Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Intelligent Manufacturing—Article

一种面向 CAD 装配模型具有完整性校验的新型属性加密方法

杨月婷 [a]，**何发智** [a,b,*]，Soonhung Han [c]，**梁亚倩** [a]，**程媛** [d]

[a] *School of Computer Science, Wuhan University, Wuhan 430072, China*
[b] *State Key Laboratory of Digital Manufacturing Equipment and Technology, Huazhong University of Science and Technology, Wuhan 430074, China*
[c] *Division of Ocean Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea*
[d] *School of Information Management, Wuhan University, Wuhan 430072, China*

ARTICLE INFO

Article history:
Received 28 November 2019
Revised 16 July 2020
Accepted 19 March 2021
Available online 29 April 2021

关键词
信息安全
云设计和云制造
协同设计
CAD装配模型
基于属性的加密

摘要

云制造是实现智能制造的三大关键技术之一。本文提出了一种新的基于属性的计算机辅助设计（CAD）装配模型加密方法，有效地支持云制造中协同设计场景的层次访问控制、完整性验证和变形保护。设计了装配层次访问树（AHAT）作为层次访问结构。部件密文（ACT）文件中包含与属性相关的密文元素，其适用于内容密钥解密而不是CAD装配体文件。我们修改原始的默克尔树（MT）并重建装配体MT。所提出的ABE框架具有将变形保护方法与CAD模型的内容保密性相结合的能力。在标准假设下，所提出的加密方案被证明是安全的。在典型的CAD装配模型上进行的实验仿真表明，该方法在应用中是可行的。

1. 引言

正如发表在*Engineering*期刊上的一篇综述性论文[1]所述，智能制造是最先进的产品开发理念，包括智能制造技术、物联网（IoT）制造和云制造[1,2]。随着云计算的发展和应用[3–5]，传统的计算机辅助设计（CAD）、计算机辅助工程（CAE）和计算机辅助制造（CAM）系统正在向基于云的设计和制造（CBDM）[6–8]转移，给企业带来了新的信息安全问题，尤其对中小企业（SME）而言[9]。

由于资金和资源的限制，中小企业无法像大公司那样构建私有云。著名的公共云服务提供商（CSP）经历了各种各样的安全问题，因此，半可信或不可信的公共云在基于云的协同设计过程中挑战了中小企业的信息安全[10–13]。作为协同产品开发的核心组成部分[14–18]，CAD模型包含丰富的知识产权，因此会遇到安全问题。信息安全取决于工业云的可靠性[19,20]。CBDM的一个重要安全问题是如何避免在协同设计环境中非法访问CAD模型中包含的机密信息[21–23]。

一种典型的访问控制方法是应用标准加密技术，如基于属性的加密（ABE）[24]。但是，将ABE访问控制简单地引入CAD装配模型是低效和不灵活的。一些灵活的访问控制方法已经被报道用于云计算[25–28]。因此，如何开发一种高效灵活的访问控制方法来保护外包

* Corresponding author.
E-mail address: fzhe@whu.edu.cn (F. He).

英文原文: Engineering 2021, 7(6): 787–797
引用本文: Yueting Yang, Fazhi He, Soonhung Han, Yaqian Liang, Yuan Cheng. A Novel Attribute-Based Encryption Approach with Integrity Verification for CAD Assembly Models. *Engineering*, https://doi.org/10.1016/j.eng.2021.03.011

和协同设计的CAD装配模型仍然是CBDM面临的一个挑战。

本文提出了一种新的基于ABE的CAD装配模型完整性验证方法。与现有的密文策略ABE（CP-ABE）和相关方法[24–28]相比，提出了一种分层访问控制加密方案，该方案能够为具有不同权限级别的用户提供灵活的身份验证，以合法访问CAD装配模型。

本文的其余部分组织如下：第2节对相关工作进行了回顾；第3节讨论了设计目标，并对问题的构建进行了阐述；第4节提出了一种基于云的装配模型共享体系结构；第5节详细阐述了该方法的加密方案，并对其安全性进行了验证和理论分析；第6节演示了所提出的加密方案的性能；最后，在第7节对论文进行总结。

