# Threshold attribute based universal designated verifier signature scheme in the standard model

Feng Cai
Xidian University
State Key Laboratory of ISN
No.2 Taibai South Road, Xi'an
China
fcai@mail.xidian.edu.cn

Wangmei Guo
Xidian University
State Key Laboratory of ISN
No.2 Taibai South Road, Xi'an
China
wangmeiguo@mail.xidian.edu.cn

Ximeng Liu
Xidian University
State Key Laboratory of ISN
No.2 Taibai South Road, Xi'an
China
snbnix@gmail.com

*Abstract:* In universal designated verifier signature scheme, signature holder can designate the signature to any desired designated verifier. Only the designated verifier can believe that the signature holder does have a valid publicly verifiable signature. Attribute based encryption is a novel public key primitive in cryptography and attribute based signature can provide a powerful way for users to control their privacy. In this paper, we propose a threshold attribute based universal designated verifier signature scheme whose security can be proven in the standard model. The security of our scheme depends on the Bilinear Diffie-Hellman (BDH) assumption.

*Key–Words:* Bilinear pairings, Attribute-based, Universal designated verifier signature, Provable secure

## 1 Introduction

Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document, which allows a user with the private key to sign the message such that anyone who possesses the public key can verify the authenticity message. It was first proposed in the original paper of Diffie and Hellman[7]. Digital signatures serve as a powerful tool. It can be used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. However, it is unsuitable for some other applications where verifier does not want other parties to present the publicly verifiable signature, such as those associated with certificates for hospital records, etc.

In recent years, attribute based cryptography has received much attention from researchers as a novel public key primitive, and many schemes have been proposed. Attribute based encryption (ABE)[18, 8] has a significant advantage over the traditional PKC since it can achieve both information security and fine-grained access control. Attribute based signatures (ABS)[9, 19] scheme provides a powerful way for user to govern their privacies. It helps to provide fine-grained access control in anonymous authentication systems. In basic ABS, a user signs with a subset of his attributes and the verification succeeds with any set of attributes that has at least $t$ common attributes with the signing attribute set. We call this scheme threshold attribute-based signature ($t$-ABS).

In universal designated verifier signature (UDVS) scheme, publicly verifiable signature was given. A signature holder can convert the publicly verifiable signature to UDVS, which is designed to a verifier. In this scenario, only designated verifier can be convinced that the message has been signed by the signer. However, any other third-party cannot believe UDVS due to verifier can use his secret key to create a valid UDVS. This UDVS signed by designated verifier is the same as the one designated to himself. Thus, one cannot distinguish a UDVS is created by the signature holder or by the designated verifier himself. When the signature holder and the signer are the same user, a universal designated signature will form a designated verifier signature.

In this paper, we consider threshold attribute based universal designated verifier signature($t$-ABUDVS) scheme. Signature holder converts the standard signature to $t$-ABUDVS with an arbitrary subset $\omega_s$ of signer attributes and subset $\omega_v$ of verifier attributes. Only when the designated verifier attribute set has an overlap at least $t_v$ with $\omega_v$, and the signature holder claims attribute set has an overlap at least $t_s$ with $\omega_s$, designated verifier can believe that the message has been signed by the signer.

### 1.1 Related Work

ABE is one of the important applications of fuzzy identity based encryption (FIBE)[18] which can be traced back to identity-based encryption[20, 4, 3]. In FIBE, the identity information is fuzzy related to the biometric information used in identification.

The identity is viewed as a set of descriptive attributes. When a message is encrypted with an attribute set $\omega$, user with private key for the attribute set $\omega'$ can decrypt the message if and only if $\omega$ and $\omega'$ have an overlap of at least $d$ attributes. There are two flavors of ABE: Ciphertext-policy attribute based encryption(CP-ABE)[2, 6] and Key-policy attribute based encryption(KP-ABE)[8]. In CP-ABE scheme, ciphertext is associated with the access structure while private key is associated with a set of attributes. In 2007, Bethencourt *et al.*[2] proposed the CP-ABE scheme, in which threshold secret sharing is used to enforce the policy during the encryption phase. KP-ABE proceeds in the dual way, where ciphertext is associated with a set of attributes and private key is associated with access structure. In 2008 Guo and Zeng[9] tried to extend Identity-based signature[20, 10, 17] to propose the ABS scheme, in which the signer is associated with a set of attributes instead of a single identity string. Subsequently, Yang *et al.*[24] introduced a new cryptographic primitive called fuzzy identity based signature(FIBS), which is analogous to FIBE. They also applied their construction to secure biometric authentication in [23]. Shahandashti and Safavi-Naini[19] proposed a threshold attribute-based signature construction. Later on, Li *et al.*[13] proposed a new construction of ABS supporting flexible threshold predicate. Meanwhile, Khader[12] drawn another concept called attribute-based group signature, which allows a verifier to request a signature from a member of a group who possesses certain attributes, and the signature should prove ownership of certain properties. Other notable ABS schemes include attribute ring signature[14], and policy-based ABS in the generic model[16].

In 2003, Steinfeld *et al.*[21] first introduced the concept of the universal designated verifier signature, in which designated verifier can verify the message signed by the signer, but unable to convince anyone else of this fact. Then, Steinfeld *et al.*[22] showed how to obtain a universal designate verifier signature from the classical Schnorr/RSA signature scheme. Zhang *et al.*[25] proposed the first UDVS without random oracles and Huang *et al.*[11] proposed a UDVS scheme without the random oracles based on Waters' signature scheme. Cao and Cao[5] proposed the identity based universal designated verifier signature scheme whose security can be proven in the standard model under computational Diffie-Hellmen assumption.

### 1.2 Our contributions

In this article, we define threshold attribute based universal designated verifier signature scheme, which combines the functionalities of attribute-based signature and universal designated verifier signature scheme. We then formalize the security model of $t$-ABUDVS and propose the construction of $t$-ABUDVS scheme. We prove that the proposed scheme is secure in the standard model. The distinguisher $\mathcal{D}$ against this scheme can have non-negligible advantage in the model of the non-transferability.

### 1.3 Organization

The remainder of the paper is organized as follows. Some concepts about bilinear pairing and complexity assumptions are given in Section 2. We present the formal models in Section 3. Then security properties of $t$-ABUDVS are presented in Section 4. In Section 5, we give the specific construction of the $t$-ABUDVS scheme. We prove the security under the standard model for $t$-ABUDVS in Section 6. Finally, we conclude the paper with a discussion in Section 7.

## 2 Preliminaries

In this section, we will briefly review the properties of bilinear map and some complexity assumptions.

### 2.1 Bilinear Map

Let $\mathbb{G}$ and $\mathbb{G}_T$ denote two cyclic groups of prime order $p$ with the multiplication. Let $g$ be a generator of $\mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear map with the following properties:

1. Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$, for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy: $e(g, g) \neq 1$.
3. Computability: There is efficient algorithm to compute bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

Notice that the map $e$ is symmetric, since $e(u^a, v^b) = e(u, v)^{ab} = e(u^b, v^a)$.

### 2.2 Complexity Assumptions

The security of our scheme will be reduced to the hard problem in which the signature is constructed. We briefly review the definition of the bilinear Diffie-Hellman problem.

**Definition 1** *Bilinear Diffie-Hellman (BDH) problem: Given $g, g^a, g^b, g^c \in \mathbb{G}$ for some unknown $a, b, c \in Z_p$, compute out $w = e(g, g)^{abc} \in \mathbb{G}_T$.*

**Definition 2** *We say that the $(\epsilon, t)$-BDH assumption holds in a group $\mathbb{G}$ if no algorithm running in time at most $t$ can solve the BDH assumption with probability at least $\epsilon$.*

# 3 Formal Models of $t$-ABUDVS

In this section, we give a formal model of threshold attribute based universal designated verifier signature scheme. Our $t$-ABUDVS scheme consists of the following algorithms: $t$-ABUDVS=(Setup , Extract, PS, PV, DS, DV, Sim).

**Setup**: The algorithm takes as input security parameter $1^\lambda$ and outputs the public parameters *params* of the scheme and a master key. The master entity publishes *params* and keeps the master secret key.

