A lightweight attribute-based authentication system with DAA

Xin Liu1,2,*, Man Guo3, Bin Zhang1,2 and Xuzhou Li1,2

1 School of Information Engineering, Shandong Youth University of Political Science, Jinan, Shandong, 250013, China
2 Key Laboratory of Information Security and Intelligent Control in Universities of Shandong (Shandong Youth University of Political Science), Shandong Youth University of Political Science, Jinan, Shandong, 250013, China
3 Public Course Teaching Department, Shandong University of Art & Design, Jinan, Shandong, 250300, China
*Corresponding author’s e-mail: lxonne@163.com

Abstract. In cloud computing environment, while preventing users from illegally accessing resources, various cloud service systems must provide protection for authorized users of their personal sensitive information. Attribute-based authentication (ABA) makes it possible to solve the above problems. An efficient ABA system was put forward by extending the direct anonymous attestation (DAA) scheme of Brickell et al. During the construction of the new system, the technique of lightweight ciphertext policy attribute-based encryption was adopted, and the online computing task of users was optimized. Compared with other similar systems, the new system is characterized by the use of trusted computing technology to improve the level of privacy protection of users, and the computational complexity of users in the authentication stage is independent of the size of access policy.

1. Introduction
At present, cloud computing technology is changing the usage of information resources and infiltrating into people’s daily life. On the other hand, the cloud computing paradigm also raises many security and privacy protection issues [1]. For the purpose of data sharing, more and more electronic resources are stored in the cloud in a centralized way. However, this storage service must provide privacy protection for users while ensuring data security. Fine grained access control requires system authorities to customize access rights for each member of the user group according to their attributes, so that users can access authorized sensitive data or services [2]. Attribute-Based Authentication (ABA) provides a feasible solution for enforcing fine-grained access control, and can meet the needs of users’ privacy protection. In an ABA system, once the Service Provider (SP) receives an access request from some anonymous user, it will return the access structure required for authentication. At this time, the user should prove to SP that he/she owns the attributes that can satisfy the structure. If the proof is accepted by SP, the user will be authorized to access.

According to the type of underlying core primitive, the existing ABA schemes can be divided into three categories, that is, the schemes based on Attribute-Based Group Signature (ABGS), the schemes based on Attribute-Based Encryption (ABE) and the schemes based on Attribute-Based Signature (ABS). Khader [3] proposed the concept of ABGS for the first time, and constructed several ABA schemes based on it. In [4], Emura et al. proposed a new method for constructing dynamic attribute
tree. Compared with the static attribute tree in [3], the dynamic attribute tree has the following advantages, i.e., when a new attribute value (i.e., leaf node) needs to be added to the attribute tree, only the attribute key needs to be recalculated for the user who owns it. Yang et al. [5] devised a dynamic ABA scheme based on the dynamic attribute tree of Emura et al. [4], but their scheme requires to construct a large-scale central attribute tree, which increases the cost of operation and storage. In [6], Zhou et al. defined an authorization access model for distributed medical systems. By combining with the technique of ABE and designated verifier signature, they constructed a privacy-preserving authentication scheme self-controlled by patients. In [7], Li et al. put forward a multi-authority ABA scheme supporting threshold predicate. Lian et al. [8] proposed the concept of adaptive anonymous authentication supporting dynamic strategy, and constructed a generic scheme based on ABS. In 2015, Li et al. [9] proposed a cooperative attribute-based access control scheme. In this scheme, users are divided into groups. Users from the same group can access the enterprise sensitive data through shared attributes. It should be noted that the disadvantages of the above schemes are as follows: (1) The length of attribute key grows linearly with the size of users’ attribute set. (2) The computing efficiency of users in the authentication stage is unappealing, i.e., the computing complexity of users depends on the size of access structure.

1.1. Related research
Direct anonymous authentication (DAA) [10, 11] is a special anonymous signature scheme. In a DAA scheme, a tamper-resistant chip called Trusted Platform Module (TPM) can generate anonymous signatures for the current state information of the host, which is conducive to direct data exchanges between the two sides of communication under the condition of ensuring privacy. The remarkable feature of DAA scheme is that the signer is further divided into two roles, i.e., the TPM chip and the host. Among them, the TPM chip has limited computing and storage capacity, but it can provide high level security guarantee. The host has stronger computing and storage capacity, but it can only perform non-critical computing tasks. At present, DAA has become a popular building block of constructing all kinds of privacy-preserving authentication systems. In [12], Dietrich et al. studies the use of DAA technology to perform anonymous authentication in NFC scenarios. In [13], Chen et al. used TLS and DAA technology to design a lightweight anonymous authentication scheme suitable for embedded devices. By using DAA, Liu et al. constructed an endorsed e-cash system [14] and they also put forward a multi-coupon system for federated environments [15]. In [16], Kumar et al. designed an anonymous subscription system, which conforms to TPM 2.0 specification.