2. 相关工作

2.1. 访问控制

访问控制是一种重要的数据保密和隐私保护方法，它起源于访问矩阵的概念[29–33]。一种 CAD 环境中的访问控制框架（FACADE）已经被提出，以保护CAD模型[34]，还提出了一种协同设计和数据管理系统的数据安全模型，将多种安全技术与访问控制相结合[35]。Chang等[36]报道了一种基于多种方法的访问控制系统，用于共享CAD设计图纸。Speiera等[37]使用混合访问控制进行产品数据安全处理。

基于角色的访问控制是协同设计的主流方法[38,39]。然而，随着复杂流程的扩展，协同设计用户和产品模型可能出现“角色爆炸”问题。此外，现有的访问控制方法基于单个模型文件，因此是不灵活的。

2.2. 加密方法

加密在多媒体数据中得到了广泛的应用[40]。Nishchal和Naughton [41]提出了一种基于光学原理的多级加密体系结构，可用于处理具有视差和多重共享的三维（3D）全息图。Huang等[42]报道了一种基于虚拟全息的三维立方体数据加密方法。将该方法应用于计算机模拟全息的三维立方体全息图像的生成，并在此基础上进行了加密处理。Kim与Yoo [43]以及Chen与Tsai [44]提出了一种装配实体模型的分层加密方法，不同的用户可以访问装配模型文件不同部分的数据。文件的每一级都用不同的密钥加密，每个密钥只授权给指定的用户使用。研究人员还将加密的概念扩展到形状变形[45–48]。

2.3. 基于属性的加密

基于模糊身份的加密（即ABE）是支持细粒度访问控制的最有前途的加密原语[24]。目前，ABE主要分为两类：CP-ABE [28]和关键政策ABE（KP-ABE）[49]。在CP-ABE中，密文与数据所有者定义的访问结构相关联，而密钥与属性相关联。相反，在KP-ABE中，密文与属性相关联，而密钥与数据所有者定义的访问结构相关联。这两个方案都是在单个文件场景中构建的。

针对多文件场景，一些基于层次属性的解决方案已经被研究出来。Miao等[25]将层次数据的思想引入云计算中基于属性的密钥搜索。Wan等[26]在基于属性集的加密方案的基础上，提出了一种基于层次属性集的加密（HASBE）方案，以实现多文件场景下更精确的属性满足策略。然而，分层访问结构过于复杂，无法应用于大型CAD模型。Wang等[27]提出了一种文件层次结构CP-ABE（FH-CP-ABE），其中密文装配体递归公式中的漏洞可能导致非法访问。

2.4. 贡献

对于访问控制认证，本文提出了一种新的CAD装配模型的ABE方案，称为CAD装配层次文件CP-ABE（CAD-CP-ABE）方案。该技术方法采用对称加密算法进行明文加密，采用CAD-CP-ABE方案进行内容密钥管理。

与现有的CP-ABE技术不同，该方案中上层节点的接入结构比下层节点更简洁。因此，我们重新定义节点定义并提交一组新的生成规则，以避免过多的冗余节点。该方法使层次访问结构装配层次访问树（AHAT）适用于CAD装配模型。AHAT包含文件节点、属性节点和阈值节点。部件密文（ACT）文件包含AHAT和所有密文元素，将由具有合法访问权限的共同设计用户使用。

在完整性验证方面，在修改原有默克尔树（MT）后，本文提出了一种装配体MT技术，以防止CAD文件被非法删除或添加到云服务中。我们还采用了基于变形的技术来保护形状信息。这两种方法结合在一起以增强我们的方法。

3. 问题表述

在介绍体系结构（第4节）之前，我们分析了有关设计链管理（DCM）和协作设计的信息安全问题[38,50–52]。文献[50]讨论了一个典型的DCM协作模型。该模型为协作建立了6个层次。协作问题包括信任通信、协商和权限分配。

在基于云的协作过程中，协作者不仅要与他人协商，还要处理安全问题。因此，身份验证、完整性和信息隐私是信息共享的关键方面。

基于以上分析，我们正式定义了我们的问题，并指出了我们的设计目标。

3.1. 威胁模型

提出的体系结构包括4个实体：数据所有者、数据用户、授权中心和CSP。数据所有者是可信的，数据用户是由权威机构授权和协作的。授权中心是一个完全可信的实体，负责生成和分发公钥和密钥（SK）。CSP是云系统中一个半可信的外包实体；因此，数据可能被非法访问，或云服务可能会偏离规定的协议并发起数据完整性攻击。为了加强信息的机密性和层次访问控制，数据所有者首先对CAD模型的私有特征进行变形，然后使用基于属性的访问策略对数据文件进行加密，最后将数据文件外包到CSP中。为了解密来自不同数据所有者的共享数据文件，数据用户向管理局提交其属性以获得SK。