**Extract**: Given an attributes set $\omega_u$, the master secret key and the *params*. This algorithm generates the private key which is associated with attributes set $\omega_u$. The PKG will use the algorithm to generate private key in the scheme and distribute the private keys to their respective owners.

**Sign (PS)**: Given the public parameters *params*, message $m$, and signers private key $d_s$ with its attribute set $\omega_s$, this algorithm outputs the signature $\sigma$ on message $m$.

**Public verification (PV)**: This algorithm takes as input public parameters *params*, the attribute $\omega'_s$ such that $|\omega'_s \cap \omega_s| \geq k_s$, the message $m$ and a valid signature $\sigma$ of the message $m$. The algorithm outputs $acc$ if $\sigma$ is a valid signature on $m$ and outputs $rej$ otherwise.

**Designation (DS)**: This algorithm takes as input the public parameters *params*, designated verifier $V$'s attributes set $\omega_v$, a valid signature $\sigma$ signed by signer $S$, and outputs the designated verifier signature $\sigma_{sv}$ for $m$.

**Designated verification (DV)**: This algorithm takes as input the public parameters, the designated verifiers secret key $d_v$ , the signed message $m$, the designate signature $\sigma_{sv}$ and the attribute set $\omega'_s$ and $\omega'_v$ such that $|\omega'_s \cap \omega_s| \geq k_s$ and $|\omega'_v \cap \omega_v| \geq k_v$, respectively, outputs the verification decision $c \in \{acc, rej\}$.

**Simulation (Sim)**: This algorithm takes as input the public parameters, signer's attributes set $\omega_s$, the designated verifiers secret key $d_v$ and the message $m$, output the designated verifier signature $\bar{\sigma}_{sv}$ which designated to himself.

## 3.1 Consistency

In [11], Huang *et al.* proposed a UDVS scheme satisfied three consistencies. In addition to the above algorithms, we also require our $t$-ABUDVS scheme should satisfy three consistencies.

(1) PV consistency: this property requires that standard signature produced by the sign algorithm is accepted as a valid signature by the public verification algorithm, i.e:

$$\Pr[PV(params, \omega'_s, m, PS(params, d_s, m)) = acc] = 1.$$

(2) DV consistency of DS: this property requires that DV signature produced by the DS algorithm is accepted as a valid signature by the designated verification algorithm, i.e:

$$\Pr[DV(params, \omega'_s, \omega'_v, d_v, m, DS(params, \omega_s, \omega_v, \sigma, m)) = acc] = 1.$$

(3) DV consistency of Sim : this property requires that DV signature produced by the Sim algorithm is accepted as a valid signature by the designated verification algorithm, i.e:

$$\Pr[DV(params, \omega'_s, \omega'_v, d_v, m, Sim(params, \omega_s, d_v, m)) = acc] = 1.$$

# 4 Security properties of $t$-ABUDVS

## 4.1 Unforgeability

We say that $t$-ABUDVS scheme is secure against existential forgery on adaptively choose message and attributes set attracts, if there is no polynomial time algorithm $\mathcal{A}$ has non-negligible advantage against a challenger $\mathcal{B}$ in the following game.

**Setup**: The challenger $\mathcal{B}$ runs the Setup algorithm to obtain both the public parameters *params* and the master key. The *params* is given to the adversary while the master key is kept secret from $\mathcal{A}$.

**Queries**: The adversary adaptively makes a number of different queries to the challenger. Each query can be one of the following:

**-Extract queries**: The adversary asks for the private key of the attribute set $\omega_u$. The adversary responds by running the Extract algorithm. $\mathcal{B}$ returns the private key to the adversary.

**-Sign queries**: The adversary asks for the private key of the attribute set $\omega_u$ on $m$. $\mathcal{B}$ return a signature which is obtained by running Sign algorithm.

**-Designation queries**: The adversary asks for the designation verifier signature which is generated by the Designation algorithm and the message $m$ under the attribute set $(\omega_s, \omega_v)$, where $\omega_s$ is the signers attributes set and $\omega_v$ is the verifiers attributes set. Firstly, $\mathcal{B}$ runs the Sign algorithm to generate the standard signature $\sigma$ on $m$. Then $\mathcal{B}$ runs the Designation algorithm to generate the universal designated verifier signature $\sigma_{sv}$. Finally, $\mathcal{B}$ returns the $\sigma_{sv}$ to $\mathcal{A}$ as the answer.

**-Simulation queries**: $\mathcal{A}$ can ask the designated verifier signature $\bar{\sigma}_{sv}$ which is generated by the Simulation algorithm and the message $m$ under the attributes set $(\omega_s, \omega_v)$, where $\omega_s$ is the signers attributes set and $\omega_v$ is the verifiers attributes set chosen by $\mathcal{A}$. $\mathcal{B}$ runs the Simulation algorithm to obtain the designed verifier signature $\bar{\sigma}_{sv}$, which is returned to $\mathcal{A}$ as the answer to response the query.

**-Designated verification queries**: $\mathcal{A}$ can ask whether the universal designated verifier signature $\sigma_{sv}$ under the attributes set $(\omega_s, \omega_v)$ is valid. The attributes set $(\omega'_s, \omega'_v)$ was chosen by $\mathcal{A}$. In response, $\mathcal{B}$ will run Designated verification algorithm and return the decision $c \in \{acc, rej\}$ to $\mathcal{A}$.

**Forgery**: the adversary outputs a message $m^*$, the attributes set $\omega_s^*$ from signer and the attribute set $\omega_v^*$ from designed verifier.

We say $\mathcal{A}$ win the game if the following hold:

1) For all Extract queried sets of attributes $\omega_s$, we have $|\omega_s^* \cap \omega_s| < k_s$.

2) For all Sign queried pair $(\omega_s, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$, or $m \neq m^*$.

3) For all Designation queried or Simulation queried triple $(\omega_s, \omega_v, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$, $|\omega_v^* \cap \omega_v| < k_v$, or $m \neq m^*$.

4) $\sigma_{sv}^*$ is a valid designation signature on $m^*$ if $DV(\omega_s^*, \omega_v^*, d_v^*, m^*, \sigma_{DV}^*) = acc$.

If no polynomial adversary has a considerable advantage in the above game, we say that the $t$-ABUDVS scheme is existentially unforgeable against chosen message and attribute set attack, or EUF-CMAA-secure for short. The advantage of adversary $Adv_{t-ABUDVS}^{EUF-CMAA}(\mathcal{A})$ is defined to be the probability of success in the above game.

**Definition 3** *We say an attacker $\mathcal{A}$ can $(t, q_e, q_{PS}, q_{DS}, q_{Sim}, q_{DV})$-break the $t$-ABUDVS scheme if $\mathcal{A}$ run in time at most $t$, make at most $q_e$ Extract queries, $q_{PS}$ Sign queries, $q_{DS}$ Designated queries, $q_{Sim}$ Simulation queries, $q_{DV}$ Designated Verification queries and $Adv_{t-ABUDVS}^{EUF-CMAA}(\mathcal{A})$ is at least $\epsilon$.*

### 4.2 Non-transferability

We say a $t$-ABUDVS scheme, which consists of seven algorithms (Setup , Extract, PS, PV, DS, DV, Sim), is secure against adaptively chosen message and attributes set attacks, if there is no polynomial time distinguisher $\mathcal{D}$ has non-negligible advantage against simulator $\mathcal{C}$ in the following game.

**Setup**: The simulator $\mathcal{C}$ runs the Setup algorithm to obtain the public parameters *params* and the master key. The *param* is given to the distinguisher $\mathcal{D}$ while the master key is kept secret.

**Phase 1**: $\mathcal{D}$ can submit Extract, Sign, Designated, Simulation and Designated Verification queries as defined in the model of unforgeability. The simulator $\mathcal{C}$ responses to these queries as same as defined in the unforgeability model.

**Challenge**: When the distinguisher $\mathcal{D}$ decides the first phase is over. He submits $\omega_s^*, \omega_v^*, m^*$ to $\mathcal{C}$ as the challenge with constrains:

1) For all Extract queried sets of attributes $\omega_s$, we have $|\omega_s^* \cap \omega_s| < k_s$.