1.2. Contribution
In this paper, we propose an efficient ABA system, which was obtained by combining the DAA scheme of Brickell et al [11] with CP-ABE scheme of Guo et al [17]. Compared with the existing similar systems, the new system has the following advantages: (1) The user’s attribute decryption private key is stored in the tamper-resistant TPM chip, which can effectively prevent the private key from leaking. (2) The user’s computing tasks are assigned to the TPM chip and the host. Even if it is corrupted, the host is not able to perform anonymous authentication independently, which can effectively prevent malicious users from launching clone attacks by sharing member credentials and decrypting private keys. (3) Attribute-based access control is achieved by adopting the underlying CP-ABE scheme, and the amount of computation in the authentication phase is independent of the size of the access structure.

1.3. Organization of the paper
In Section 2, we introduce the main concepts and building blocks used in this paper. In Section 3, we present the syntax definition and security definition of ABA systems. In Section 4, we propose a new ABA system with DAA. In Section 5 and 6, we provide security analysis and performance analysis, respectively. In Section 7, we summarize and discuss future work.
2. Preliminaries

2.1. Bilinear pairing

In this paper, we will use bilinear mapping \( \hat{e} : G_1 \times G_2 \rightarrow G_r \), where \( G_1, G_2, G_r \) are cyclic groups of prime order \( p \). At the same time, the mapping \( \hat{e} \) has the following properties: (1) Bilinear: for all \( g \in G_1, h \in G_2, a, b \in \mathbb{Z}_p \), \( \hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab} \). (2) Non-degeneracy: there exists \( g \in G_1, h \in G_2 \), s.t., \( \hat{e}(g, h) \neq 1_{G_r} \). (3) Computable: for any \( g \in G_1, h \in G_2 \), \( \hat{e}(g, h) \) can be calculated efficiently.

2.2. Signature of knowledge

Zero-knowledge proof of knowledge is a kind of three rounds interactive protocol executed by a prover \( P \) and a verifier \( V \). In the random oracle model, such protocol can be transformed into non-interactive version by using the Fiat-Shamir heuristics, and it can also be used to generate signature on the given message. In such circumstance, it is called a signature of knowledge. Using the symbols introduced by Camenich et al. [18], we denote such protocols as \( (x, y) \rightarrow g^y \ldots (m) \).

2.3. The DAA scheme of Brickell et al.

In a DAA scheme, there are three participants: an issuer \( I \), a user \( U \) and a verifier \( V \). A DAA scheme comprises multiple algorithms or protocols. Specifically, the Setup algorithm is used to generate the group public key and issuer’s private key. \( U \) obtains his/her membership credential by executing the Join protocol with \( I \). \( U \) can use the Sign algorithm to generate a DAA signature anonymously. \( V \) verifies \( Y \)'s signature by executing the Verify algorithm. It should be noted that in a DAA scheme, the user’s role is divided into two entities, i.e., the TPM chip \( M \) and the host \( H \). In other words, the Join protocol and the Sign/Verify protocol can be regarded as a tripartite interaction protocol cooperately performed by \( M, H \) and \( \xi \). In [11], Brickell et al. proposed an efficient DAA scheme. The characteristic of this scheme is that \( M \) only needs to perform a few exponential operations in group \( G_r \).

2.4. The CP-ABE scheme of Guo et al.

In [17], Guo et al. proposed a lightweight CP-ABE scheme. Define the attribute universe \( U = \{ A_1, \ldots, A_n \} \). In order to encrypt a message \( M \), the data owner defines the AND gate access structure \( P = b_1 b_2 \cdots b_n \), s.t.,

\[
\begin{align*}
    b_i &= \begin{cases} 1, & A_i \in P \\ 0, & A_i \notin P 
\end{cases}
\end{align*}
\]

In this scheme, the attribute set \( A \) can be defined as \( A = a_1 a_2 \cdots a_n \), s.t.,

\[
\begin{align*}
    a_i &= \begin{cases} 1, & A_i \in A \\ 0, & A_i \notin A 
\end{cases}
\end{align*}
\]

Given the ciphertext \( CT \), for the user who owns the decryption private key \( sk_A \), he can successfully decrypt when his attribute set \( A \) fulfils the access structure \( P \), i.e., \( P \subseteq A \). In other words, for \( i = 1, \ldots, n \), two bits \( a_i \) and \( b_i \) satisfy \( a_i - b_i \in \{0, 1\} \). Since the decryption private key \( sk_A \) contains only two group elements, the scheme is suitable for deployment on devices with limited storage capacity.