3.2. 设计目标

提出的方法旨在实现以下功能和安全目标：

身份验证。应通过有效的访问权限访问每个CAD模型数据文件。我们的方法可确保明文数据不会被泄露。对手无法从ACT文件中获得任何有用的信息。除了实现授权之外，我们还确保上层特权用户可以访问其所有下层特权用户文件。

完整性。CAD装配模型通常由一组数据文件组成。必须确保模型的任何文件都不会被篡改、添加或删除。有了ABE，文件的明文可以完全隐藏。这种完整性确保了CAD模型的固定树结构不会被CSP或恶意访问者通过装配体MT技术篡改。

保密。由于机密信息与合作者共享，而合作者可能是潜在的竞争对手，因此可能会发生信息泄漏。通过在共享CAD模型草图之前对其进行变形，可以解决此问题。

3.3. 预备工作

双线性映射：设p是素数，G_0和G_T是模p的两个乘法整数组。G_0的生成元是g。

双线性映射 e：$G_0 \times G_0 \rightarrow G_T$满足以下特性。

• 双线性——对于任何$u, v \in G_0$及$a, b \in Z_p$, $Z_p = \{0, 1, 2, ..., p-1\}$，有$e(u^a, v^b) = e(u, v)^{ab}$。

• 非退化性——存在$u, v \in G_0$，使得$e(u, v) \neq 1$。

• 可计算性——对于$u, v \in G_0$，存在一个有效计算e(u, v)。

定义1：双线性Diffie-Hellman（BDH）生成器。如果一个随机算法Γ以一个安全参数k（$k > 0$）作为输入，并输出对两个乘法循环群G_0和G_T的描述、公共素数阶p，以及在k次多项式时间内可以有效计算的双线性映射e，即$G_0 \times G_0 \rightarrow G_T$，那么该算法称为BDH参数生成器。

定义2：行列式双线性Diffie-Hellman（DBDH）问题。设G_0、G_T以及e是上述参数生成器的输出，并令g是G_0的生成元。那么，DBDH问题定义为，给定$< g, g^a, g^b, g^c, T >$，其中随机元素$a, b, c \in Z_p$，$T \in G_T$，判断等式$e(g, g)^{abc} = T$是否成立在多项式时间内是计算困难的。

MT：在计算机科学中，哈希树（hash tree）是一种类似树的数据结构，也称为MT [53]。如图1所示，每个叶节点使用其自身的哈希值作为其标签[如H3 = hash(A)]，而非叶节点使用其子节点标签的加密哈希作为其标签。MT可以验证具有以下特征的大型数据结构的内容。

• MT是一种树状结构，具有所有树状结构特征。

• 在不检查整个数据集的情况下，可以简洁地证明一个数据是否属于一个数据组。

• MT中每个节点的哈希值将证明数据内容的完整性和正确性。

4. 方法概述

4.1. 系统组织架构

图2展示了我们为CBDM提出的方法的系统架构。

授权中心：授权中心是一个完全受信任的实体，可以验证用户的身份属性。

数据所有者：数据所有者将通过CSP存储和共享CAD装配模型。该实体负责创建装配体MT和AHAT，变形草图以及执行加密功能。它将一个模型的加密文件、一个ACT文件和一个装配体MT加载到CSP。