2) For all Sign queried pair $(\omega_s, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$, or $m \neq m^*$.

3) For all Designation queried or Simulation queried triple $(\omega_s, \omega_v, m)$, we have $|\omega_s^* \cap \omega_s| < k_s$, $|\omega_v^* \cap \omega_v| < k_v$, or $m \neq m^*$.

As response, the simulator $\mathcal{C}$ chooses a random bit $b \in \{0, 1\}$. If $b = 0$, $\mathcal{C}$ runs Designated algorithm and returns $\sigma_{sv}$ to $\mathcal{D}$. Otherwise, $\mathcal{C}$ runs Simulation algorithm and returns $\bar{\sigma}_{sv}$ to $\mathcal{D}$.

**Phase 2**: Upon receiving the challenge signature, the distinguisher can submit the more Extract, Sign, Designated, Simulation and Designated verification queries with constrains:

1) For all Extract queried sets of attributes $\omega_s$, we have $|\omega_s^* \cap \omega_s| < k_s$.

2) For all Sign queried pair $(\omega_s^*, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$, or $m \neq m^*$.

3) For all Designation queried or Simulation queried triple $(\omega_s^*, \omega_v^*, m)$, we have $|\omega_s^* \cap \omega_s| < k_s$, $|\omega_v^* \cap \omega_v| < k_v$, or $m \neq m^*$.

**Guess**: Finally, the distinguisher $\mathcal{D}$ outputs a guess $b'$. The adversary wins the game if $b = b'$.

The advantage of an adaptively chosen message and attribute set distinguish $\mathcal{D}$ in the above game is defined as $Adv_{t-ABUDVS}^{TRANS-CMAA}(\mathcal{D}) = |\Pr[b' = b] - \frac{1}{2}|$.

**Definition 4** *We say a $t$-ABUDVS scheme is non-transferable against a $(t, q_e, q_{PS}, q_{DS}, q_{Sim}, q_{DV})$ adaptively chosen message and attributes set distinguisher $\mathcal{D}$, if $Adv_{t-ABUDVS}^{TRANS-CMAA}(\mathcal{D})$ is negligible after making at most $q_e$ Extract queries, $q_{PS}$ Sign queries, $q_{DS}$ Designated queries, $q_{Sim}$ Simulation queries, $q_{DV}$ Designated Verification queries in time $t$.*

## 5 Construction

In this section, we will construct threshold attribute based universal designated verifier signature scheme in the standard model. We give the concrete construction of $t$-ABUDVS scheme at first. Then we analyze the consistency of our scheme.

The concrete construction is as follows:

**Setup**: First, choose two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order $p$ such that pairing

$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be constructed and pick a generator $g$ of $\mathbb{G}$. Then, randomly choose number $\alpha \in Z_p^*$, calculate $g_1 = g^\alpha$ and pick $g_2 \in \mathbb{G}$ randomly. Next, choose $t_1, \cdots, t_{n+1}$ uniformly at random from $\mathbb{G}$. Let $N$ be the set $\{1, \cdots, n+1\}$ and we define a function $T$ as: $T(x) = g_2^{x^n} \prod_{j=1}^{n+1} t_j^{\Delta_{j,N}(x)}$.

Next, select random values $v'$ and a vector $\mathbf{V} = (v_1, \cdots, v_k)$ whose elements are chosen from $\mathbb{G}$ randomly, and set the degree of the polynomial as $d_u - 1$ such that $Q_u(0) = 1$. The public parameters of the system are

$$params = (\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, t_1, \cdots, t_{n+1}, \mathbf{V}, Q_u),$$

and the master key is given by

$$\text{MSK} = g_2^\alpha.$$

**Extract**: Let $\omega_u$ be the set of attributes, pick random $x_u \in Z_p$ and compute the public parameters as $pk_u = e(g_1, g_2)^{x_u}$. Choose a $k_u - 1$ degree polynomial such that $q_u(0) = x_u$. Pick random $r_{u,i} \in Z_p$ and compute private key as $d_u = (d_{u,1}^{(i)}, d_{u,2}^{(i)})_{i \in \omega_u}$, where $d_{u,1}^{(i)} = g_2^{\alpha q_u(i)} T(i)^{r_{u,i}}$, $d_{u,2}^{(i)} = g^{r_{u,i}}$.

**Sign:** Let $\omega_u$ be the set of attributes and $m = (\mu_1, \cdots, \mu_m)$ be a message represented by bit string. Let $M = (1, \cdots, m)$ be the set of indices of the string such that $m[k] = \mu_k$, for $k \in M$, i.e., $m[k]$ is the $k$th bit of $m$. Choose random $r_m \in Z_p$ and compute:

$$\sigma_u = \{\sigma_{u,1}^{(i)}, \sigma_{u,2}^{(i)}, \sigma_{u,3}^{(i)}\}_{i \in \omega_u},$$

where $\sigma_{u,1}^{(i)} = g_2^{\alpha q_u(i)} T(i)^{r_{u,i}} (v' \prod_{k=1}^m v_j^{\mu_j})^{r_{m,i}}$, $\sigma_{u,2}^{(i)} = g^{r_{u,i}}$, $\sigma_{u,3}^{(i)} = g^{r_{m,i}}$.

**Verify:** To verify a signature $\sigma_u = \{\sigma_{u,1}^{(i)}, \sigma_{u,2}^{(i)}, \sigma_{u,3}^{(i)}\}_{i \in \omega_u}$ against attribute set $\omega_u'$, where $|\omega_u \cap \omega_u'| \geq k_u$ and a message $m$. Choose an arbitrary $k_u$-elements subset $S$ of $\omega_u \cap \omega_u'$, and verify that:

$$\prod_i \left( \frac{e(\sigma_{u,1}^{(i)}, g)}{e(T(i), \sigma_{u,2}^{(i)}) e(v' \prod_{j=1}^m v_j^{\mu_j}, \sigma_{u,3}^{(i)})} \right)^{\Delta_{i,S}(0)} = e(g_1, g_2)^{x_u}.$$

**Designation:** Let $\omega_s$ and $\omega_v$ be the signer attributes set and verifier attributes set, respectively. Given a message signature pair $(m, \sigma)$, where $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, the signature holder (SH) selects $r_{s,i}', r_{v,i,j}', r_{m,i,j}' \in Z_p$ at random, and computes

$$\sigma_{sv} = (\{\sigma_{sv,1}^{(i,j)}\}, \{\sigma_{sv,2}^{(i,j)}\}, \{\sigma_{sv,3}^{(i,j)}\}, \{\sigma_{sv,4}^{(i,j)}\})_{i \in \omega_s, j \in \omega_v},$$

where

$\sigma_{sv,1}^{(i,j)} = (\sigma_{u,1}^{(i)})^{Q_v(j)} T(j)^{r_{v,i,j}'} T(i)^{r_{s,i}'} (v' \prod_{k=1}^m v_j^{\mu_j})^{r_{m,i,j}'}$, $\sigma_{sv,2}^{(i,j)} = (\sigma_{u,2}^{(i)})^{Q_v(j)} g^{r'_{s,i}}$, $\sigma_{sv,3}^{(i,j)} = \sigma_{u,3}^{Q_v(j)} g^{r'_{m,i,j}}$, and $\sigma_{sv,4}^{(i,j)} = g^{r'_{v,i,j}}$.