3. System syntax and security definition

An ABA system consists of the following algorithms / protocols:

- **Setup.** The algorithm is performed by the trusted party \( T \). On input of \( 1^k \), \( T \) outputs the system parameter \( gpk \).
**AASetup.** The algorithm is performed by attribute authority AA. Taking the security parameter $\lambda$ and the system parameter $gpk$ as input, AA outputs the public key $apk$, the private key $ask$ and the master key $msk$.

**AttGen.** This is a two-party protocol jointly executed by user U and AA. U takes the system parameter $gpk$, the attribute public key $apk$ and the attribute set $A$ as input. AA takes the system parameter $gpk$, the attribute public key $apk$, the private key $ask$ and the master key $msk$ as input. Finally, U outputs the member credential $cre$ and the attribute key $sk_A$.

**Authentication.** This is a two-party protocol between Y and $\Sigma \Pi$. Y takes the system parameter $gpk$, the attribute public key $apk$, the member credential $cre$, the attribute set $A$ and the attribute key $sk_A$ as input. $\Sigma \Pi$ takes the system parameter $gpk$, the attribute public key $apk$ and the access structure $P$ as input. Finally, $\Sigma \Pi$ returns accept or reject.

A secure ABA system should meet the following properties:

**Correctness.** Suppose U obtains the valid member credential $cre$ and the attribute key $sk_A$ of attribute set $A$ by executing the AttGen protocol. When SP specifies the access structure $P$, U can successfully execute the AttGen protocol with SP, if and only if, $\{P\} \subseteq A$.

**Privacy.** Even if conspired with AA, SP cannot obtain the real identity of U by executing the Authentication protocol with the latter. Moreover, they can neither decide whether two executions of the Authentication protocol are participated by U, nor can they judge whether an execution of the Authentication protocol and an execution of the AttGen protocol correspond to U.

**Soundness.** If the following conditions are satisfied, U and SP successfully execute the Authentication protocol: 1) U has a valid member credential $cre$ and attribute key $sk_A$. 2) The attribute set of U satisfies the access structure $P$ prescribed by SP.

**Coalition-resistance.** Suppose that user $U_1$ and $U_2$ have attribute sets $A_1$ and $A_2$ respectively. In the case that both $A_1$ and $A_2$ do not satisfy the access structure $P$, even if $U_1$ colludes with $U_2$, they cannot successfully execute the Authentication protocol with SP.

4. A new lightweight ABA system

4.1. High level description

The new system is constructed by extending the DAA scheme of Brickell et al. [11]. In the new system, there are the following parties, namely an attribute authority AA, a user U and a service provider SP, and they correspond to an issuer, a user and a verifier in a DAA scheme respectively. At the same time, we divide U into two independent entities, i.e., the TPM chip M and the host H. We divide the initialization phase of the system into the Setup algorithm and the AASetup algorithm. As an alternative, the two algorithms can also be combined, that is, the public parameter $gpk$ and the attribute public key $apk$ are generated by AA. The AttGen protocol corresponds to the Join protocol of DAA scheme. In this protocol, AA generates the member credential $cre$ in DAA scheme and the attribute key of the underlying CP-ABE Scheme [17] for U. The Authentication protocol corresponds to the Sign protocol of the DAA scheme (this is a complex three-party protocol, and the interaction between the participants is shown in Figure 1). In this protocol, SP encrypts the challenge string $n_{sp}$ with access policy $P$, and provides the resulting ciphertext $CT$ to H. After receiving the $CT$, H and M jointly perform the decryption of $CT$ to recover $n_{sp}$. Then, H and M jointly generate the signature of knowledge $SPK\{s\} = (g_og')^{(e\cdot y)} \land B = K^e(n_{sp})$, which proves the following facts: (1)
U owns a valid member credential. U has not been revoked because its TPM private key does not appear in the revocation list. To note that, in order to avoid bilinear pairing operations, we adopt the technique of in [19] to convert equivalently the above signature of knowledge to the following form, i.e., $SPK\{\beta, \beta s, e, s\} : \tilde{A} = g_0^\beta g_0^{e \beta} \tilde{A}^\gamma \land B = K^s(n_w)$. As a cost, SP is required to additionally verify whether $e(\tilde{A}, h) = e(\tilde{A}, w)$ and $\tilde{A} \neq 1_w$ are satisfied.

