvert g_1\rvert+\mathcal{O}(n)\lvert g_2\rvert$	$\lvert g_1\rvert+\mathcal{O}(n)\lvert g_1\rvert$	$\mathcal{O}\left(((q_r+q_s)l)^n\right)$	coCDH
$\mathrm{HIBS}_{\mathrm{CS2}}$ [15]	–	$\mathcal{O}(l+n)(\lvert g_1\rvert+\lvert g_2\rvert)+\lvert g_T\rvert$	$\mathcal{O}(n)\lvert g_1\rvert$	$\mathcal{O}(n)\lvert g_1\rvert$	$\mathcal{O}\left(((q_r+q_s)l)^n\right)$	coCDH
HIBEtoHIBS	$\mathrm{HIBE}_{\mathrm{BGP}}$ [7]	$\mathcal{O}(lnk^2)\lvert g_1\rvert$	$\mathcal{O}(lnk^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin
HIBEtoHIBS	$\mathrm{HIBE}_{\mathrm{LP1}}$ [23]	$\mathcal{O}(ln^2k^2)(\lvert g_1\rvert+\lvert g_2\rvert)$	$\mathcal{O}(ln^2k^2)\lvert g_2\rvert$	$(4k+1)\lvert g_2\rvert$	$\mathcal{O}(ln^2k)$	k-Lin
HIBEtoHIBS	$\mathrm{HIBE}_{\mathrm{LP2}}$ [23]	$\mathcal{O}(ln^2k^2)(\lvert g_1\rvert+\lvert g_2\rvert)$	$(3k\hat{n}+k+1)\lvert g_2\rvert$	$(3k\hat{n}+k+1)\lvert g_2\rvert$	$\mathcal{O}(lnk)$	k-Lin
DIBStoHIBS1(2)	$\mathrm{DIBS}_{\mathrm{Ours}}$	$\mathcal{O}((ln+m)k^2)\lvert g_1\rvert$	$\mathcal{O}((ln+m)k^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin
WkIBEtoWkIBS	$\mathrm{WkIBE}_{\mathrm{BGP}}$ [7]	$\mathcal{O}(lnk^2)\lvert g_1\rvert$	$\mathcal{O}(lnk^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin
DIBStoWkIBS1(2)	$\mathrm{DIBS}_{\mathrm{Ours}}$	$\mathcal{O}((ln+m)k^2)\lvert g_1\rvert$	$\mathcal{O}((ln+m)k^2)\lvert g_2\rvert$	$(2k+2)\lvert g_2\rvert$	$\mathcal{O}(q_r+q_s)$	k-Lin

Table 3. Comparison in terms of efficiency and security among existing *non-wildcarded* IBS schemes which are adaptively and weakly (existentially) unforgeable under standard (static) assumptions. There are 3 categories: (from top to bottom) IBS, HIBS and WkIBS. The message space is basically $\{0,1\}^m$. For the IBS categories, the ID space is $\{0,1\}^l$. For the HIBS categories, it is $(\{0,1\}^l)^{\leq n}$. For the WkIBS categories, it is $(\{0,1\}^l \bigcup \{\#\})^n$. For schemes obtained via the encryption-to-signatures transformations, e.g., HIBEtoHIBS, WkIBEtoWkIBS, spaces for message and ID are commonly $\{0,1\}^l$. For schemes based on symmetric bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, $|g|$ (resp. $|g_T|$) denotes bit length of an element in $\mathbb{G}$ (resp. $\mathbb{G}_T$). For schemes based on asymmetric bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, $|g_1|$ (resp. $|g_2|$, $|g_T|$) denotes bit length of an element in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$, $\mathbb{G}_T$). q_r (resp. q_s) denotes total number that $\mathcal{A}$ issues a query to $\mathfrak{Reveal}$ (resp. $\mathfrak{Sign}$). $\mathrm{HIBE}_{\mathrm{CS1}}$ (resp. $\mathrm{HIBE}_{\mathrm{CS2}}$) denotes the 1st (resp. 2nd) HIBS scheme in [15]. $\mathrm{HIBE}_{\mathrm{BGP}}$ (resp. $\mathrm{WkIBE}_{\mathrm{BGP}}$) denotes the HIBE (resp. WkdIBE) scheme in [7] (instantiated from their DIBE scheme). $\mathrm{HIBE}_{\mathrm{LP1}}$ (resp. $\mathrm{HIBE}_{\mathrm{LP2}}$) denotes the 1st (resp. 2nd) HIBKEM scheme in [23] (originally denoted by HIBKEM_1 (resp. HIBKEM_2)).

D Security Analysis of the Existing TSS Constructions

Security Analysis of TSS_{YSL}. We present three theorems related to the security of $\mathrm{TSS}_{\mathrm{YSL}}$.

Theorem 22. *TSS_{YSL} is perfectly* $\mathtt{TRN}$*.*

Proof. In the experiment $\boldsymbol{Expt}_0$ w.r.t. $\mathrm{TSS}_{\mathrm{YSL}}$, to generate the signature $\sigma = (\sigma_0, \sigma_1, \hat{VK})$ on $\mathfrak{San}/\mathfrak{Sig}$, we firstly generate σ_1 on $\hat{VK}||\hat{msg}||msg$ by $\hat{SK}$, then $\overline{\sigma}_1$ on $\hat{VK}||\hat{msg}||\overline{msg}$ by the same $\hat{SK}$. $\overline{\sigma}_1$ is independent of σ_1. Hence, the signature σ distributes identically to the one in $\boldsymbol{Expt}_1$ w.r.t. $\mathrm{TSS}_{\mathrm{YSL}}$. □

Theorem 23. *TSS_{YSL} is not statistically* $\mathtt{UNL}$*.*

Proof. We consider a probabilistic adversary $\mathcal{A}$ which behaves in $\boldsymbol{Expt}_b^{\mathtt{UNL}}$ w.r.t. $\mathrm{TSS}_{\mathrm{YSL}}$ as follows.

$\mathcal{A}$ arbitrarily chooses $(msg, \mathbb{T})$, then asks them to $\mathfrak{Sign}$ to get (σ_0, td_0), where $\sigma_0 = (\hat{VK}_0, \sigma_{00}, \sigma_{10})$ and $td_0 = \hat{SK}_0$. $\mathcal{A}$ secondly asks the same $(msg, \mathbb{T})$ to $\mathfrak{Sign}$ to get (σ_1, td_1), where $\sigma_1 = (\hat{VK}_1, \sigma_{01}, \sigma_{11})$ and $td_1 = \hat{SK}_1$. If $\hat{VK}_0 = \hat{VK}_1$, then $\mathcal{A}$ aborts. Then, $\mathcal{A}$ asks $(msg, \mathbb{T}, \sigma_0, td_0, msg, \mathbb{T}, \sigma_1, td_1, msg, \mathbb{T})$ to $\mathfrak{SanLR}$ to get $(\overline{\sigma}, \overline{td})$.

$\mathcal{A}$ outputs $b' := 0$ if the first element of $\overline{\sigma}$ is $\hat{VK}_0$. $\mathcal{A}$ outputs $b' := 1$ if the first element of $\overline{\sigma}$ is $\hat{VK}_1$. $\mathcal{A}$ correctly guesses b except for the case where $\mathcal{A}$ aborts with a negligible probability. □

Theorem 24. *TSS_{YSL} is not statistically* $\mathtt{INV}$ *if the underlying digital signature scheme is* $\mathtt{EUF\text{-}CMA}$*.*

Proof. We consider a probabilistic adversary $\mathcal{A}$ which behaves in $\boldsymbol{Expt}_b^{\mathtt{INV}}$ w.r.t. $\mathrm{TSS}_{\mathrm{YSL}}$ as follows.

$\mathcal{A}$ arbitrarily chooses $(msg, \mathbb{T}_0, \mathbb{T}_1)$ s.t. $\mathbb{T}_0 \neq \mathbb{T}_1$ to $\mathfrak{SigLR}$, then gets $\sigma = (\hat{VK}, \sigma_0, \sigma_1)$. For each $\beta \in \{0, 1\}$, let $\hat{msg}_\beta := ||_{i=1}^{l}\hat{msg}[i]$, where $\hat{msg}[i]$ is set to $\star$ (if $i \in \mathbb{T}_\beta$) or $msg[i]$ (otherwise).