**Designated verification:** Given a designated verifier signature $\sigma_{sv} = (\{\sigma_{sv,1}^{(i,j)}\}, \{\sigma_{sv,2}^{(i,j)}\}, \{\sigma_{sv,3}^{(i,j)}\}, \{\sigma_{sv,4}^{(i,j)}\})_{i \in \omega_s, j \in \omega_v}$ against an attributes set $\omega_s'$, $\omega_v'$, where $|\omega_s \cap \omega_s'| \geq k_s$, $|\omega_v \cap \omega_v'| \geq k_v$.

$$\prod_j \prod_i \left( \begin{array}{l} e(\sigma_{sv,1}^{(i,j)}, g) \\ \cdot e(T(j)^{Q_s(i)}, d_{v,2}^{(i)}) \\ \cdot e(T(i), \sigma_{sv,2}^{(i,j)})^{-1} \\ \cdot e(v' \prod_{j=1}^m v_j^{\mu_j}, \sigma_{sv,3}^{(i,j)})^{-1} \\ \cdot e(T(j), \sigma_{u,4}^{(i,j)})^{-1} \\ \cdot e((d_{v,1}^{(i)})^{Q_s(i)}, g)^{-1} \end{array} \right)^{\Delta_{i,S}(0)\Delta_{j,S'}(0)} = \frac{e(g_1, g_2)^{x_s}}{e(g_1, g_2)^{x_v}}.$$

**Simulation:** Given the signers attributes sets, the message $m$ and the verifiers secret key $\bar{d}_v = (g_2^{\alpha q_v(j)} T(j)^{r_{v,j}}, g^{r_{v,j}})_{j \in \omega_v}$, the verifier V selects $\bar{r}_{s,i,j}', \bar{r}_{m,i,j}', \bar{r}_{v,j}' \in Z_p$ at random, then computes $\bar{\sigma}_{sv,2}^{(i,j)} = g^{\bar{r}'_{s,i,j}}$, $\bar{\sigma}_{sv,3}^{(i,j)} = g^{\bar{r}'_{m,i,j}}$, $\bar{\sigma}_{sv,4}^{(i,j)} = g^{\bar{r}_{v,j} Q_s(i)} g^{\bar{r}'_{v,j}}$, and $\bar{\sigma}_{sv,1}^{(i,j)} = g_2^{\alpha Q_s(i) q_v(j)} T(j)^{\bar{r}_{v,j} Q_s(i) + \bar{r}'_{v,j}} T(i)^{\bar{r}'_{s,i,j}} (v' \prod_{k=1}^m v_j^{\mu_j})^{\bar{r}'_{m,i,j}}$. The universal designated verifier signature generated by the verifier is

$$\bar{\sigma}_{sv} = (\{\bar{\sigma}_{sv,1}^{(i,j)}\}, \{\bar{\sigma}_{sv,2}^{(i,j)}\}, \{\bar{\sigma}_{sv,3}^{(i,j)}\}, \{\bar{\sigma}_{sv,4}^{(i,j)}\})_{i \in \omega_s, j \in \omega_v}.$$

**Consistency:**

1. PV consistency: If $\sigma_u = \{\sigma_{u,1}^{(i)}, \sigma_{u,2}^{(i)}, \sigma_{u,3}^{(i)}\}_{i \in \omega_u}$ is publicly verifiable signature generated by the Sign algorithm, then

$$\prod_i \left( \frac{e(\sigma_{u,1}^{(i)}, g)}{e(T(i), \sigma_{u,2}^{(i)}) e(v' \prod_{j=1}^m v_j^{\mu_j}, \sigma_{u,3}^{(i)})} \right)^{\Delta_{i,S}(0)}$$

$$= \prod_i \left( \frac{e(g_2^{\alpha q_u(i)} T(i)^{r_{u,i}} (v' \prod_{k=1}^m v_j^{\mu_j})^{r_{m,i}}, g)}{e(T(i), g^{r_{u,i}}) e(v' \prod_{j=1}^m v_j^{\mu_j}, g^{r_{m,i}})} \right)^{\Delta_{i,S}(0)}$$

$$= \prod_i \left( e(g_2^{\alpha q_u(i)}, g) \right)^{\Delta_{i,S}(0)}$$

$$= e(g_1, g_2)^{x_u}.$$

Therefore

$$\Pr[PV(params, \omega_s', m, PS(params, d_s, m)) = acc] = 1.$$

2. DV consistency of DS: if the designated verifier signature $\sigma_{sv} = (\{\sigma_{sv,1}^{(i,j)}\}, \{\sigma_{sv,2}^{(i,j)}\}, \{\sigma_{sv,3}^{(i,j)}\}, \{\sigma_{sv,4}^{(i,j)}\})_{i\in\omega_s, j\in\omega_v}$ is generated by the DS algorithm, then

$$\prod_j \prod_i \begin{pmatrix} e(\sigma_{sv,1}^{(i,j)}, g) \\ \cdot e(T(j)^{Q_s(i)}, d_{v,2}^{(i)}) \\ \cdot e(T(i), \sigma_{sv,2}^{(i,j)})^{-1} \\ \cdot e(v' \prod_{j=1}^m v_j^{\mu_j}, \sigma_{sv,3}^{(i,j)})^{-1} \\ \cdot e(T(j), \sigma_{u,4}^{(i,j)})^{-1} \\ \cdot e((d_{v,1}^{(i)})^{Q_s(i)}, g)^{-1} \end{pmatrix}^{\Delta_{i,S}(0)\Delta_{j,S'}(0)}$$
$$= \prod_j \prod_i \left( \frac{e(g_2^{\alpha q_s(i) Q_v(j)}, g)}{e(g_2^{\alpha q_v(j) Q_s(i)}, g)} \right)^{\Delta_{i,S}(0)\Delta_{j,S'}(0)}$$
$$= \frac{e(g_1, g_2)^{x_s}}{e(g_1, g_2)^{x_v}}$$

Therefore,

$$\Pr[DV(params, \omega_s', \omega_v', d_v, m, DS(params, \omega_s, \omega_v, \sigma, m)) = acc] = 1.$$

3. DV consistency of Sim: if the simulation algorithm generated signature

$$\bar{\sigma}_{sv} = (\{\bar{\sigma}_{sv,1}^{(i,j)}\}, \{\bar{\sigma}_{sv,2}^{(i,j)}\}, \{\bar{\sigma}_{sv,3}^{(i,j)}\}, \{\bar{\sigma}_{sv,4}^{(i,j)}\})_{i\in\omega_s, j\in\omega_v},$$

then

$$\prod_j \prod_i \begin{pmatrix} e(\bar{\sigma}_{sv,1}^{(i,j)}, g) \\ \cdot e(T(j)^{Q_s(i)}, d_{v,2}^{(i)}) \\ \cdot e(T(i), \bar{\sigma}_{sv,2}^{(i,j)})^{-1} \\ \cdot e(v' \prod_{j=1}^m v_j^{\mu_j}, \bar{\sigma}_{sv,3}^{(i,j)})^{-1} \\ \cdot e(T(j), \sigma_{u,4}^{(i,j)})^{-1} \\ \cdot e((d_{v,1}^{(i)})^{Q_s(i)}, g)^{-1} \end{pmatrix}^{\Delta_{i,S}(0)\Delta_{j,S'}(0)}$$
$$= \prod_j \prod_i \left( \frac{e(g_2^{\alpha Q_s(i) q_v(j)}, g)}{e(g_2^{\alpha Q_v(j) q_s(i)}, g)} \right)^{\Delta_{i,S}(0)\Delta_{j,S'}(0)}$$
$$= \frac{e(g_1, g_2)^{x_v}}{e(g_1, g_2)^{x_s}}$$

Therefore,

$$\Pr[DV(params, \omega_s', \omega_v', d_v, m, Sim(params, \omega_s, d_v, m)) = acc] = 1.$$

# 6 Security

In this section, we will show the security property of $t$-ABUDVS scheme by giving the following two theorems. Theorem 5 shows that $t$-ABUDVS scheme is unforgeable against adaptively chosen message and attributes set attracts. Theorem 6 shows that $t$-ABUDVS scheme is non-transferable against adaptively chosen message and attributes set distinguisher.