![Authentication diagram](attachment:image.png)

**Figure 1. Interaction of participants in the authentication phase.**

4.2. Detailed description

We now detail the construction of the new scheme.

**Setup.** With the security parameter $\ell^*$ as input, the trusted party T performs the following steps:

1. Define the bilinear group environment $(G_1, G_2, G_3, p, \hat{e})$, where $G_1, G_2, G_3$ are prime $p$-order cyclic groups and $\hat{e}$ is an asymmetric bilinear mapping, s.t., $\hat{e} : G_1 \times G_2 \rightarrow G_3$.
2. Select $g_0, g, h \in G_2$, compute $\hat{e}(g, h)$ and define the following collision-resistant hash functions, i.e., $H_i : \{0, 1\}^* \rightarrow Z_p^*, H_1 : \{0, 1\}^* \rightarrow \{0, 1\}^*$. $H_i : \{0, 1\}^* \rightarrow \{0, 1\}^*$.
3. Set the public key $gpk = (G_1, G_2, G_3, p, h, g_0, g, h, \hat{e}(g, h), H_1, H_2, H_3)$.

**AASetup.** AA does the following steps:

1. Select $\alpha, \gamma \in Z_p$ and set $w = h^\gamma$. For $i = 1, \ldots, n$, set $v_i = g^\alpha, h_i = h^\alpha$.
2. Define the attribute universe $U = \{A_1, \ldots, A_n\}$.
3. Initialize the public table $RL \leftarrow \emptyset$.
4. Set the attribute public key $apk = (U, \{v_i\}_{i=1}^n, \{h_i\}_{i=1}^n, w, RL)$ and keeps secretly $ask = \gamma, msk = \alpha$.

**AttGen.** Suppose M has established a trusted communication channel with AA by using it’s endorsement key. In order to register and obtain the attribute key, M and H perform the following steps with AA:

1. AA selects $n_{AA} \in \{0, 1\}^*$ and sends $n_{AA}$ to M.
2. M computes $s = H_1(DAASeed || cnt || K_{AA})$, where $DAASeed$ represents M’s internal secret value, and its function is to help M generate it’s private key. $cnt$ is a counter that records the number of times M has executed the $AttGen$ protocol. $K_{AA}$ represents the identity of AA.
3. M computes $F_1 = g^\gamma, F_2 = h^\gamma$ and generates the signature of knowledge $\pi_m^A = SPK\{(s) : F_1 = g^\gamma \land F_2 = h^\gamma\}(n_{AA})$. Then M sends $F_1, F_2, A, \pi_m^A$ to AA, where $A$ represents the attribute set of $Y$. 

5
(4) AA performs the verification of $\pi^3_M$. If $\pi^3_M$ is valid, AA performs the following steps:

(4.1) Select $e \in \mathbb{Z}_p$, compute $A = (g_F^{\xi-e/p})$ and set $cre = (A,e)$.

(4.2) Parse $A$ into $A = a_0a_1...a_n$, define a polynomial $f(\alpha,A) = \prod_{i=1}^n (\alpha + H_i(i))^{-a_i}$ of degree $n$, and calculate $sk_A = (sk_{A,1},sk_{A,2})$, where $sk_{A,1} = (F_1)^{\xi/(\alpha,A)}$, $sk_{A,2} = (F_2h^{-1})^{\xi/a}$.

(4.3) Return $cre,sk_A$ to $M$.

(5) $M$ sends $cre,F_1$ to $H$, who verifies if $\hat{e}(A,wh') = \hat{e}(g_F^{e_1},h)$. If so, $H$ stores $cre$. Meanwhile, $M$ stores $sk_A$ and sets $cnt' = cnt + 1$.

**Authentication.** To access the desired resources, $M$ and $H$ perform the following steps with $SP$:

(1) $H$ sends an authentication request $req$ to $SP$.