We consider the following three cases.

1. σ_0 is (resp. is not) a correct signature on $\hat{VK}||\hat{msg}_0$ (resp. $\hat{VK}||\hat{msg}_1$).
2. σ_0 is not (resp. is) a correct signature on $\hat{VK}||\hat{msg}_0$ (resp. $\hat{VK}||\hat{msg}_1$).
3. σ_0 is (resp. is) a correct signature on $\hat{VK}||\hat{msg}_0$ (resp. $\hat{VK}||\hat{msg}_1$).

Because of correctness of the digital signature scheme, either of the three cases must occur.

If the first case occurs, because of the correctness, b must be 0. $\mathcal{A}$ outputs $b' := 0$. Else if the second case occurs, because of the correctness, b must be 1. $\mathcal{A}$ outputs $b' := 1$.

Else if the third case occurs, in any case of $b = 0$ and $b = 1$, that contradicts to the $\mathtt{EUF\text{-}CMA}$ of the digital signature scheme. Let us consider the case of $b = 0$. σ_0 has been generated as a signature on $\hat{VK}||\hat{msg}_0$. The fact that σ_0 is a correct signature on $\hat{VK}||\hat{msg}_1$ implies that $\mathcal{A}$ found a correct forged signature. □

Security Analysis of TSS_{CLM}. We present two theorems related to the security of $\mathrm{TSS}_{\mathrm{CLM}}$.

Theorem 25. *TSS_{CLM} is not statistically* `wPRV` *if the underlying IBCH scheme is collision-resistant under the definition in [14].*

Proof. We consider a probabilistic adversary $\mathcal{A}$ which behaves in $\boldsymbol{Expt}_b^{\mathtt{wPRV}}$ w.r.t. $\mathrm{TSS}_{\mathrm{CLM}}$ as follows.

$\mathcal{A}$ arbitrarily chooses $(msg_0, msg_1, \mathbb{T}, \overline{msg})$ s.t. $msg_0 \neq msg_1$ to $\mathfrak{SigSanLR}$ to get $(\overline{\sigma}, \overline{td})$, where $\overline{\sigma} = (\cdot, \{\cdot, \cdot \mid i \in \mathbb{T}\}, \overline{h}, \overline{r})$. We remind us that $\overline{h}$ is an IBCH hash of the message $\overline{msg}$ and the randomness $\overline{r}$ under the message msg_b as an ID, and that $\overline{td}$ is an IBCH secret-key for the message msg_b as an ID.

Let us consider the following three cases, where $\hat{msg} \notin \{msg_0, msg_1\}$ is an arbitrarily chosen message.

1. $\overline{h}$ is identical to the hash value of $(\overline{msg}, \overline{r})$ under msg_0, and is not identical to the one under msg_1.
2. $\overline{h}$ is identical to the hash value of $(\overline{msg}, \overline{r})$ under msg_1, and is not identical to the one under msg_0.
3. $\overline{h}$ is identical to the hash value of $(\overline{msg}, \overline{r})$ under msg_0, and is identical to the one under msg_1. Moreover, $\mathcal{A}$ finds a pair of a message $\hat{msg} \notin \{msg_0, msg_1\}$ and a randomness $\hat{r}$ whose hash value under msg_0 is identical to $\hat{h}$ by the collision-finder algorithm using the IBCH secret-key td. $\mathcal{A}$ also finds a pair of a message $\tilde{msg} \notin \{msg_0, msg_1\}$ and a randomness $\tilde{r}$ whose hash value under msg_1 is identical to $\hat{h}$ by the collision-finder algorithm using the IBCH secret-key td.

Because of correctness of IBCH, either of the three cases must occur.

If the first case occurs, because of the correctness of IBCH, b must be 0. $\mathcal{A}$ outputs $b' := 0$.

If the second case occurs, because of the correctness of IBCH, b must be 1. $\mathcal{A}$ outputs $b' := 1$.

If the third case occurs, in any case of $b = 0$ and $b = 1$, that contradicts to the collision-resistance of IBCH under the definition in [14]. Let us consider the case of $b = 0$. $\overline{td}$ has been generated as an IBCH secret-key for the message msg_0 as an ID. The fact that the third case occurs implies that $\mathcal{A}$ found a collision under msg_1 even though $\mathcal{A}$ is not given any secret-key for msg_1. □

Theorem 26. *TSS_{CLM} is not statistically* `INV`*.*

Proof. We consider a probabilistic adversary $\mathcal{A}$ which behaves in $\boldsymbol{Expt}_b^{\mathtt{INV}}$ w.r.t. $\mathrm{TSS}_{\mathrm{CLM}}$ as follows.

$\mathcal{A}$ arbitrarily chooses $(msg, \mathbb{T}_0, \mathbb{T}_1)$ s.t. $\mathbb{T}_0 \neq \mathbb{T}_1 \wedge |\mathbb{T}_0| \neq |\mathbb{T}_1|$ to $\mathfrak{SigLR}$, then gets $\sigma = (\cdot, \{h_i, r_i \mid i \in \mathbb{T}_b\}, \cdot, \cdot)$.

$\mathcal{A}$ correctly guesses the bit b by counting number of the randomness $\{r_i\}$. If the number is $|\mathbb{T}_0|$, $\mathcal{A}$ outputs $b' := 0$. Else if the number is $|\mathbb{T}_1|$, $\mathcal{A}$ outputs $b' := 1$. □

E Downgradable Identity-Based Trapdoor Sanitizable Signatures (DIBTSS)

E.1 Our DIBTSS Model

Syntax. Downgradable Identity-Based Trapdood Sanitizable Signatures (DIBTSS) consist of following 7 polynomial time algorithms, where $\mathtt{Ver}$ is deterministic and the others are probabilistic.

$(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$**:** The same as the one for DIBS (in Subsect. 4.1).
$sk_{id}^{\mathbb{J}} \leftarrow \mathtt{KGen}(msk, id)$**:** The same as the one for DIBS.
$sk_{id}^{\mathbb{J}'} \leftarrow \mathtt{Weaken}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, \mathbb{J}')$**:** The same as the one for DIBS.
$sk_{id'}^{\mathbb{J}'} \leftarrow \mathtt{Down}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, id')$**:** The same as the one for DIBS.
$(\sigma, td) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{J}}, id, \mathbb{J}, msg, \mathbb{T})$**:** The signing algorithm $\mathtt{Sig}$ takes a secret-key $sk_{id}^{\mathbb{J}}$ for an identity $id \in \{0,1\}^l$ and a set $\mathbb{J} \subseteq \mathbb{I}_1(id)$, a message $msg \in \{0,1\}^m$ and a set $\mathbb{T} \subseteq [1, m]$ indicating modifiable parts, then outputs a signature σ and a trapdoor td.
$(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$**:** The sanitizing algorithm $\mathtt{Sanit}$ takes an identity $id \in \{0,1\}^l$, a message $msg \in \{0,1\}^m$, a set $\mathbb{T} \subseteq [1, m]$, a signature σ, a trapdoor td, a modified message $\overline{msg} \in \{0,1\}^l$ and a modified set $\overline{\mathbb{T}} \subseteq \mathbb{T}$, then outputs a sanitized signature $\overline{\sigma}$ and a trapdoor $\overline{td}$.
$1/0 \leftarrow \mathtt{Ver}(\sigma, id, msg)$**:** The same as the one for DIBS.

We require every DIBTSS scheme to be correct.