**Theorem 5** *If the $(\epsilon, t)$-BDH assumption holds, then our threshold attribute based universal designated verifier signature scheme is $(\epsilon', t')$-secure against adaptively chosen message and attributes set attacks, where*

$$\epsilon' \geq \frac{\epsilon}{4(n_m+1)(q_s + q_{DS} + q_{sim} + q_{DV}) p^{2n_\omega}},$$

$$\begin{aligned} t' = t + \mathcal{O}((n_\omega q_e + n_\omega \cdot n_m(q_s + q_{DS}) \\ + n_\omega^2 \cdot n_m q_{sim})\tau + n_\omega^2 q_{DV} t_k \\ + ((q_e + q_s + q_{DS})n_\omega + (q_{sim} + q_{DV})n_\omega^2)t_e \\ + n_\omega^2 q_{DV} t_u), \end{aligned}$$

*and $\tau, t_e$ are the time necessary to do a multiplication and a exponentiation in $\mathbb{G}$, respectively. $t_k$ is the time for a multiplication in $\mathbb{G}_T$ and $t_u$ is the time for pairing operation in $(\mathbb{G}, \mathbb{G}_T)$.*

**Proof**: Suppose there exists an attacker $\mathcal{A}$ who can $(t, q_e, q_{PS}, \ q_{DS}, q_{Sim}, q_{DV})$-break the $t$-ABUDVS scheme, then we can construct an algorithm $\mathcal{B}$ which will be used to solve the BDH problem. Such a simulation can be created in the following way:

**Setup:** The challenger assigns the public parameters as follows: $g_1 = g^a$ , $g_2 = g^b$. Choose a random $k \in \{0, \cdots, q\}$ , and random numbers $x', x_1, \cdots, x_q$ in the interval $\{0, \cdots, 2l-1\}$. Then chooses a random $n$ degree polynomial $f(x)$ and an $n$ degree polynomial $u(x)$ such that $\forall x \ u(x) = -x^n$ if and only if $x \in \alpha$. $\mathcal{B}$ sets $t_i = g_2^{u(i)} g^{f(i)}$, for $i$ from 1 to $n$. Since $t_i$ is chosen independently at random, we have $T(i) = g_2^{i^n} \prod_{j=1}^{n+1} \left(g_2^{u(j)} g^{f(j)}\right)^{\Delta_{j,N}(i)} = g_2^{i^n + u(i)} g^{f(i)}$. It also chooses additional random exponents $z', z_1, \cdots, z_q \in Z_p$ such that $v' = g_2^{x' - l_m k'_m} g^{z'}, v_k = g_2^{x_k} g^{z_k}$, for $1 \leq k \leq q$.

To make the notion easy, we define two functions $F(m)$ and $J(m)$ as follows,

$$F(m) = x' - k'l - \sum_j x_j m_j,$$

$$J(m) = z' + \sum_j z_j m_j.$$

The master secret key will be $g_2^{\alpha} = g_2^{a} = g^{ab}$ and the following equations hold,

$$v' \prod_{j \in M} v_j^{m_j} = g_2^{F(m)} g^{J(m)}.$$

**Queries:** When the adversary is running, Extract queries, Sign queries, Designation queries, Simulation queries and DV queries are likely to occur. $\mathcal{B}$ answers these in the following way:

**-Extract queries:** Consider a query for the private key of attributes sets $\Gamma$, $\Gamma'$ and $S$, where $|\Gamma'| = d-1$, $S = \Gamma' \cup \{0\}$. $i^n + u(i) \neq 0$, since $i \notin \omega_u$. We define the private key, where $\lambda_i$ and $r_{u,i}$ are randomly chosen in $Z_p$. We also define the $k_u - 1$ degree polynomial $q_u(x)$ as $q_u(i) = \lambda_i$, where $q(0) = c$.

Next we compute the private key as follows:

$$\begin{aligned}
d_{u,1}^{(i)} &= \Big(\prod\nolimits_{k \in \Gamma'} g_2^{\lambda_j \Lambda_{j,S}(i)}\Big) \\
&\quad \cdot \left(g_1^{-\frac{f(i)}{i^n+u(i)}} \big(g_2^{i^n+u(i)} g^{f(i)}\big)^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)}, \\
d_{u,2}^{(i)} &= \left(g^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)} \\
&= \left(g_1^{-\frac{1}{i^n+u(i)}} g^{r'_{u,i}}\right)^{\Delta_{0,S}(i)}.
\end{aligned}$$

We claim that such construction is valid response to this private key query. To see this, let $r_i = (r'_{u,i} - \frac{\alpha}{i^n+u(i)})^{\Delta_{0,S}(i)}$, we have

$$\begin{aligned}
d_{u,1}^{(i)} &= \Big(\prod\nolimits_{k \in \Gamma'} g_2^{\lambda_j \Lambda_{j,S}(i)}\Big) \\
&\quad \cdot \left(g_1^{-\frac{f(i)}{i^n+u(i)}} \big(g_2^{i^n+u(i)} g^{f(i)}\big)^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)} \\
&= \Big(\prod\nolimits_{k \in \Gamma'} g_2^{\lambda_j \Lambda_{j,S}(i)}\Big) \\
&\quad \cdot \left(g^{-\frac{\alpha f(i)}{i^n+u(i)}} \big(g_2^{i^n+u(i)} g^{f(i)}\big)^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)} \\
&= \Big(\prod\nolimits_{k \in \Gamma'} g_2^{\lambda_j \Lambda_{j,S}(i)}\Big) \\
&\quad \cdot \left(g_2^{\alpha} \big(g_2^{i^n+u(i)} g^{f(i)}\big)^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)} \\
&= \Big(\prod\nolimits_{k \in \Gamma'} g_2^{\lambda_j \Lambda_{j,S}(i)}\Big) g_2^{\alpha \Delta_{0,S}(i)} (T(i))^{r_{u,i}} \\
&= g_2^{\alpha q(i)} (T(i))^{r_{u,i}}, \\
d_{u,2}^{(i)} &= \left(g^{r'_{u,i} - \frac{\alpha}{i^n+u(i)}}\right)^{\Delta_{0,S}(i)} \\
&= \left(g_1^{-\frac{1}{i^n+u(i)}} g^{r'_{u,i}}\right)^{\Delta_{0,S}(i)}.
\end{aligned}$$

**-Sign queries:** Consider the query for a signature of attribute set $\omega_u$ on $m$. If $F(m) = 0$, the simulation aborts. Otherwise, if $i^n + u(i) \neq 0 \pmod p$, $\mathcal{B}$ can use the Sign algorithm to create a signature on $m$. If $i^n + u(i) = 0 \pmod p$, $\mathcal{B}$ selects a random set $\Lambda$ such that $\Lambda \subseteq \omega_u^*$ and $|\Lambda| = k_u - 1$, and define $g^{q'(i)} = g^{\lambda'_i}$, where $i$ is chosen randomly in $\omega_u^* - \Lambda$. Then it computes $g^{q'(i)} = \left(\prod_{k=1}^{d-1} g^{\lambda' {}_k \Delta_{k,\omega_u^*}(i)}\right) g^{a\Delta_{0,\omega_u^*}(i)}$ for $i \in \omega_u^* - \Lambda$. $\mathcal{B}$ picks random $r_{u,i}, r'_m$ for $i \in \omega_u^*$, and computes the public signature $\sigma_{u,1} = (\sigma_{u,1}^{(i)}, \sigma_{u,2}^{(i)}, \sigma_{u,3}^{(i)})$, where

$$\begin{aligned}
\sigma_{u,1}^{(i)} &= g^{-aq'(i)J(m)/F(m)} (g^{f(i)})^{r_{u,i}} (g_2^{F(m)} g^{J(m)})^{r'_{m,i}}, \\
\sigma_{u,2}^{(i)} &= g^{r_{u,i}}, \\
\sigma_{u,3}^{(i)} &= g^{r'_{m,i} - aq'(i)/F(m)}.
\end{aligned}$$

For $r_{m,i} = r'_{m,i} - aq'(i)/F(m)$,

$$\begin{aligned}
\sigma_{u,1}^{(i)} &= g^{-aq'(i)J(m)/F(m)} (g^{f(i)})^{r_{u,i}} (g_2^{F(m)} g^{J(m)})^{r'_{m,i}} \\
&= g_2^{\alpha q(i)} (g^{f(i)})^{r_{u,i}} (g_2^{F(m)} g^{J(m)})^{r'_{m,i} - aq'(i)/F(m)} \\
&= g_2^{\alpha q(i)} (T(i))^{r_{u,i}} (v' \prod\nolimits_{j=1}^{m} v_j^{\mu_j})^{r_{m,i}}, \\
\sigma_{u,3}^{(i)} &= g^{r'_{m,i} - aq'(i)/F(m)} = g^{r_{m,i}}.
\end{aligned}$$