(2) $SP$ sets the access control policy $P = h_0...h_l$ and defines a polynomial $f(x,P)$ of degree $n-1$, i.e., $f(x,P) = \prod_{i=1}^n (x + H_i(i))^{-h} = \sum_{i=1}^{n-1} f_i x^i$. $SP$ selects $n_{sp} \in \{0,1\}^l$ and generates the ciphertext $CT$ of $n_{sp}$. Specifically, $SP$ selects $r \in \mathbb{Z}_{p^*}, \sigma \in \{0,1\}^l$ and sets $C_1 = (h^l\prod_{i=1}^{n-1} h_{i}^{e_r})$. For $i = 1,..,n-1$, $SP$ calculates $C_{i+1} = V_i$. $SP$ sets $C_3 = H_2(\hat{e}(g,h')) \otimes \sigma, C_4 = H_3(\sigma) \otimes n_{sp}$. Finally, $SP$ returns $CT = (P,C_1,\{C_{i+1}\}_{i=1}^{n-1},C_3,C_4)$ to $H$.

(3) $H$ parses $CT$ into $CT = (P,C_1,\{C_{i+1}\}_{i=1}^{n-1},C_3,C_4)$. Then, it checks if $P \subseteq A$. Specifically, for $i = 1,...,n$, it checks if $a_i - b_i \in \{0,1\}$. If not, $H$ aborts the current protocol. Else, $H$ defines a polynomial $F(x) = \prod_{i=1}^n (x + H_i(i))^{e_r} = \sum_{i=1}^{n-1} F_i x^i$ of degree $n-|P|$, and computes $U = \hat{e}(C_{n+1},\prod_{i=1}^n h_{i}^{e_r})$, $V'_i = \prod_{i=1}^{n-1} (C_{i+1})^{e_r}$. $H$ selects $\beta \in \mathbb{Z}_p$, and computes $\tilde{A} = A' = (g_F^{e_1})^{e_r}$. Finally, $H$ sends $req$, $\beta,V'_1,C_1$ to $M$.

(4) $M$ selects $B \in G_1, \rho, \rho_{\beta}, \rho_{\beta_s}, r_1, r_2 \in \mathbb{Z}_p^*$, computes $s = H_1(DAASeed \| cnt \| K_{AA}), K = B^s, R_{ul} = g_{\rho_{\beta_s}}$, $V_1 = (V'_1)^{s}, V_2 = (sk_{A,1})^{s}, W_1 = (sk_{A,2})^{s}, W_2 = C_{i+1}^{s}$ and returns $R_{u1}, R_{u2}, B, K, V_1, V_2, W_1, W_2$ to $H$.

(5) $H$ calculates $V = \hat{e}(V_1, V'_2)$, $W = \hat{e}(W_1, W_2)$, $\hat{e}(g,h) = (W \cdot U^{-1} \cdot V^{-1})^{e_r}$, and recovers $n_{sp} = H_1(\hat{e}(g,h') \otimes C_3) \otimes C_4$. $H$ selects $\rho_{\beta_s} \in \mathbb{Z}_p$, computes $R_1 = g^{e_1} r_{ul} \tilde{A}^{e_r}$, sets $c_{ui} = H_1(g_{\rho_{\beta_s}} || Apk || B || K || \tilde{A} || \tilde{R} || R_1 || R_2 || n_{sp})$ and sends $c_{ui}$ to $M$.

(6) $M$ selects $n_{m} \in \{0,1\}^*$, sets $c = H_1(c_{ui} \| n_{m} \| req), \xi_{\beta} = \rho_{\beta_s} + c \beta s (mod \ p)$ and returns $n_{m,c}, c_{\xi_{\beta}}, c_{\xi_{\beta_s}}$ to $H$.

(7) $H$ computes $\hat{\xi}_{\beta} = \rho_{\beta} + c \beta (mod \ p), \xi_{\beta} = \rho_{\beta} + ce (mod \ p)$ and provides $\sigma = (B,K,\tilde{A},c,n_{m,c},\xi_{\beta},\xi_{\beta_s},\xi_{\beta_s})$ to $SP$.

(8) $SP$ parses $\sigma$ into $\sigma = (B,K,\tilde{A},c,n_{m,c},\xi_{\beta},\xi_{\beta_s},\xi_{\beta_s})$. Then, $SP$ performs the following verification steps in turn.

(8.1) Check whether $B,K,\tilde{A} \in G_1$ and $\xi_{\beta}, \xi_{\beta_s}, \xi_{\beta_s} \in \mathbb{Z}_p$.