Definition 15. *A DIBS scheme $\Sigma_{\mathrm{DIBTSS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$ is correct, if $\forall \lambda \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall m \in \mathbb{N}$, $\forall (mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$, $\forall id_0 \in \{0,1\}^l$, $\forall sk_{id_0}^{\mathbb{I}_1(id_0)} \leftarrow \mathtt{KGen}(msk, id_0)$, $\forall \mathbb{J}_0' \subseteq \mathbb{I}_1(id_0)$, $\forall sk_{id_0}^{\mathbb{J}_0'} \leftarrow \mathtt{Weaken}(sk_{id_0}^{\mathbb{I}_1(id_0)}, id_0, \mathbb{I}_1(id_0), \mathbb{J}_0)$, $\forall id_1 \in \{0,1\}^l$ s.t. $id_1 \preceq_{\mathbb{J}_0'} id_0$, $\forall sk_{id_1}^{\mathbb{J}_1} \leftarrow \mathtt{Down}(sk_{id_0}^{\mathbb{J}_0'}, id_0, \mathbb{J}_0', id_1)$, where $\mathbb{J}_1 := \mathbb{J}_0' \backslash \mathbb{I}_0(id_1), \cdots, \forall \mathbb{J}_{n-1}' \subseteq \mathbb{J}_{n-1}$, $\forall sk_{id_{n-1}}^{\mathbb{J}_{n-1}'} \leftarrow \mathtt{Weaken}(sk_{id_{n-1}}^{\mathbb{J}_{n-1}}, id_{n-1}, \mathbb{J}_{n-1}, \mathbb{J}_{n-1})$, $\forall id_n \in \{0,1\}^l$ s.t. $id_n \preceq_{\mathbb{J}_{n-1}'} id_{n-1}$, $\forall sk_{id_n}^{\mathbb{J}_n} \leftarrow \mathtt{Down}(sk_{id_{n-1}}^{\mathbb{J}_{n-1}'}, id_{n-1}, \mathbb{J}_{n-1}', id_n)$, where $\mathbb{J}_n := \mathbb{J}_{n-1}' \setminus \mathbb{I}_0(id_n)$, $\forall msg_0 \in \{0,1\}^m$, $\forall \mathbb{T}_0 \subseteq [1, m]$, $\forall (\sigma_0, td_0) \leftarrow \mathtt{Sig}(sk_{id_n}^{\mathbb{J}_n}, id_n, \mathbb{J}_n, msg_0, \mathbb{T}_0)$, $\forall msg_1 \in \{0,1\}^m$ s.t. $\forall msg_1 \in \{0,1\}^m$ s.t. $\bigwedge_{i \in [1,m] \text{ s.t. } msg_1[i] \neq msg_0[i]} i \in \mathbb{T}_0$, $\forall \mathbb{T}_1 \subseteq \mathbb{T}_0$, $\forall (\sigma_1, td_1) \leftarrow \mathtt{Sanit}(id_n, msg_0, \mathbb{T}_0, \sigma_0, td_0, msg_1, \mathbb{T}_1), \cdots, \forall msg_{n'} \in \{0,1\}^m$ s.t. $\bigwedge_{i \in [1,m] \text{ s.t. } msg_{n'}[i] \neq msg_{n'-1}[i]} i \in \mathbb{T}_{n'-1}$, $\forall \mathbb{T}_{n'} \subseteq \mathbb{T}_{n'-1}$, $\forall (\sigma_{n'}, td_{n'}) \leftarrow \mathtt{Sanit}(id_n, msg_{n'-1}, \mathbb{T}_{n'-1}, \sigma_{n'-1}, td_{n'-1}, msg_{n'}, \mathbb{T}_{n'})$, $\bigwedge_{i=0}^{n'} 1 \leftarrow \mathtt{Ver}(\sigma_i, id_i, msg_i)$.*

Security of DIBTSS. We require a DIBTSS satisfy the following seven security notions, namely (weak) EUF-CMA (EUF-CMA), signer-privacy (SP), transparency (TRN), weak privacy (wPRV), unlinkability (UNL), invisibility (INV) and strong privacy (sPRV). We introduced key-invariance for DIBS in Subsect. 5.3. We introduce it for DIBTSS. The eight security notions are defined by the following three definitions, namely Def. 16, Def. 17 and Def. 18, using the four experiments depicted in Fig. 21, Fig. 22, Fig. 23 and Fig. 24.

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A}}(1^\lambda, l)$:
    $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$.
    $(\sigma^*, id^*, msg^*) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanitizeTd}}(mpk)$, where
    $-\mathfrak{Reveal}(id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id))$ :
        $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \texttt{KGen}(msk, id)$. $sk_{id}^{\mathbb{J}} \leftarrow \texttt{Weaken}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), \mathbb{J})$.
        $\mathbb{Q}_r := \mathbb{Q}_r \bigcup \{(id, \mathbb{J})\}$. $\mathbf{Rtn}$ $sk_{id}^{\mathbb{J}}$.
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m])$:
        $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \texttt{KGen}(msk, id)$. $(\sigma, td) \leftarrow \texttt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), msg, \mathbb{T})$.
        $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}$ $\sigma$.
    $-\mathfrak{Sanitize}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m], \sigma, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
        $\mathbf{Rtn}$ $\perp$ if $(id, msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q}_s \bigvee \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,m] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (id, msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}_s$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q}_s := \mathbb{Q}_s \bigcup \{(id, \overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}$ $\overline{\sigma}$.
    $-\mathfrak{SanitizeTd}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m], \sigma, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
        $\mathbf{Rtn}$ $\perp$ if $(id, msg, \mathbb{T}, \sigma, \cdot) \notin \mathbb{Q}_s \bigvee \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i \in [1,m] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $\exists (id, msg, \mathbb{T}, \sigma, td) \in \mathbb{Q}_s$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q}_{st} := \mathbb{Q}_{st} \bigcup \{(id, \overline{msg}, \overline{\mathbb{T}})\}$. $\mathbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
    $\mathbf{Rtn}$ $0$ if $0 \leftarrow \texttt{Ver}(\sigma^*, id^*, msg^*) \bigvee_{(id,\mathbb{J}) \in \mathbb{Q}_r} id^* \preceq_{\mathbb{J}} id$
      $\bigvee_{(id,msg,\mathbb{T}) \in \mathbb{Q}_{st}} \bigwedge_{i \in [1,m] \text{ s.t. } msg^*[i] \neq msg[i]} i \in \mathbb{T}$.
    $\mathbf{Rtn}$ $1$ if $\bigwedge_{(id,msg,\cdot,\cdot,\cdot) \in \mathbb{Q}_s} (id, msg) \neq (id^*, msg^*)$. $\mathbf{Rtn}$ $0$.
```

Fig. 21. Experiments for weak EUF-CMA w.r.t. a DIBTSS scheme $\Sigma_{\mathrm{DIBTSS}} = \{\texttt{Setup}, \texttt{KGen}, \texttt{Weaken}, \texttt{Down}, \texttt{Sig}, \texttt{Sanit}, \texttt{Ver}\}$.

```
$\boldsymbol{Expt}^{\texttt{SP}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:    // $b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \texttt{Setup}(1^\lambda, l, m)$. $(mpk, msk') \leftarrow \texttt{Setup}'(1^\lambda, l, m)$.
    $\mathbf{Rtn}$ $b \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Weaken},\mathfrak{Down},\mathfrak{Sign}}(mpk, msk)$, where
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:
        $sk \leftarrow \texttt{KGen}(msk, id)$. $sk \leftarrow \texttt{KGen}'(msk', id)$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J}, \mathbb{J}' \subseteq [1,l])$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        $sk' \leftarrow \texttt{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$. $sk' \leftarrow \texttt{Weaken}'(sk, id, \mathbb{J}, \mathbb{J}')$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id, \mathbb{J}')\}$. $\mathbf{Rtn}$ $sk'$.
    $-\mathfrak{Down}(sk, id, id' \in \{0,1\}^l, \mathbb{J} \subseteq [1,l])$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        $sk' \leftarrow \texttt{Down}(sk, id, \mathbb{J}, id')$. $sk' \leftarrow \texttt{Down}'(sk, id, \mathbb{J}, id')$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id', \mathbb{J} \setminus \mathbb{I}_0(id'))\}$. $\mathbf{Rtn}$ $sk'$.
    $-\mathfrak{Sign}(sk, id, id' \in \{0,1\}^l, \mathbb{J} \subseteq [1,l], msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m])$:
        $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        $sk' \leftarrow \texttt{Down}(sk, id, \mathbb{J}, id')$. $\sigma \leftarrow \texttt{Sig}(sk, id', \mathbb{J} \setminus \mathbb{I}_0(id'), msg, \mathbb{T})$.
        $\sigma \leftarrow \texttt{Sig}'(msk', id', msg, \mathbb{T})$.
        $\mathbf{Rtn}$ $\sigma$.
```

Fig. 22. Experiments for signer-privacy w.r.t. a DIBTSS scheme Σ_{DIBTSS} and its simulation algorithms $\Sigma'_{\mathrm{DIBTSS}} = \{\texttt{Setup}', \texttt{KGen}', \texttt{Weaken}', \texttt{Down}', \texttt{Sig}', \texttt{Sanit}'\}$