**-Designation queries:** Suppose $\mathcal{A}$ issues a DS query for a message $m$ and the designated verifier attribute set $\omega_v$. If $F(m) = 0$, the simulation aborts. Otherwise, if $i^n + u(i) \neq 0 \pmod p$, $\mathcal{B}$ can use the Designation algorithm to create a signature on $m$. If $i^n + u(i) = 0 \pmod p$, $\mathcal{B}$ can obtain the publicly verifiable signature $\sigma_s = (\{\sigma_{s,1}^{(i)}\}, \{\sigma_{s,2}^{(i)}\}, \{\sigma_{s,3}^{(i)}\})_{i \in s}$. Then $\mathcal{B}$ chooses a random $\bar{r}_{v,i,j}, \bar{r}_{s,i}, \bar{r}_{m,i,j}$ and computes the designated verifier signature $\sigma_{sv} = (\{\sigma_{sv,1}^{(i,j)}\}, \{\sigma_{sv,2}^{(i,j)}\}, \{\sigma_{sv,3}^{(i,j)}\}, \{\sigma_{sv,4}^{(i,j)}\})_{i \in \omega_s, j \in \omega_v}$, where

$$\begin{aligned}
&\sigma_{sv,1}^{(i,j)} = \\
&g^{-J(m)\alpha q'_1(i) Q'(j)/F(m)} \Big(g^{f(j)}\Big)^{\bar{r}_{v,i,j}} \\
&\quad \cdot \Big(g^{f(i)}\Big)^{\bar{r}_{s,i} + r_{s,i} Q'(j)} (g_2^{F(m)} g^{J(m)})^{\bar{r}'_{m,i,j} + Q'(j) r_{m,i}} \\
=&g_2^{\alpha q'_1(i) Q'(j)} \Big(g^{f(j)}\Big)^{\bar{r}_{v,i,j}} \Big(g^{f(i)}\Big)^{\bar{r}_{s,i} + r_{s,i} Q'(j)} \\
&\quad \cdot (g_2^{F(m)} g^{J(m)})^{\bar{r}'_{m,i,j} + Q'(j) r_{m,i} - \alpha q'_1(i) Q'(j)/F(m)} \\
=&g_2^{\alpha q'_1(i) Q'(j)} T(j)^{\bar{r}_{v,i,j}} T(i)^{\bar{r}_{s,i} + r_{s,i} Q'(j)} \\
&\quad \cdot (v' \prod\nolimits_{j=1}^{m} v_j^{\mu_j})^{\bar{r}_{m,i,j} + Q'(j) r_{m,i}} \\
=&\sigma_{u,1}^{Q'(j)} T(j)^{\bar{r}_{v,i,j}} T(i)^{\bar{r}_{s,i}} (v' \prod\nolimits_{j=1}^{m} v_j^{\mu_j})^{\bar{r}_{m,i,j}},
\end{aligned}$$

$$\begin{aligned}
\sigma_{sv,2}^{(i,j)} &= g^{r_{s,i} Q'(j)} g^{\bar{r}_{s,i}} = (\sigma_{u,2}^{(i)})^{Q'(j)} g^{\bar{r}_{s,i}}, \\
\sigma_{sv,3}^{(i,j)} &= g^{Q'(j) r_{m,i} - \alpha q'_1(i) Q'(j)/F(m)} g^{\bar{r}'_{m,i,j}},
\end{aligned}$$

$$\sigma_{sv,4}^{(i,j)} = g^{\bar{r}_{v,i,j}}.$$

**-Simulation queries:** Suppose that $\mathcal{A}$ issues a Sim query for a message $m$ under attribute set $(\omega_u, \omega_v)$, where $\omega_u$ and $\omega_v$ are chosen by $\mathcal{A}$. If $F(m) = 0$, the simulation aborts. Otherwise, if $i^n + u(i) \neq 0 \pmod p$, $\mathcal{B}$ can use the Simulation algorithm to create a signature on $m$. If $i^n + u(i) = 0 \pmod p$, $\mathcal{B}$ chooses a random $\hat{r}'_{v,j}, \hat{r}'_{s,i,j}, \hat{r}'_{m,i,j}$ and simulates the designated verifier signature as

$$\begin{aligned}
\bar{\sigma}_{sv,1}^{(i,j)} =& g^{-J(m)^{\alpha Q''(i) q'_2(j)/F(m)}} \left(g^{f(j)}\right)^{\hat{r}_{v,j} Q''(i) + \hat{r}'_{v,j}} \\
& \cdot \left(g^{f(i)}\right)^{\hat{r}'_{s,i,j}} (g_2^{F(m)} g^{J(m)})^{\hat{r}''_{m,i,j}} \\
=& g_2^{\alpha Q''(i) q'_2(j)} \left(g^{f(j)}\right)^{\hat{r}_{v,j} Q''(i) + \hat{r}'_{v,j}} \left(g^{f(i)}\right)^{\hat{r}'_{s,i,j}} \\
& \cdot (g_2^{F(m)} g^{J(m)})^{\hat{r}''_{m,i,j} - \alpha Q''(i) q'_2(j)/F(m)} \\
=& g_2^{\alpha Q''(i) q'_2(j)} T(j)^{\hat{r}_{v,j} Q''(i) + \hat{r}'_{v,j}} \\
& \cdot T(i)^{\hat{r}'_{s,i,j}} (v' \prod_{j=1}^{m} v_j^{\mu_j})^{\hat{r}'_{m,i,j}},
\end{aligned}$$

$$\bar{\sigma}_{sv,2}^{(i,j)} = g^{\hat{r}'_{s,i,j}},$$

$$\bar{\sigma}_{sv,3}^{(i,j)} = g^{\hat{r}''_{m,i,j} - \alpha Q''(i) q''(j)/F(m)},$$

$$\bar{\sigma}_{sv,4}^{(i,j)} = g^{\hat{r}_{v,j} Q''(i)} g^{\hat{r}'_{v,j}}.$$

**-DV queries:** For given query of DV queries on universal designated verifier signature, signer attributes set $\omega_u$ and designated verifier attributes set $\omega_v$.

If $F(m) \neq 0 \pmod{l_m}$, it can perform the designated verification algorithm to verify the signature. If the equation hold

$$\frac{e(g^a, g^b)^{x_s}}{e(g^a, g^b)^{x_v}} = \prod_j \prod_i \begin{pmatrix} e(\sigma_{sv,1}^{(i,j)}, g) \\ \cdot e(T(j)^{Q_s(i)}, d_{u,2}^{(i)}) \\ \cdot e(T(i), \sigma_{sv,2}^{(i,j)})^{-1} \\ \cdot e(g_2^{F(m)} g^{J(m)}, \sigma_{sv,3}^{(i,j)})^{-1} \\ \cdot e(T(j), \sigma_{u,4}^{(i,j)})^{-1} \\ \cdot e((d_{v,1}^{(i)})^{Q_s(i)}, g)^{-1} \end{pmatrix}^{\Delta_{i,S}(0)\Delta_{j,S'}(0)},$$

$\mathcal{B}$ outputs $acc$ to adversary, otherwise $rej$.

**Forgery:** If $\mathcal{B}$ does not abort during the simulation, $\mathcal{A}$ will output a valid universal designated verifier signature $S^* = (S_1^*, S_2^*, S_3^*, S_4^*)$ under attribute set $(\omega_s^*, \omega_v^*)$ with probability $\epsilon$. If $i^n + u(i) \neq 0 \pmod p$, $j^n + u(j) \neq 0 \pmod p$, $F(m) \neq 0 \pmod p$, then $\mathcal{B}$ abort. On the other hand, if $F(m) = 0 \pmod p$ and $j^n + u(j) = 0 \pmod p$ and $i^n + u(i) = 0 \pmod p$, $\mathcal{B}$ selects random set $\Lambda' \subseteq \omega_s^*$, $\Lambda'' \subseteq \omega_v^*$, and computes as follows:

$$\begin{aligned}
S_1^* &= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(\sigma_{sv,1}^{(i,j)}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j)} \\
&= g^{abc} \\
&\cdot \prod_{i \in \Lambda' j \in \Lambda''} \begin{pmatrix} \left(g^{f(j)}\right)^{\bar{r}_{v,j}} \\ \cdot \left(g^{f(i)}\right)^{\bar{r}_{s,i} + r_{s,i} Q'(j)} \\ \cdot \left(g^{J(m)}\right)^{\bar{r}'_{m,i,j} + Q'(j) r_{m,i}} \end{pmatrix}^{\Delta_{i,S'}(i)\Delta_{j,s''}(j)}, \\
S_2^* &= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(\sigma_{sv,2}^{(i,j)}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j) f(i)} \\
&= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(g^{r_{s,i} Q'(j)} g^{\bar{r}_{s,i}}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j) f(i)}, \\
S_3^* &= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(\sigma_{sv,3}^{(i,j)}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j) f(i)} \\
&= g^{Q'(j) r_{m,i}} g^{\bar{r}'_{m,i,j}}, \\
S_4^* &= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(\sigma_{sv,4}^{(j)}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j) f(j)} \\
&= \prod_{i \in \Lambda'} \prod_{j \in \Lambda''} \left(g^{\bar{r}_{v,i,j}}\right)^{\Delta_{i,S'}(i)\Delta_{j,s''}(j) f(j)}.
\end{aligned}$$