(8.2) Compute $\hat{R}_1 = g_{\xi_{\beta}} g_{\xi_{\beta_s}} \tilde{A}^{\hat{\xi}_{\beta}}$, $\hat{R}_2 = B^{\hat{\xi}_{\beta_s}} K^{-\hat{\xi}_{\beta}}$.

(8.3) Check if $c = H_1(H_1(g_{\rho_{\beta_s}} || Apk || B || K || \tilde{A} || \tilde{R} || R_1 || n_{sp}) \| n_{m} \| req)$.

(8.4) Verify that $e(\tilde{A},h) = e(\tilde{A},w)$ and $\tilde{A} \neq 1_{G_1}$.

(8.5) For each $s' \in RL$, check if $K \neq B^{s'}$. 

---

**Note:** The above text appears to be a fragment of a larger document, possibly related to the Journal of Physics: Conference Series with the reference 1601 (2020) 032025. Further context or the complete document would be necessary to provide a complete and accurate transcription. The content seems to involve cryptographic or security protocol steps.
If all the above verifications success, SP returns accept, otherwise, SP returns reject.

5. Security analysis
In this section, we prove that the new scheme verifies all security properties defined in Section 2.

Correctness. First, we prove that if $\mathbf{P} \subseteq \mathbf{A}$, U can successfully recover the challenge string $n_{sp}$ from $CT$. Specifically, when $\mathbf{P} \subseteq \mathbf{A}$, M provides $V_1, V_2, W_1, W_2$ to H. So, H can calculate

$$V = \hat{e}(V_1, V_2) = \hat{e}\left(\prod_{i=1}^{a_{sp}} (C_{2i})^{\alpha_i}, h^{(s-1)/a}\right) = \hat{e}(g, h)^{\alpha F(a) - \alpha F(a)} \quad (1)$$

and

$$W = \hat{e}(W_1, W_2) = \hat{e}(g^{s/(a, \lambda)}, C_1) = \hat{e}(g, h)^{\alpha F(a)} \quad (2)$$

In addition, H calculates

$$U = \hat{e}(C_{22}, \prod_{i=1}^{s_{sp}} h^{\alpha_i}) = \hat{e}(g, h)^{\alpha F(a) - \alpha F(a)} \quad (3)$$

Obviously, according to formula (1), (2), (3), $n_{sp} = H_1(H_2(\hat{e}(g, h)^{\alpha})) \oplus C_1 \oplus C_4$.

Next, we prove that the signature of knowledge $\sigma$ generated by the legal user U in the Authentication protocol can pass the verification of SP. According to the generation of $\sigma$, it can be seen that the condition of successful verification is that, $\hat{R}_1 = R_1, \hat{R}_2 = R_2$. Specifically, the following two equations can be proved to hold:

$$\hat{R}_1 = g^{a_{sp}^2 g_{to}^{\beta_1}} A^{\beta_1} = g^{a_{sp}^2 g_{to}^{\beta_1}} g^{\beta_1 s_{sp}^{(s-1)/a}} A^{\beta_1} = R_1 (g_0 g_{to}^{\beta_1} g_0^{(s-1)/a})^{-\alpha} = R_1 \quad (4)$$

$$\hat{R}_2 = B^{s_{sp}^2 K^{\gamma}} = B^{s_{sp}^2 K^{\gamma}} = R_2 (KK^{-1})^{\gamma} = R_2 \quad (5)$$

Privacy. In the AttGen protocol, M provides the signature of knowledge $\pi_{sm} = SPK\{s\}$: $F_1 = g^s \land F_2 = h^s (n_{\lambda})$ to AA. In the Authentication protocol, M and H jointly generate the signature of knowledge $\sigma = SPK\{\beta, \beta s, e, s\} : \bar{A} = g_{to}^{\beta_1} g^{\beta_{sp}} \wedge B = K^{\gamma} (n_{sp})$. According to the simulability of the signature of knowledge, the TPM private key $s$ and member credential $cre$ cannot be extracted from $\pi_{sm}$ and $\sigma$ even if SP and AA are collusive, so the identity of U cannot be determined. In addition, in each Authentication protocol, M randomly selects an element $B$ in group $G_1$ and calculates $K = B^{\gamma}$. According to the DDH assumption, even if SP conspires with AA, the element pairs $(B, K)$ and $(B^{\gamma}, K^{\gamma})$ produced by M in different authentication transcripts cannot be correlated.