```
$\boldsymbol{Expt}^{\mathtt{TRN}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   $//\ b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{San}/\mathfrak{Sig}}(mpk, msk)$, where
    $-\mathfrak{San}/\mathfrak{Sig}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m], \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
        $\mathbf{Rtn} \perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i\in[1,m] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
        $sk_{id}^{\mathbb{J}_1(id)} \leftarrow \mathtt{KGen}(msk, id)$.
        $(\sigma, td) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), msg, \mathbb{T})$. $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
$\boldsymbol{Expt}^{\mathtt{PRV}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   $//\ b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigSanLR}}(mpk, msk)$, where
    $-\mathfrak{SigSanLR}(id \in \{0,1\}^l, msg_0, msg_1 \in \{0,1\}^m, \mathbb{T} \subseteq [1,m], \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
        $\mathbf{Rtn} \perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{\beta\in\{0,1\}} \bigvee_{i\in[1,m] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
        $sk_{id}^{\mathbb{J}_1(id)} \leftarrow \mathtt{KGen}(msk, id)$. $(\sigma, td) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), msg_b, \mathbb{T})$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg_b, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
$\boldsymbol{Expt}^{\mathtt{UNL}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   $//\ b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{Sign},\mathfrak{Sanitize},\mathfrak{SanLR}}(mpk, msk)$, where
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m])$:
        $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \mathtt{KGen}(msk, id)$.
        $(\sigma, td) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), msg, \mathbb{T})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}\ (\sigma, td)$.
    $-\mathfrak{Sanitize}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m], \sigma, td, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
        $\mathbf{Rtn} \perp$ if $(id, msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigwedge \overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee_{i\in[1,m] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, \overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
    $-\mathfrak{SanLR}(id \in \{0,1\}^l, msg_0 \in \{0,1\}^m, \mathbb{T}_0 \subseteq [1,m], \sigma_0, td_0, msg_1 \in \{0,1\}^m, \mathbb{T}_1 \subseteq [1,m], \sigma_1, td_1,$
                                                          $\overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
        $\mathbf{Rtn} \perp$ if $\bigvee_{\beta\in\{0,1\}} \left[\overline{\mathbb{T}} \not\subseteq \mathbb{T}_\beta \bigvee (id, msg_\beta, \mathbb{T}_\beta, \sigma_\beta, td_\beta) \notin \mathbb{Q} \bigvee_{i\in[1,m] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}_\beta\right]$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg_b, \mathbb{T}_b, \sigma_b, td_b, \overline{msg}, \overline{\mathbb{T}})$. $\mathbf{Rtn}\ (\overline{\sigma}, \overline{td})$.
$\boldsymbol{Expt}^{\mathtt{INV}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   $//\ b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $\mathbf{Rtn}\ b' \leftarrow \mathcal{A}^{\mathfrak{SigLR},\mathfrak{SanLR}}(mpk, msk)$, where
    $-\mathfrak{SigLR}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,m])$:
        $sk_{id}^{\mathbb{I}_1(id)} \leftarrow \mathtt{KGen}(msk, id)$.
        $(\sigma, td) \leftarrow \mathtt{Sig}(sk_{id}^{\mathbb{I}_1(id)}, id, \mathbb{I}_1(id), msg, \mathbb{T}_b)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td)\}$. $\mathbf{Rtn}\ \sigma$.
    $-\mathfrak{SanLR}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T}_0, \mathbb{T}_1 \subseteq [1,m], \sigma, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1 \subseteq [1,m])$:
        $\mathbf{Rtn} \perp$ if $\bigvee_{\beta\in\{0,1\}} \left[\overline{\mathbb{T}}_\beta \not\subseteq \mathbb{T}_\beta \bigvee_{i\in[1,m] \text{ s.t. } msg_\beta[i] \neq \overline{msg}[i]} i \notin \mathbb{T}_\beta\right] \bigvee (id, msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, \cdot) \notin \mathbb{Q}$.
        $\exists (id, msg, \mathbb{T}_0, \mathbb{T}_1, \sigma, td) \in \mathbb{Q}$ for some $td$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg, \mathbb{T}_b, \sigma, td, \overline{msg}, \overline{\mathbb{T}}_b)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, \overline{msg}, \overline{\mathbb{T}}_0, \overline{\mathbb{T}}_1, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}\ \overline{\sigma}$.
```

Fig. 23. Experiments for transparency, privacy, unlinkability and invisibility w.r.t. a DIBTSS scheme $\Sigma_{\mathrm{DIBTSS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$.

```
$\boldsymbol{Expt}^{\mathsf{sPRV}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   // $b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$. $\mathbf{Rtn}$ $b' \leftarrow \mathcal{A}^{\mathfrak{Sign}, \mathfrak{San}/\mathfrak{Sig}}(mpk, msk)$, where
    ----------------------------------------------------------------
    $-\mathfrak{Sign}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1, m])$:
        $sk^{\mathbb{I}_1(id)}_{id} \leftarrow \mathtt{KGen}(msk, id)$. $(\sigma, td) \leftarrow \mathtt{Sig}(sk^{\mathbb{I}_1(id)}_{id}, id, \mathbb{I}_1(id), msg, \mathbb{T})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, msg, \mathbb{T}, \sigma, td)\}$. $\mathbf{Rtn}$ $(\sigma, td)$.
    $-\mathfrak{San}/\mathfrak{Sig}(id \in \{0,1\}^l, msg \in \{0,1\}^m, \mathbb{T} \subseteq [1, m], \sigma, td, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1, m])$:
        $\mathbf{Rtn}$ $\perp$ if $\overline{\mathbb{T}} \not\subseteq \mathbb{T} \bigvee (id, msg, \mathbb{T}, \sigma, td) \notin \mathbb{Q} \bigvee_{i \in [1,m] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T}$.
        $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg}, \overline{\mathbb{T}})$.
        $sk^{\mathbb{I}_1(id)}_{id} \leftarrow \mathtt{KGen}(msk, id)$. $(\overline{\sigma}, \overline{td}) \leftarrow \mathtt{Sig}(sk^{\mathbb{I}_1(id)}_{id}, id, \mathbb{I}_1(id), msg, \mathbb{T})$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(id, \overline{msg}, \overline{\mathbb{T}}, \overline{\sigma}, \overline{td})\}$. $\mathbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.
```

Fig. 24. Experiments for strong privacy w.r.t. a DIBTSS scheme $\Sigma_{\mathrm{DIBTSS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$.