用户：用户将从一台云服务器（B）下载ACT文件

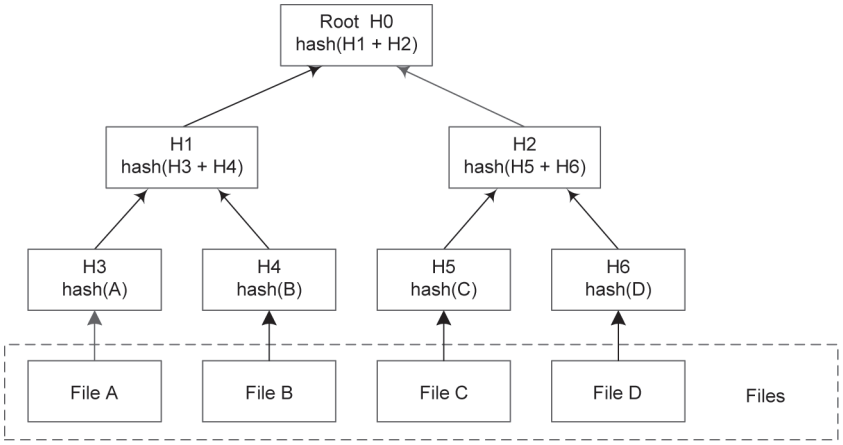

图1. 一个MT的例子。A、B、C和D是4个需要被MT加密的文件；H0、H1、H2、H3、H4、H5和H6是MT中节点的标签。

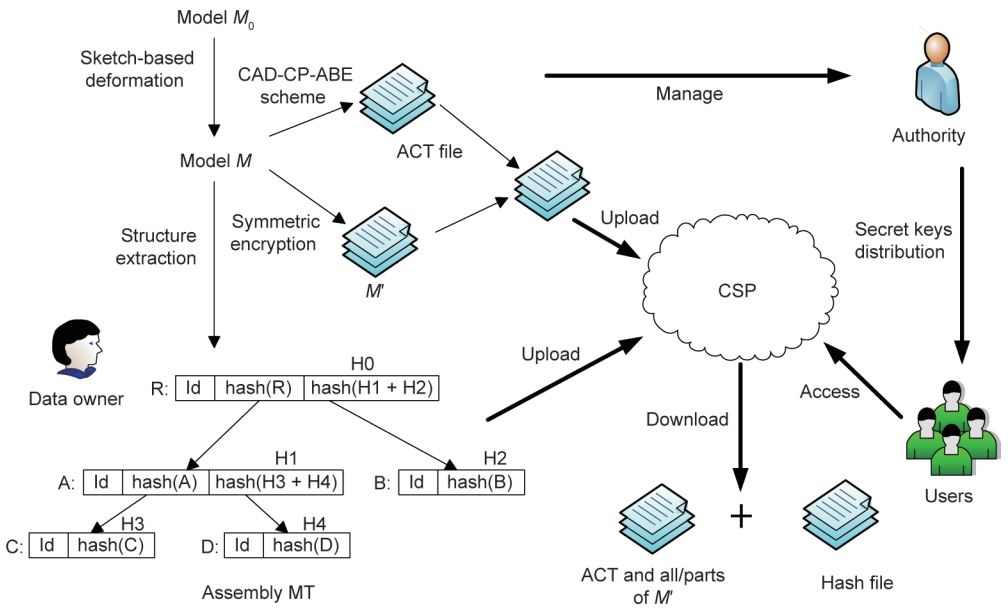

图2. CBDM装配体MT的方法的体系结构。A、B、C、D和R是M的5个文件。M_0：初始的CAD装配体模型；M：变形的CAD装配模型；M'：M的密文；Id：装配体MT中每个文件节点的标识。

以及加密文件的全部或部分。云服务器B执行解密功能。用户将通过另一个云服务器（A）验证下载文件的结构完整性。

CSP：CSP是提供密文存储和传输服务的半信任外包实体。

4.2. 方法基础

CAD装配模型的安全协同设计涉及三个构建块：装配体MT、基于变形的保护和CAD-CP-ABE方案。

如图所示。如图3（a）、（b）所示，装配体Assem02具有固定的结构，可以抽象地显示为树形图。每个零部件（零件和装配体的统称）成为该树形图的一个节点。

我们构建了一个装配体MT以支持完整性验证，如图3所示。在装配体MT中有两种类型的节点。部分（叶）节点表示为[identity (Id), value]对，其中，value是通过抗冲突哈希函数[如消息摘要算法5（MD5）和安全哈希算法]计算出的叶子文件的哈希（SHA）。装配体（非叶）节点表示为[Id, value1, value2]对，其中value1等于其哈希值，而value2等于由所有子级哈希顺序连接的字符串的哈希值。

当用户可以特权访问Assem6的所有文件并将Id Assem6-1提交给CSP时，云生成的正确哈希值文件的内容应为：[Assem6-1, H4, hash(H1 + H2)]；[Part004-1, H1]；[Part003-1, H2]，如图3（c）所示。用户将计算下载文