Soundness. For the malicious user $U^*$, assume that he/she does not have a valid member credential $cre$, or that his/her attribute set $\mathbf{A}$ does not satisfy the access policy $\mathbf{P}$ defined by SP, or that his/her TPM private key has been compromised. It can be proved that he/she will not be able to pass the authentication process with SP. The function of the signature of knowledge $\sigma$ is to force $U^*$ to prove to SP that he/she has a valid member credential and his/her TPM private key has not been disclosed. According to the unforgeability of the signature of knowledge, $U^*$ cannot cheat SP by forging $\sigma$. Moreover, according to the security of the underlying CP-ABE encryption scheme, in the case of $\mathbf{P} \not\subseteq \mathbf{A}$, $U^*$ will not be able to recover the challenge string $n_{sp}$ from the challenge ciphertext $CT$ provided by SP, so $U^*$ will fail to generate $\sigma$.

Coalition-resistance. For the malicious users $U^1, U^2$, suppose they have the decryption keys $sk_{\lambda_1}$ and $sk_{\lambda_2}$ respectively. Suppose that the ciphertext $CT$ provided by SP is generated by access structure $\mathbf{P}$, which satisfies $\mathbf{P} \not\subseteq \mathbf{A}_1, \mathbf{P} \not\subseteq \mathbf{A}_2$. According to the generation process of decryption key in the underlying CP-ABE scheme, it can be concluded that $sk_{\lambda_1} = (g^{s/(a, \lambda_1)}, h^{(s-1)/a}), sk_{\lambda_2} = (g^{s/(a, \lambda_2)}, h^{(s-1)/a})$. 


In other words, due to the existence of unknown random numbers \( s_i, s_j \ (s_i \neq s_j) \) in the exponential part of \( sk_{\alpha_i} \) and \( sk_{\alpha_j} \), \( U_1^* \) and \( U_2^* \) cannot merge their decryption keys, that is, they will fail to launch collusion attacks.

6. Performance analysis

We compare the new system with several previous systems in Table 1. First of all, the new system and the system in [6] are based on ABE, and other systems are based on ABS or ABGS. The decryption key of the new system contains only two group elements, while in other systems, the length of decryption key grows linearly with the size of users’ attribute set. In terms of the efficiency of the authentication protocol, the new system has obvious advantages, that is, users’ computational complexity is \( O(|P|) \). In contrast, in other systems, users’ computational complexity is \( O(n - |P|) \).

Each system adopts different access policies. It should be acknowledged that among the four type of access policies involved in the comparison, LSSS policy and attribute tree are more flexible. Finally, the new system is based on a Trusted Platform (TP), while other systems can only be deployed on the standard PC platforms.

| System       | Type   | Length of Decryption Key | Authentication Efficiency | Access Policy | Computing Platform |
|--------------|--------|--------------------------|---------------------------|---------------|-------------------|
| Khader[3]    | ABGS   | \( O(A) \)               | \( O(P) \)               | Attribute tree | PC                |
| Yang et al.[5]| ABGS   | \( O(A) \)               | \( O(P) \)               | Attribute tree | PC                |
| Zhou et al.[6]| ABE    | \( O(A) \)               | \( O(P) \)               | Attribute tree | PC                |
| Li et al.[7] | ABS    | \( O(A) \)               | \( O(P) \)               | Threshold     | PC                |
| Lian et al.[8]| ABS    | \( O(A) \)               | \( O(P) \)               | LSSS          | PC                |
| Li et al.[9] | ABS    | \( O(A) \)               | \( O(P) \)               | LSSS          | PC                |
| Ours         | ABE    | \( O(A) \)               | \( O(n - |P|) \)          | AND gates     | TP                |

Now, we analyze the performance efficiency of each participant in the Authentication protocol. We use the symbols \( Exp(G_i) \) and \( Exp(G_j) \) to represent performing one single exponential operation in groups \( G_i \) and \( G_j \) respectively, and \( P \) to perform one bilinear pairing operation. It’s computation cost is \( (n - |P| + 4)Exp(G_i) + (n - |P|)Exp(G_j) + Exp(G_r) + 3P \), M’s computation cost is \( 4Exp(G_i) + 2Exp(G_j) \), and \( 2T \)’s computation cost is \( (n - |P| + 3 + |RL|)Exp(G_i) + nExp(G_j) + 2P \). It should be pointed out that by introducing the technique of pre-computation, the operation efficiency of M can be significantly improved, that is, the computation cost of M can be reduced to \( Exp(G_i) + Exp(G_j) \).