```
$\boldsymbol{Expt}^{\mathtt{KI}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)$:   // $b \in \{0, 1\}$.
    $(mpk, msk) \leftarrow \mathtt{Setup}(1^\lambda, l, m)$.
    $\mathbf{Rtn}$ $b \leftarrow \mathcal{A}^{\mathfrak{Reveal}, \mathfrak{Weaken}, \mathfrak{Down}}(mpk, msk)$, where
    ----------------------------------------------------------------
    $-\mathfrak{Reveal}(id \in \{0,1\}^l)$:   $sk \leftarrow \mathtt{KGen}(msk, id \in \{0,1\}^l)$. $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk, id, \mathbb{I}_1(id))\}$. $\mathbf{Rtn}$ $sk$.
    $-\mathfrak{Weaken}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1, l], \mathbb{J} \subseteq [1, l])$:   $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee \mathbb{J}' \not\subseteq \mathbb{J}$.
        $sk' \leftarrow \mathtt{Weaken}(sk, id, \mathbb{J}, \mathbb{J}')$. $sk \leftarrow \mathtt{KGen}(msk, id)$. $sk' \leftarrow \mathtt{Weaken}(sk, id, \mathbb{I}_1(id), \mathbb{J}')$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id, \mathbb{J})\}$. $\mathbf{Rtn}$ $sk'$.
    $-\mathfrak{Down}(sk, id \in \{0,1\}^l, \mathbb{J} \subseteq [1, l], id' \in \{0,1\}^l)$:   $\mathbf{Rtn}$ $\perp$ if $(sk, id, \mathbb{J}) \notin \mathbb{Q} \bigvee id' \not\preceq_{\mathbb{J}} id$.
        $sk' \leftarrow \mathtt{Down}(sk, id, \mathbb{J}, id')$. $sk \leftarrow \mathtt{KGen}(msk, id')$. $sk' \leftarrow \mathtt{Weaken}(sk, id', \mathbb{I}_1(id'), \mathbb{J} \setminus \mathbb{I}_0(id'))$.
        $\mathbb{Q} := \mathbb{Q} \bigcup \{(sk', id', \mathbb{J})\}$. $\mathbf{Rtn}$ $sk'$.
```

Fig. 25. Experiments for key-invariance w.r.t. a DIBTSS scheme $\Sigma_{\mathrm{DIBTSS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$

Definition 16. *A DIBTSS scheme* Σ_{DIBTSS} *is* $\texttt{EUF-CMA}$*, if* $\forall\lambda \in \mathbb{N}$*,* $\forall l \in \mathbb{N}$*,* $\forall m \in \mathbb{N}$*,* $\forall\mathcal{A} \in \mathsf{PPTA}_\lambda$*,* $\exists\epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{\mathit{Adv}}^{\texttt{EUF-CMA}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},l}(\lambda) := \Pr[1 \leftarrow \boldsymbol{\mathit{Expt}}^{\texttt{EUF-CMA}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A}}(1^\lambda, l)] < \epsilon$*.*

Definition 17. *A DIBTSS scheme* Σ_{DIBTSS} *is statistically signer private, if for every* $\lambda \in \mathbb{N}$*, every* $l \in \mathbb{N}$*, every* $m \in \mathbb{N}$*, and every probabilistic algorithm* $\mathcal{A}$*, there exist polynomial time algorithms* $\Sigma'_{\mathrm{DIBTSS}} := \{\mathtt{Setup}', \mathtt{KGen}', \mathtt{Weaken}', \mathtt{Down}', \mathtt{Sig}'\}$ *and a negligible function* $\epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{\mathit{Adv}}^{\mathit{SP}}_{\Sigma_{\mathrm{DIBTSS}},\Sigma'_{\mathrm{DIBTSS}},\mathcal{A},l,m}(\lambda) := |\sum_{b=0}^{1}(-1)^b \Pr[1 \leftarrow \boldsymbol{\mathit{Expt}}^{\mathit{SP}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},0}(1^\lambda, l, m)]| < \epsilon$*.*

Definition 18. *Let* $\mathtt{Z} \in \{\mathtt{TRN}, \mathtt{wPRV}, \mathtt{UNL}, \mathtt{INV}, \mathtt{sPRV}\}$*. A DIBTSS scheme* Σ_{DIBTSS} *is statistically (resp. perfectly)* $\mathtt{Z}$*, if* $\forall\lambda, l, m \in \mathbb{N}$*,* $\forall\mathcal{A} \in \mathsf{PA}$*,* $\exists\epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{\mathit{Adv}}^{\mathtt{Z}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},l}(\lambda) := |\sum_{b=0}^{1}(-1)^b \Pr[1 \leftarrow \boldsymbol{\mathit{Expt}}^{\mathtt{Z}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l)]| < \epsilon$ *(resp.* $\boldsymbol{\mathit{Adv}}^{\mathtt{Z}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},l}(\lambda) = 0$*).*

Theorem 4 guarantees that the five implications among the four security notions for TSS, i.e., $\mathtt{TRN}$, $\mathtt{wPRV}$, $\mathtt{UNL}$ and $\mathtt{sPRV}$, hold. The same implications hold in DIBTSS. The following theorem can be proven in the same manner as Theorem 4.

Theorem 27. *For any DIBTSS scheme, (1)* $\mathtt{TRN}$ *implies* $\mathtt{wPRV}$*, (2)* $\mathtt{UNL}$ *implies* $\mathtt{wPRV}$*, (3)* $\mathtt{sPRV}$ *implies* $\mathtt{TRN}$*, (4)* $\mathtt{sPRV}$ *implies* $\mathtt{UNL}$*, and (5)* $\mathtt{TRN} \bigwedge \mathtt{UNL}$ *implies* $\mathtt{sPRV}$*. Note that they hold even if the security notions are perfect ones.*

Definition 19. *A DIBTSS scheme* $\Sigma_{\mathrm{DIBTSS}} = \{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$ *is statistically key-invariant, if* $\forall\lambda \in \mathbb{N}$*,* $\forall l \in \mathbb{N}$*,* $\forall m \in \mathbb{N}$*,* $\forall\mathcal{A} \in \mathsf{PA}$*,* $\exists\epsilon \in \mathsf{NGL}_\lambda$ *s.t.* $\boldsymbol{\mathit{Adv}}^{\mathit{KI}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},l,m}(\lambda) := |\sum_{b=0}^{1}(-1)^b \Pr[1 \leftarrow \boldsymbol{\mathit{Expt}}^{\mathit{KI}}_{\Sigma_{\mathrm{DIBTSS}},\mathcal{A},b}(1^\lambda, l, m)]| < \epsilon$*.*

E.2 Our DIBTSS Construction DAMACtoDIBTSS

A formal description of our DAMAC-based DIBTSS construction is divided into Fig. 26 and Fig. 27. Its security, i.e., statistical signer-privacy, statistical strong privacy, EUF-CMA, perfect privacy, perfect invisibility and statistical key-invariance are guaranteed by Theorems 28-32.

Theorem 28. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is statistically signer-private.*

Theorem 29. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is statistically* $\mathtt{sPRV}$*.*

Theorem 30. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is* $\mathtt{EUF-CMA}$ *if the* $\mathcal{D}_k$*-MDDH assumption on* $\mathbb{G}_1$ *holds and the underlying* Σ_{DAMAC} *is* $\mathtt{PR-CMA1}$*.*

Theorem 31. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is perfectly* $\mathtt{wPRV}$ *and perfectly* $\mathtt{INV}$*.*

Theorem 32. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is statistically key-invariance.*

From Theorem 27 and Theorem 29, we obtain Corollary 2.

Corollary 2. $\Omega^{\mathrm{DIBTSS}}_{\mathrm{DAMAC}}$ *is statistically* $\mathtt{TRN}$ *and statistically* $\mathtt{UNL}$*.*