Then $\mathcal{B}$ computes and outputs

$$\frac{S_1^*}{S_2^* (S_3^*)^{J(m)} S_4^*} = g^{abc}.$$

We define the events $A_k$, $A^*$, $B$ and $C$ do not abort during Designation queries, Simulation queries and DV queries. That is,

$$\begin{aligned}
A_k &: F(m_k) \neq 0 \pmod{l_m}, \\
A^* &: F(m^*) = 0 \pmod p, \\
B &: j^n + u(j) = 0 \pmod p, \\
C &: i^n + u(i) = 0 \pmod p.
\end{aligned}$$

From the analysis above, the probability that $\mathcal{B}$ does not abort is

$$\Pr[Not - abort] \geq \Pr[\bigwedge_{k=1}^{q_I} A_k \wedge A^* \wedge B \wedge C].$$

The events $\bigwedge_{k=1}^{q_I} A_k \wedge A^*$ and $B$,$C$ are independent. The assumption $l_m(n_m + 1) < p$ implies that if

$F(m^*) = 0 \pmod p$, then $F(m^*) = 0 \pmod{l_m}$.

$$\begin{aligned}\Pr[A^*] =& \Pr[F(m^*) = 0(\mathrm{mod} p) \\ & \wedge F(m^*) = 0(\mathrm{mod} l_m)] \\ =& \Pr[F(m^*) = 0(\mathrm{mod} l_m)] \\ & \cdot \Pr[F(m^*) = 0(\mathrm{mod} p) \\ & \wedge F(m^*) = 0(\mathrm{mod} l_m)] \\ =& \frac{1}{l_m(n_m+1)}.\end{aligned}$$

We also have

$$\begin{aligned}\Pr[\bigwedge_{k=1}^{q_I} A_k | A^*] &= 1 - \Pr[\bigvee_{k=1}^{q_I} \bar{A_k} | A^*] \\ &\geq 1 - \sum_{k=1}^{q_I} \Pr[\bar{A_k} | A^*].\end{aligned}$$

Since the output of $F(m_{i_1})$ and $F(m_{i_2})$ $(i_1 \neq i_2)$ will differ at least one random chosen value, the events $F(m_{i_1}) = 0 \pmod{l_m}$ and $F(m_{i_2}) = 0 \pmod{l_m}$ are independent. The events $A_i$ and $A^*$ are independent for any $i$. Hence, we have

$$\begin{aligned}&\Pr[\bigwedge_{k=1}^{q_I} A_k \wedge A^*] \\ &\geq \frac{1}{l_m(n_m+1)} \left(1 - \frac{q_s + q_{DS} + q_{sim} + q_{DV}}{l_u}\right).\end{aligned}$$

Let $l_m = 2(q_s + q_{DS} + q_{sim} + q_{DV})$ and we get

$$\begin{aligned}&\Pr[Not - abort] \\ &\geq \Pr[\bigwedge_{k=1}^{q_I} A_k \wedge A^* \wedge B \wedge C] \\ &\geq \Pr[\bigwedge_{k=1}^{q_I} A_k \wedge A^*] \Pr[B] \Pr[C] \\ &\geq \frac{1}{4(n_m+1)(q_s + q_{DS} + q_{sim} + q_{DV})} \cdot \frac{1}{p^{n_\omega}} \cdot \frac{1}{p^{n_\omega}}.\end{aligned}$$

If the simulation does not abort, $\mathcal{A}$ will create a valid forgery with probability at least $\epsilon$. The algorithm $\mathcal{B}$ can compute $g^{abc}$ from forgery as shown above.

The time complexity of the challenger is dominated by the exponentiations, multiplications and pairing operations performed in queries. Extract queries need to do $\mathcal{O}(n_\omega)$ multiplications and $\mathcal{O}(n_\omega)$ exponentiations. Sign queries and designation queries need to do $\mathcal{O}(n_\omega \cdot n_m)$ multiplications and $\mathcal{O}(n_\omega)$ exponentiations. Simulation queries need to do $\mathcal{O}(n_\omega^2 \cdot n_m)$ multiplications and $\mathcal{O}(n_\omega^2)$ exponentiations. Designated verification queries need to do $\mathcal{O}(n_\omega^2)$ multiplications, $\mathcal{O}(n_\omega^2)$ exponentiations and $\mathcal{O}(1)$ pairing operations. Thus, we have

$$\begin{aligned}t' = t + \mathcal{O}((&n_\omega q_e + n_\omega \cdot n_m(q_s + q_{DS}) \\ &+ n_\omega^2 \cdot n_m q_{sim})\tau + n_\omega^2 q_{DV} t_k \\ &+ ((q_e + q_s + q_{DS})n_\omega + (q_{sim} + q_{DV})n_\omega^2)t_e \\ &+ n_\omega^2 q_{DV} t_u)\end{aligned}$$

□

**Theorem 6** *The proposed t-ABUDVS scheme is non-transferable against a* $(t, q_e, q_{PS}, q_{DS}, q_{Sim}, q_{DV})$ *adaptively chosen message and attributes set distinguisher* $\mathcal{D}$.

**Proof**: The Simulator $\mathcal{C}$ first runs setup algorithm, picks a secret $\alpha \in Z_p$ , computes $g_1 = g^\alpha$ and chooses $g_2 \in Z_p$.

Then the distinguisher starts performing following queries.

**Phase 1:** Since $\mathcal{C}$ knows the master key, he can run Extract algorithm, Sign algorithm, Designate algorithm, Simulation algorithm, and Designated algorithm to response Extract queries, Sign queries, Designate queries, Simulation queries, and Designated Verification queries, respectively.

**Challenge:** When the distinguisher $\mathcal{D}$ decides the first phase is over, he submits $(\omega_s^*, \omega_v^*, m^*)$ to the challenge. Then the simulator chooses a random coin $c \in \{0, 1\}$.

If $c = 1$, $\mathcal{C}$ runs sign algorithm, obtain $\sigma$, then he runs Designated algorithm, obtain $\sigma_{sv}$, and returns $\sigma_{sv}^* = \sigma_{sv}$ to $\mathcal{D}$.

If $c = 0$ , $\mathcal{C}$ runs simulation algorithm, obtain $\bar{\sigma}_{sv}$ , Then he returns $\sigma_{sv}^* = \bar{\sigma}_{sv}$ to $\mathcal{D}$.

**Phase 2:** Upon receiving the challenge message signature pair, the distinguish still can submit the more Extract, Sign, Designated, Simulation and Designated verification queries with constrains that:

1) For all Extract queries sets of attributes $\omega_s$ , we have $|\omega_s^* \cap \omega_s| < k_s$.

2) For all Sign queries pair $(\omega_s^*, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$ or $m \neq m^*$.

3) For all Designation queries or Simulation queries triple $(\omega_s^*, \omega_v^*, m)$ , we have $|\omega_s^* \cap \omega_s| < k_s$, $|\omega_v^* \cap \omega_v| < k_v$ or $m \neq m^*$.