7. Conclusion

In this work, we provide a lightweight ABA system based on DAA. In the new system, the tamper-resistant TPM chip is responsible for storing its short private key for decryption and performing critical computing tasks in the authentication phase. Meanwhile, the host is responsible for performing remaining non-critical computing tasks. Compared with previous similar systems, the advantages of the new system are that it can enhance the level of privacy protection of users and can effectively resist clone attacks and collusion attacks launched by malicious users. In future research, we will improve the security model of ABA systems, design ABA systems supporting more flexible access policies, and design lightweight ABA systems that conforms to the TPM 2.0 specification.

Acknowledgments

This work was supported in part by the Project of Shandong Province Higher Educational Science and Technology Program under Grant J17KA081, in part by the Undergraduate Education Reform Project of Higher Education in Shandong Province under Grant M2018X245, in part by the Scientific...
Research Project of Shandong Youth University of Political Science under Grant XJPY2021, and in part by the Project of Educational Reform and Research in Shandong Youth University of Political Science under Grant JG201905.

References

[1] Belguith S, Kaaniche N and Hammoudeh M 2019 Analysis of attribute-based cryptographic techniques and their application to protect cloud services Transactions on Emerging Telecommunications Technologies (Preprint 10.1002/ett.3667)

[2] Goyal V, Pandey O, Sahai A and Waters B 2006 Attribute-based encryption for fine-grained access control of encrypted data Proc. of ACM CCS 2006 (New York: ACM Press) p 89

[3] Khader D 2009 Attribute-based authentication scheme Ph. D thesis University of Bath

[4] Emura K, Miyaji A and Omote K 2009 A dynamic attribute-based group signature scheme and its application in an anonymous survey for the collection of attribute statistics Information and Media Technologies 4 1060-75

[5] Yang H and Oleschchuk V A 2015 A dynamic attribute-based authentication scheme Proc. of C2SI 2015 (Berlin: Springer) p 106

[6] Zhou J and Cao Z 2012 PSCPA: patient self-controllable privacy-preserving cooperative authentication in distributed m-healthcare systems Cryptology ePrint Archive (2012/044)

[7] Li J, Au M H and Susilo S 2010 Attribute-based signature and its applications Proc. of ASIA CCS 2010 (New York: ACM Press) p 60

[8] Lian Y, Huang X and Mu Y 2014 SA3: Self-adaptive anonymous authentication for dynamic authentication policies Future Generation Computer Systems 30 133-39

[9] Li M, Huang X, Liu J K, Xu L and Wu W 2015 Cooperative attribute-based access control for enterprise computing system International Journal of Embedded Systems 3-4 191-202

[10] Camenisch J, Drijvers M and Lehmann A 2017 Anonymous attestation with subverted TPMs Proc. of CRYPTO 2017 (Berlin: Springer) p 427

[11] Brickell E and Li J 2010 A pairing-based DAA scheme further reducing TPM resources Proc. of TRUST 2010 (Berlin: Springer) p 181

[12] Dietrich K 2010 Anonymous RFID authentication using trusted computing technologies Proc. of RFIDSec 2010 (Berlin: Springer) p 91

[13] Chen L, Dietrich K and Löhr H 2011 Lightweight anonymous authentication with TLS and DAA for embedded mobile devices Proc. of ISC 2010 (Berlin: Springer) p 84

[14] Liu X and Zhang B 2016 Improved endorsed e-cash system with DAA-A Journal of Computer Research and Development, 53 2412-29

[15] Liu X, Xu Q and Zhang B 2018 Lightweight multi-coupon system for multi-merchant environments with DAA Journal on Communications 37 30-45

[16] Kumar V, Li H, Luther N, Asokan P, Park J M, Bian K, Weiss M B H and Znati T 2018 Direct anonymous attestation with efficient verifier-local revocation for subscription system Proc. of ASIA CCS 2018 (New York: ACM Press) p 567

[17] Guo F, Mi Y, Susilo W, Wong D S and Varadharajan V 2014 CP-ABE with constant-size keys for lightweight devices IEEE Transactions on Information Forensics and Security 5 763-71

[18] Camenisch J and Stadler M 1997 Efficient group signature schemes for large groups Proc. of CRYPTO’97 (Berlin: Springer) p 410

[19] Camenisch J, Drijvers M and Hajny J 2016 Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs Proc. of ACM WPES 2016 (New York: ACM Press) p 123