```
$\mathtt{Setup}(1^\lambda, l, m)$:
    $A \leftsquigarrow \mathcal{D}_k$. $sk_{\mathrm{MAC}} \leftarrow \mathtt{Gen}_{\mathrm{MAC}}(1^\lambda, l+m)$.
    Parse $sk_{\mathrm{MAC}} = (B, \boldsymbol{x}_0, \cdots, \boldsymbol{x}_{l+m}, x)$.   $//\ B \in \mathbb{Z}_p^{n \times n'}$, $\boldsymbol{x}_i \in \mathbb{Z}_p^n$, $x \in \mathbb{Z}_p$.
    For $i \in [0, l+m]$:   $Y_i \leftsquigarrow \mathbb{Z}_p^{n \times k}$, $Z_i := (Y_i \mid \boldsymbol{x}_i)\, A \in \mathbb{Z}_p^{n \times k}$.
    $\boldsymbol{y} \leftsquigarrow \mathbb{Z}_p^{1 \times k}$, $\boldsymbol{z} := (\boldsymbol{y} \mid x)\, A \in \mathbb{Z}_p^{1 \times k}$.
    $mpk := \left([A]_1, \left\{[Z_i]_1 \mid i \in [0, l+m]\right\}, [\boldsymbol{z}]_1\right)$, $msk := (sk_{\mathrm{MAC}}, \{Y_i \mid i \in [0, l+m]\}, \boldsymbol{y})$.
    Rtn $(mpk, msk)$.
$\mathtt{KGen}(msk, id \in \{0,1\}^l)$:
    $\tau \leftarrow \mathtt{Tag}(sk_{\mathrm{MAC}}, id||1^m)$.
    Parse $\tau = ([\boldsymbol{t}]_2, [u]_2, \{[d_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\})$.
        $//\ \boldsymbol{s} \leftsquigarrow \mathbb{Z}_p^{n'}$, $\boldsymbol{t} := B\boldsymbol{s} \in \mathbb{Z}_p^n$, $d_i := h_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t}$, $u := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top \boldsymbol{t} + x \in \mathbb{Z}_p$.
    $\boldsymbol{u} := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top \boldsymbol{t} + \boldsymbol{y}^\top \in \mathbb{Z}_p^k$.
    $S \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $T := BS \in \mathbb{Z}_p^{n \times n'}$.
    $\boldsymbol{w} := \sum_{i=0}^{l+m} f_i(id||1^m)\boldsymbol{x}_i^\top T \in \mathbb{Z}_p^{1 \times n'}$, $W := \sum_{i=0}^{l+m} f_i(id||1^m) Y_i^\top T \in \mathbb{Z}_p^{k \times n'}$.
    For $i \in \mathbb{I}_1(id||1^m)$: $\boldsymbol{d}_i := h_i(id||1^m) Y_i^\top \boldsymbol{t}$, $\boldsymbol{e}_i := h_i(id||1^m)\boldsymbol{x}_i^\top T$, $E_i := h_i(id||1^m) Y_i^\top T$.
    Rtn $sk_{id}^{\mathbb{I}_1(id)} := \left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{I}_1(id||1^m)\right\}\right)$.
$\mathtt{Weaken}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id))$:
    Rtn $\perp$ if $\mathbb{J}' \not\subseteq \mathbb{J}$.
    $(sk_{id}^{\mathbb{J}})' \leftarrow \mathtt{VRnd}(sk_{id}^{\mathbb{J}}, id||1^m, \mathbb{J} \bigcup_{i=l+1}^{l+m} \{i\})$.
    Parse $(sk_{id}^{\mathbb{J}})'$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\right\}\right)$.
    Rtn $sk_{id}^{\mathbb{J}'} := \left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}' \bigcup \mathbb{K}\right\}\right)$.
$\mathtt{Down}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), id' \in \{0,1\}^l)$:
    Rtn $\perp$ if $id' \not\preceq_{\mathbb{J}} id$.
    $(sk_{id}^{\mathbb{J}})' \leftarrow \mathtt{VRnd}(sk_{id}^{\mathbb{J}}, id||1^m, \mathbb{J} \bigcup_{i=l+1}^{l+m} \{i\})$.
    Parse $(sk_{id}^{\mathbb{J}})'$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J} \bigcup \mathbb{K}\right\}\right)$.
    $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$. $\mathbb{I}^* := \mathbb{I}_1(id) \bigcap \mathbb{I}_0(id')$.
    $[u']_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$. $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
    $[\boldsymbol{w}']_2 := \left[\boldsymbol{w} - \sum_{i \in \mathbb{I}^*} \boldsymbol{e}_i\right]_2$. $[W']_2 := \left[W - \sum_{i \in \mathbb{I}^*} E_i\right]_2$.
    Rtn $sk_{id'}^{\mathbb{J}'} := \left([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2, [T]_2, [\boldsymbol{w}']_2, [W']_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{J}' \bigcup \mathbb{K}\right\}\right)$.
$\mathtt{VRnd}(var, str \in \{0,1\}^{l+m}, \mathbb{R} \subseteq [1, l+m])$:
    Parse $var$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \mid i \in \mathbb{R}\right\}\right)$.
    $\boldsymbol{s}' \leftsquigarrow \mathbb{Z}_p^{n'}$, $S' \leftsquigarrow \mathbb{Z}_p^{n' \times n'}$, $[T']_2 := [TS']_2$.
    $[\boldsymbol{w}']_2 := [\boldsymbol{w}S']_2$, $[W']_2 := [WS']_2$, $[\boldsymbol{t}']_2 := [\boldsymbol{t} + T'\boldsymbol{s}']_2$.
    $[u']_2 := [u + \boldsymbol{w}'\boldsymbol{s}']_2$, $[\boldsymbol{u}']_2 := [\boldsymbol{u} + W'\boldsymbol{s}']_2$.
    For $i \in \mathbb{R}$:
        $[\boldsymbol{e}_i']_2 := [\boldsymbol{e}_i S']_2$, $[E_i']_2 := [E_i S']_2$, $[d_i']_2 := [d_i + \boldsymbol{e}_i'\boldsymbol{s}']_2$, $[\boldsymbol{d}_i']_2 := [\boldsymbol{d}_i + E_i'\boldsymbol{s}']_2$.
    Rtn $var' := \left([\boldsymbol{t}']_2, [u']_2, [\boldsymbol{u}']_2, [T']_2, [\boldsymbol{w}']_2, [W']_2, \left\{[d_i']_2, [\boldsymbol{d}_i']_2, [\boldsymbol{e}_i']_2, [E_i']_2 \mid i \in \mathbb{R}\right\}\right)$.
```

Fig. 26. The first 4 algorithms of Our DIBTSS scheme DAMAC**to**DIBTSS (or interchangeably $\Omega_{\mathrm{DAMAC}}^{\mathrm{DIBTSS}}$) with $\{\mathtt{Setup}, \mathtt{KGen}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Sig}, \mathtt{Sanit}, \mathtt{Ver}\}$ (and a subroutine variable-randomizing algorithm $\mathtt{VRnd}$) based on a DAMAC scheme $\Sigma_{\mathrm{DAMAC}} = \{\mathtt{Gen}_{\mathrm{MAC}}, \mathtt{Tag}, \mathtt{Weaken}, \mathtt{Down}, \mathtt{Ver}\}$. Note that $\mathbb{K}$ denotes a set $[l+1, l+m]$ of successive integers.

```
$\texttt{Sig}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m])$:
    $(sk_{id}^{\mathbb{J}})' \leftarrow \texttt{VRnd}(sk_{id}^{\mathbb{J}}, id||1^m, \mathbb{J} \bigcup_{i=l+1}^{l+m}\{i\})$.
    Parse $(sk_{id}^{\mathbb{J}})'$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \;\middle|\; i \in \mathbb{J} \bigcup_{j=l+1}^{l+m}\{j\}\right\}\right)$.
    $msg' := \Phi_{\mathbb{T}}(msg)$.
    $\mathbb{I}^* := \mathbb{I}_0(1^l||msg)$. $\mathbb{I}' := \mathbb{I}_0(1^l||msg')$.
    $[u^*]_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$. $[\boldsymbol{u}^*]_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
    $[u']_2 := \left[u - \sum_{i \in \mathbb{I}'} d_i\right]_2$. $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}'} \boldsymbol{d}_i\right]_2$.
    $\sigma := \left([\boldsymbol{t}]_2, [u^*]_2, [\boldsymbol{u}^*]_2\right)$.
    $td := \left([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \;\middle|\; i \in \bigcup_{i \in \mathbb{T}}\{l+i\}\right\}\right)$.
    $\textbf{Rtn}$ $(\sigma, td)$.