In the designated algorithm, given the signers attributes set $\omega_s$ and the designated verifiers attributes set $\omega_v$, and a message signature pair $(m, \sigma)$, where $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, the signature holder SH selects $r_{(i,j)_a}, r_{(i,j)_b}, r_{m,i,j} \in Z_p$ and computes

$$\sigma_{sv} = (\sigma_{sv,1}^{(i,j)}, \sigma_{sv,2}^{(i,j)}, \sigma_{sv,3}^{(i,j)}, \sigma_{sv,4}^{(i,j)})_{i \in \omega_s, j \in \omega_v},$$

where

$$\sigma_{sv,1}^{(i,j)} = \sigma_3^{Q(j)} T(i)^{r_{(i,j)_a}} T(j)^{r_{(i,j)_b}} \cdot (v' \prod_{j=1}^{m} v_j^{\mu_j})^{r_{m,i,j}},$$

$$\sigma_{sv,2}^{(i,j)} = \sigma_2^{Q(j)} g^{r_{(i,j)_a}},$$

$$\sigma_{sv,3}^{(i,j)} = \sigma_3^{Q(j)} g^{r_{m,i,j}},$$

$$\sigma_{sv,4}^{(i,j)} = g^{r_{(i,j)_b}}.$$

Then we show that the signature simulated by the simulation algorithm is distinguishable from algorithm designated. The following distributions are

$$\bar{\sigma}_{sv,1}^{(i,j)} = g_2^{\alpha Q(i) q_2(j)} T(j)^{\bar{r}_{(i,j)_b}} T(i)^{\bar{r}_{(i,j)_c}} \cdot (v' \prod_{k=1}^{m} v_j^{\mu_j})^{\bar{r}_{(i,j)_d}},$$

$$\bar{\sigma}_{sv,2}^{(i,j)} = g^{\bar{r}_{(i,j)_c}}, \bar{\sigma}_{sv,3}^{(j)} = g^{\bar{r}_{(i,j)_d}}, \bar{\sigma}_{sv,4}^{(j)} = g^{\bar{r}_{(i,j)_b}},$$

$$\hat{\sigma}_{sv,1}^{(i,j)} = g_2^{\alpha Q_s(i) q_v(j)} T(j)^{\hat{r}_{(i,j)_b}} T(i)^{\hat{r}_{(i,j)_c}} \cdot (v' \prod_{k=1}^{m} v_j^{\mu_j})^{\hat{r}_{(i,j)_d}},$$

$$\hat{\sigma}_{sv,2}^{(i,j)} = g^{\hat{r}_{(i,j)_c}}, \hat{\sigma}_{sv,3}^{(i,j)} = g^{\hat{r}_{(i,j)_d}}, \hat{\sigma}_{sv,4}^{(i,j)} = g^{\hat{r}_{(i,j)_b}},$$

$$\Pr[\sigma_{sv} = \sigma_{sv}^*] = \frac{1}{p^{11|\omega_s||\omega_v|}},$$

$$\Pr[\bar{\sigma}_{sv} = \sigma_{sv}^*] = \frac{1}{p^{11|\omega_s||\omega_v|}}.$$

Which means both distributions of probability are the same. Hence, our proposed scheme satisfies the non-transferable property. □

**Delegatability:** Lipmaa *et al.*[15] proposed a new security notion for designated verifier signature called non-delegatability. Non-delegatability means that there exists an efficient knowledge extractor either the signers secret key or the designated verifier secret key, when given oracle access to an adversary who can create valid signatures with a high probability. The proposed scheme in this paper does not satisfy this property because anyone who has the knowledge of the trapdoor$(g_2^{\alpha q_s(i) Q_v(j)} T(j)^{r'_{v,i,j}} T(i)^{r'_{s,i,j}}, g^{r'_{s,i,j}}, g^{r'_{v,i,j}})_{i \in \omega_s, j \in \omega_v}$ can compute a valid signature designated to a verifier. Moreover we note that the ring signature scheme recently proposed in [1] might be used to construct a non-delegatable UDVS scheme without random oracles.

# 7 Conclusion

In this paper, we introduced a threshold attribute based universal designated verifier signature scheme and gives the definition, formalization and security model of the threshold attribute based universal designated verifier signature. The proposed scheme satisfies the privacy property of UDVS and is unforgeable against an adaptively chosen message and attributes set attack under BDH assumption.

**Acknowledgements:** The research was supported by Natural Science Foundation of China (grant No. 61271174 and 61301178).

*References:*

[1] A. Bender, J. Katz and R. Morselli, Ring signatures: Stronger definitions, and constructions without random oracles, *Theory of Cryptography,* 2006, pp. 60–79.

[2] J. Bethencourt, A. Sahai and B. Waters, Ciphertext-policy attribute-based encryption, *Security and Privacy, 2007. SP'07. IEEE Symposium on,* 2007, pp. 321–334.

[3] D. Boneh and X. Boyen, Efficient selective-ID secure identity-based encryption without random oracles, *Advances in Cryptology–EUROCRYPT,* 2004, pp. 223–238.

[4] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology–CRYPTO,* 2001, pp. 213–229.

[5] F. Cao and Z. Cao, An identity based universal designated verifier signature scheme secure in the standard model, *Journal of Systems and Software,* 82, 2009, pp. 643–649.

[6] L. Cheung and C. Newport, Provably secure ciphertext policy ABE, *Proceedings of the 14th ACM conference on Computer and communications security,* 2007, pp. 456–465.

[7] W. Diffie and M. Hellman, New directions in cryptography, *Information Theory, IEEE Transactions on,* 22, 1976, pp. 644–654.

[8] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, *Proceedings of the 13th ACM conference on Computer and communications security,* 2006, pp. 89–98.

[9] S. Guo and Y. Zeng, Attribute-based signature scheme, *Information Security and Assurance, 2008. ISA 2008. International Conference on,* 2008, pp. 509–511.

[10] F. Hess, Efficient identity based signature schemes based on pairings, *Selected Areas in Cryptography,* 2003, pp. 310–324.

[11] X. Huang, W. Susilo, Y. Mu and W. Wu, Secure universal designated verifier signature without random oracles, *International Journal of Information Security,* 7, 2008, pp. 171–183.

[12] D. Khader, Attribute Based Group Signatures, *IACR Cryptology ePrint Archive,* 2007, p. 159.

[13] J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren, Attribute-based signature and its applications, *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security,* 2010, pp. 60–69.

[14] J. Li and K. Kim, Attribute-Based Ring Signatures, *IACR Cryptology ePrint Archive,* 2008, p. 394.

[15] H. Lipmaa, G. Wang and F. Bao, Designated verifier signature schemes: attacks, new security notions and a new construction, *Automata, Languages and Programming,* 2005, pp. 459–471.

[16] H.K. Maji, M. Prabhakaran and M. Rosulek, Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance, *IACR Cryptology ePrint Archive,* 2008, p. 328.

[17] K.G. Paterson and J.C.N. Schuldt, Efficient identity-based signatures secure in the standard model, *Information Security and Privacy,* 2006, pp. 207–222.

[18] A. Sahai and B. Waters, Fuzzy identity-based encryption, *Advances in Cryptology–EUROCRYPT,* 2005, pp. 457–473.

[19] S.F. Shahandashti and R. Safavi-Naini, Threshold attribute-based signatures and their application to anonymous credential systems, *Progress in Cryptology–AFRICACRYPT,* 2009, pp. 198–216.

[20] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology,* 1985, pp. 47–53.

[21] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, Universal designated-verifier signatures, *Advances in Cryptology–ASIACRYPT,* 2003, pp. 523–542.

[22] R. Steinfeld, H. Wang and J. Pieprzyk, Efficient extension of standard Schnorr/RSA signatures into universal designated–verifier signatures, *Public Key Cryptography–PKC,* 2004, pp. 86–100.

[23] P. Yang, Z. Cao and X. Dong, Fuzzy identity based signature with applications to biometric authentication, *Computers & Electrical Engineering,* 37, 2011, pp. 532–540.

[24] P. Yang, Z. Cao and X. Dong, Fuzzy Identity Based Signature, *IACR Cryptology ePrint Archive,* 2008, p. 2.

[25] R. Zhang, J. Furukawa and H. Imai, Short signature and universal designated verifier signature without random oracles, *Applied cryptography and network security,* 2005, pp. 483–498.