$\texttt{Sanit}(id \in \{0,1\}^l, \mathbb{T} \subseteq [1,m], msg \in \{0,1\}^m, \sigma, td,$
                                $\overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq \mathbb{T})$:
    $\textbf{Rtn}$ $\perp$ if $0 \leftarrow \texttt{Ver}(\sigma, id, msg) \bigvee_{i \in [1,m] \text{ s.t. } \overline{msg}[i] \neq msg[i]} i \notin \mathbb{T}$.
    $td' \leftarrow \texttt{VRnd}(td, id||msg', \bigcup_{i \in \mathbb{T}}\{l+i\})$.
    Parse $td'$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \;\middle|\; i \in \bigcup_{i \in \mathbb{T}}\{l+i\}\right\}\right)$.
    $\overline{msg}' := \Phi_{\mathbb{T}}(\overline{msg})$.
    $\mathbb{I}^* := \mathbb{I}_0(1^l||\overline{msg})$. $\mathbb{I}' := \mathbb{I}_0(1^l||\overline{msg}')$.
    $[u^*]_2 := \left[u - \sum_{i \in \mathbb{I}^*} d_i\right]_2$. $[\boldsymbol{u}^*]_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}^*} \boldsymbol{d}_i\right]_2$.
    $[u']_2 := \left[u - \sum_{i \in \mathbb{I}'} d_i\right]_2$. $[\boldsymbol{u}']_2 := \left[\boldsymbol{u} - \sum_{i \in \mathbb{I}'} \boldsymbol{d}_i\right]_2$.
    $\overline{\sigma} := \left([\boldsymbol{t}]_2, [u^*]_2, [\boldsymbol{u}^*]_2\right)$.
    $\overline{td} := \left([\boldsymbol{t}]_2, [u']_2, [\boldsymbol{u}']_2, [T]_2, [\boldsymbol{w}]_2, [W]_2, \left\{[d_i]_2, [\boldsymbol{d}_i]_2, [\boldsymbol{e}_i]_2, [E_i]_2 \;\middle|\; i \in \bigcup_{i \in \mathbb{T}}\{l+i\}\right\}\right)$.
    $\textbf{Rtn}$ $(\overline{\sigma}, \overline{td})$.

$\texttt{Ver}(\sigma, id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
    Parse $\sigma$ as $\left([\boldsymbol{t}]_2, [u]_2, [\boldsymbol{u}]_2\right)$.
    $\boldsymbol{r} \leftsquigarrow \mathbb{Z}_p^k$. $[\boldsymbol{v}_0]_1 := [A\boldsymbol{r}]_1 \in \mathbb{G}^{k+1}$. $[v]_1 := [\boldsymbol{z}\boldsymbol{r}]_1 \in \mathbb{G}$. $[\boldsymbol{v}_1]_1 := \left[\sum_{i=0}^{l+m} f_i(id||msg) Z_i \boldsymbol{r}\right]_1 \in \mathbb{G}^n$.
    $\textbf{Rtn}$ 1 if $e\left([\boldsymbol{v}_0]_1, \begin{bmatrix} \boldsymbol{u} \\ u \end{bmatrix}_2\right) \cdot e\left([\boldsymbol{v}_1]_1, [\boldsymbol{t}]_2\right)^{-1} = e\left([v]_1, [1]_2\right)$.
    $\textbf{Rtn}$ 0 otherwise.
```

Fig. 27. The last 3 algorithms of Our DIBTSS scheme DAMAC$\texttt{to}$DIBTSS (or interchangeably $\Omega_{\text{DAMAC}}^{\text{DIBTSS}}$) with $\{\texttt{Setup}, \texttt{KGen}, \texttt{Weaken}, \texttt{Down}, \texttt{Sig}, \texttt{Sanit}, \texttt{Ver}\}$ (and a subroutine variable-randomizing algorithm $\texttt{VRnd}$) based on a DAMAC scheme $\Sigma_{\text{DAMAC}} = \{\texttt{Gen}_{\text{MAC}}, \texttt{Tag}, \texttt{Weaken}, \texttt{Down}, \texttt{Ver}\}$.

```
$\texttt{Setup}(1^\lambda, l, m)$:   $\textbf{Rtn}\ (mpk, msk) := (pk, sk) \leftarrow \texttt{KGen}'(1^\lambda, l+m)$.
$\texttt{KGen}(msk, id \in \{0,1\}^l)$:   $\textbf{Rtn}\ sk_{id}^{\mathbb{I}_1(id)} := (\sigma, td) \leftarrow \texttt{Sig}'(pk, sk, id||1^m, \mathbb{I}_1(id) \bigcup [l+1, l+m])$.
$\texttt{Weaken}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id))$:
    $\textbf{Rtn}\ \bot$ if $\mathbb{J}' \not\subseteq \mathbb{J}$. Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$.
    $\textbf{Rtn}\ sk_{id}^{\mathbb{J}'} := (\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||1^m, \mathbb{J}' \bigcup [l+1, l+m])$.
$\texttt{Down}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), id' \in \{0,1\}^l)$:
    $\textbf{Rtn}\ \bot$ if $id' \not\preceq_{\mathbb{J}} id$. Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$. $\mathbb{J}' := \mathbb{J} \bigcup [l+1, l+m] \setminus \mathbb{I}_0(id')$.
    $\textbf{Rtn}\ sk_{id'}^{\mathbb{J}'} := (\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id'||1^m, \mathbb{J}')$.
$\texttt{Sig}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m \setminus \{1^m\}, \mathbb{T} \subseteq [1, m])$:
    Parse $sk_{id}^{\mathbb{J}}$ as $(\sigma, td)$.
    $\textbf{Rtn}\ (\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}'(pk, id||1^m, \mathbb{J} \bigcup [l+1, l+m], \sigma, td, id||msg, \bigcup_{i \in \mathbb{T}} \{l+i\})$.
$\texttt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1, m])$:
    $\textbf{Rtn}\ \bot$ if $0 \leftarrow \texttt{Ver}(\sigma, id, msg) \bigvee_{i \in [1,m] \text{ s.t. } msg[i] \neq \overline{msg}[i]} i \notin \mathbb{T} \bigvee \overline{\mathbb{T}} \not\subseteq \mathbb{T}$.
    $\textbf{Rtn}\ (\overline{\sigma}, \overline{td}) \leftarrow \texttt{Sanit}'(pk, id||msg, \bigcup_{i \in \mathbb{T}} \{l+i\}, \sigma, td, id||\overline{msg}, \bigcup_{i \in \overline{\mathbb{T}}} \{l+i\})$.
$\texttt{Ver}(\sigma, id \in \{0,1\}^l, msg \in \{0,1\}^m \setminus \{1^m\})$:   $\textbf{Rtn}\ 1/0 \leftarrow \texttt{Ver}'(pk, \sigma, id||msg)$.
```

Fig. 28. A generic DIBTSS construction TSS`to`DIBTSS (or interchangeably $\Omega_{\text{TSS}}^{\text{DIBTSS}}$) with $\{\texttt{Setup}, \texttt{KGen}, \texttt{Weaken}, \texttt{Down}, \texttt{Sig}, \texttt{Sanit}, \texttt{Ver}\}$ from a TSS construction $\Sigma_{\text{TSS}} = \{\texttt{KGen}', \texttt{Sig}', \texttt{Sanit}', \texttt{Ver}'\}$.

E.3 Implication from TSS to DIBTSS (TSS`to`DIBTSS)

A generic DIBTSS construction TSS`to`DIBTSS (interchangeably $\Omega_{\text{TSS}}^{\text{DIBTSS}}$) from a TSS scheme is described in Fig. 28. Its existential unforgeability, statistical signer-privacy, transparency, weak privacy, unlinkability, invisibility and strong privacy are guaranteed by the following three theorems. The first two can be proven in the same manner as the corresponded ones for TSS`to`DIBS, i.e., Theorems 16, 17. The last one is obviously true.

Theorem 33. *$\Omega_{\text{TSS}}^{\text{DIBTSS}}$ is EUF-CMA if the underlying TSS Σ_{TSS} is EUF-CMA.*

Theorem 34. *$\Omega_{\text{TSS}}^{\text{DIBTSS}}$ is signer private if the underlying TSS Σ_{TSS} is TRN and UNL.*

Theorem 35. *For each $Z \in \{$TRN, wPRV, UNL, INV, sPRV$\}$, $\Omega_{\text{TSS}}^{\text{DIBTSS}}$ is Z if the underlying TSS Σ_{TSS} is Z.*

E.4 Implication from DIBS to DIBTSS (DIBS`to`DIBTSS)

A generic DIBTSS construction DIBS`to`DIBTSS (interchangeably $\Omega_{\text{DIBS}}^{\text{DIBTSS}}$) is described in Fig. 29. Its EUF-CMA, strong privacy, invisibility, signer-privacy and key-invariance are guaranteed by the following five theorems. The first three can be formally proven in the same manner as the corresponded ones for DIBS`to`TSS, i.e., Theorems 13, 14, 15. The last two are obviously true.

Theorem 36. *$\Omega_{\text{DIBS}}^{\text{DIBTSS}}$ is EUF-CMA if the underlying DIBS Σ_{DIBS} is EUF-CMA and key-invariant.*

```
$\texttt{Setup}(1^\lambda, l, m)$:
    $(mpk, msk) \leftarrow \texttt{Setup}'(1^\lambda, l+m, m)$.
$\texttt{KGen}(msk, id \in \{0,1\}^l)$:
    $sk_{id}^{\mathbb{I}_1(id)} := sk_{id||1^m}^{\mathbb{I}_1(id)\bigcup_{i=l+1}^{l+m}\{i\}} \leftarrow \texttt{KGen}'(msk, id||1^m)$.
$\texttt{Weaken}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), \mathbb{J}' \subseteq \mathbb{I}_1(id))$:
    Rtn $\perp$ if $\mathbb{J}' \nsubseteq \mathbb{J}$. Parse $sk_{id}^{\mathbb{J}}$ as $sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}$.
    Rtn $sk_{id}^{\mathbb{J}'} := sk_{id||1^m}^{\mathbb{J}'\bigcup_{i=l+1}^{l+m}\{i\}} \leftarrow \texttt{Weaken}(sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}, id||1^m, \mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}, \mathbb{J}'\bigcup_{i=l+1}^{l+m}\{i\})$.
$\texttt{Down}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), id' \in \{0,1\}^l)$:
    Rtn $\perp$ if $id' \npreceq_{\mathbb{J}} id$. Parse $sk_{id}^{\mathbb{J}}$ as $sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}$.
    Rtn $sk_{id'}^{\mathbb{J}'} := sk_{id'||1^m}^{\mathbb{J}'\bigcup_{i=l+1}^{l+m}\{i\}} \leftarrow \texttt{Down}(sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}, id||1^m, \mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}, id')$,
        where $\mathbb{J}' := \mathbb{J} \setminus \mathbb{I}_0(id')$.
$\texttt{Sig}(sk_{id}^{\mathbb{J}}, id \in \{0,1\}^l, \mathbb{J} \subseteq \mathbb{I}_1(id), msg \in \{0,1\}^m, \mathbb{T} \subseteq [1,m])$:
    Write $sk_{id}^{\mathbb{J}}$ as $sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}$. $msg' \leftarrow \mathit{\Phi}_{\mathbb{T}}(msg)$.
    $sk_{id||msg'}^{\mathbb{J}\bigcup\mathbb{I}_1(msg')} \leftarrow \texttt{Down}'(sk_{id||1^m}^{\mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}}, id, \mathbb{J}\bigcup_{i=l+1}^{l+m}\{i\}, id||msg')$.
    $td := sk_{id||msg'}^{\mathbb{T}} \leftarrow \texttt{Weaken}'(sk_{id||msg'}^{\mathbb{J}\bigcup\mathbb{I}_1(msg')}, id||msg', \mathbb{J}\bigcup\mathbb{I}_1(msg'), \mathbb{T})$.
    $sk_{id||msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)} \leftarrow \texttt{Down}'(sk_{id||msg'}^{\mathbb{T}}, id||msg', \mathbb{T}, msg)$.
    $\sigma := sk_{id||msg}^{\emptyset} \leftarrow \texttt{Weaken}'(sk_{id||msg}^{\mathbb{T}\setminus\mathbb{I}_0(msg)}, id||msg, \mathbb{T}\setminus\mathbb{I}_0(msg), \emptyset)$.
    Rtn $(\sigma, td)$.
$\texttt{Sanit}(id, msg, \mathbb{T}, \sigma, td, \overline{msg} \in \{0,1\}^m, \overline{\mathbb{T}} \subseteq [1,m])$:
    Rtn $\perp$ if $\overline{\mathbb{T}} \nsubseteq \mathbb{T} \bigvee_{i\in[1,m] \text{ s.t. } msg[i]\neq msg'[i]} i \notin \mathbb{T}$.
    $msg' \leftarrow \mathit{\Phi}_{\mathbb{T}}(msg)$, $\overline{msg}' \leftarrow \mathit{\Phi}_{\overline{\mathbb{T}}}(\overline{msg})$. Write $td$ as $sk_{id||msg'}^{\mathbb{T}}$.
    $sk_{id||\overline{msg}'}^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg}')} \leftarrow \texttt{Down}'(sk_{id||msg'}^{\mathbb{T}}, id||msg', \mathbb{T}, id||\overline{msg}')$.
    $\overline{td} := sk_{id||\overline{msg}'}^{\overline{\mathbb{T}}} \leftarrow \texttt{Weaken}'(sk_{id||\overline{msg}'}^{\mathbb{T}\setminus\mathbb{I}_0(\overline{msg})}, id||\overline{msg}', \mathbb{T}\setminus\mathbb{I}_0(\overline{msg}), \overline{\mathbb{T}})$.
    $sk_{id||\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})} \leftarrow \texttt{Down}'(sk_{id||\overline{msg}'}^{\overline{\mathbb{T}}}, id||\overline{msg}', \overline{\mathbb{T}}, id||\overline{msg})$.
    $\overline{\sigma} := sk_{id||\overline{msg}}^{\emptyset} \leftarrow \texttt{Weaken}'(sk_{id||\overline{msg}}^{\overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg})}, id||\overline{msg}, \overline{\mathbb{T}}\setminus\mathbb{I}_0(\overline{msg}), \emptyset)$.
    Rtn $(\overline{\sigma}, \overline{td})$.
$\texttt{Ver}(\sigma, id \in \{0,1\}^l, msg \in \{0,1\}^m)$:
    Write $\sigma$ as $sk_{id||msg}^{\emptyset}$. $\hat{msg} \leftarrow\!\!\!\sim \{0,1\}^m$.
    $\hat{\sigma} \leftarrow \texttt{Sig}'(sk_{id||msg}^{\emptyset}, id||msg, \emptyset, \hat{msg})$.
    Rtn $1/0 \leftarrow \texttt{Ver}'(\hat{\sigma}, id||msg, \hat{msg})$.
$\mathit{\Phi}_{\mathbb{T}}(msg \in \{0,1\}^m)$:  // $\mathbb{T} \subseteq [1,m]$
    $msg' := msg$. For every $i \in \mathbb{T}$ s.t. $msg[i] = 0$, let $msg'[i] := 1$.
    Rtn $msg' \in \{0,1\}^m$.
```

Fig. 29. A generic DIBTSS construction DIBStoDIBTSS (or interchangeably $\mathit{\Omega}_{\mathrm{DIBS}}^{\mathrm{DIBTSS}}$) with $\{\texttt{Setup}, \texttt{KGen}, \texttt{Weaken}, \texttt{Down}, \texttt{Sig}, \texttt{Sanit}, \texttt{Ver}\}$ from a DIBS construction $\mathit{\Sigma}_{\mathrm{DIBS}} = \{\texttt{Setup}', \texttt{KGen}', \texttt{Weaken}', \texttt{Down}', \texttt{Sig}', \texttt{Ver}'\}$

Theorem 37. $\Omega_{\mathrm{DIBS}}^{\mathrm{DIBTSS}}$ *is* `sPRV` *if the underlying DIBS* Σ_{DIBS} *is* `KI`.

Theorem 38. $\Omega_{\mathrm{DIBS}}^{\mathrm{DIBTSS}}$ *is* `INV` *if the underlying DIBS* Σ_{DIBS} *is* `KI`.

Theorem 39. $\Omega_{\mathrm{DIBS}}^{\mathrm{DIBTSS}}$ *is signer-private if the underlying DIBS* Σ_{DIBS} *is signer-private.*

Theorem 40. $\Omega_{\mathrm{DIBS}}^{\mathrm{DIBTSS}}$ *is* `KI` *if the underlying DIBS* Σ_{DIBS} *is* `KI`.