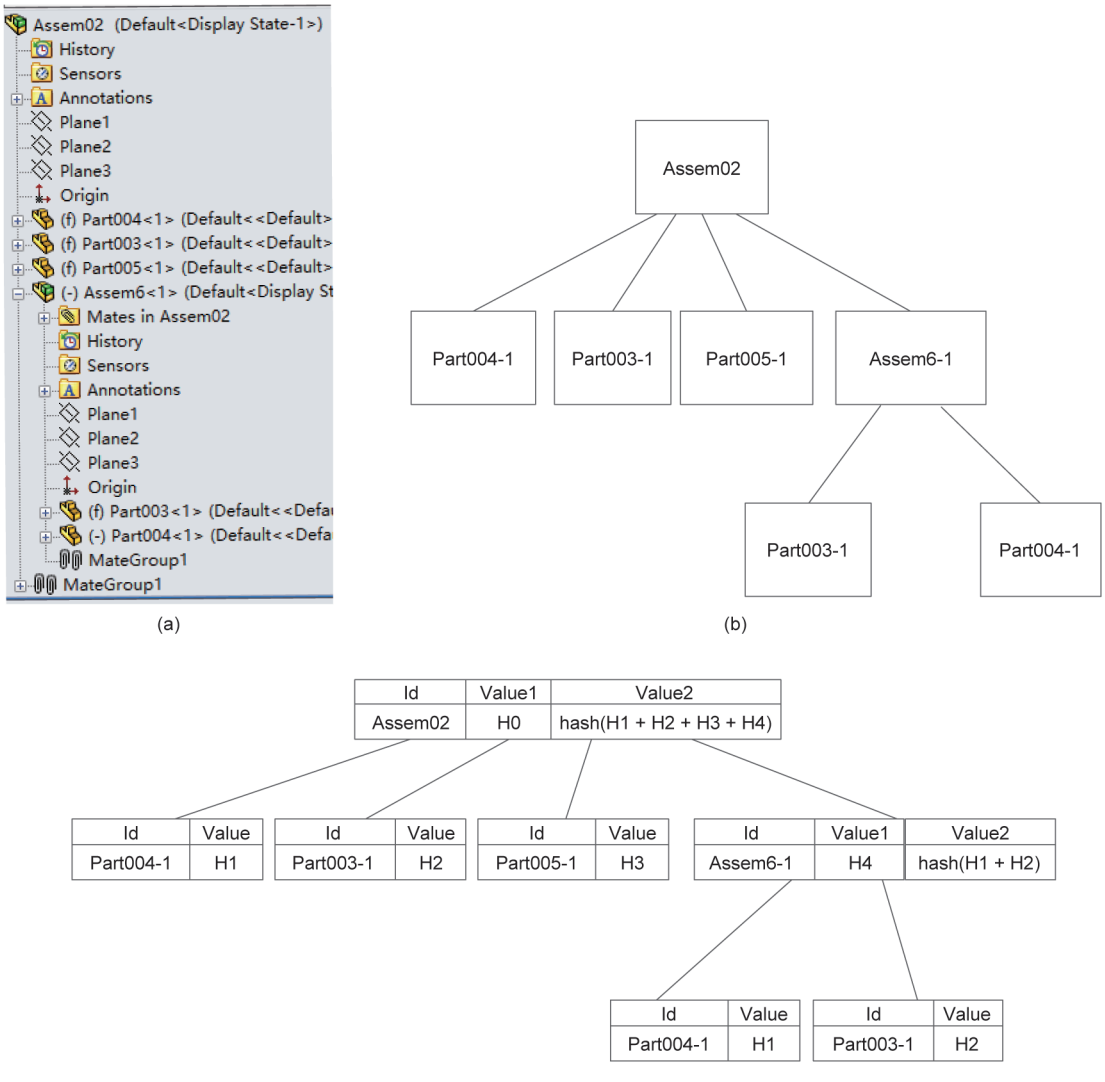

图3. Assem02的说明性示例。（a）SolidWorks中Assem02的装配结构；（b）Assem02的抽象结构树；（c）Assem02的装配体MT。

件的哈希并将它们与接收到的哈希进行比较。如果文件已被修改或结构已被破坏，则用户可以很容易地发现这些问题。

4.2.1. 基于变形的保护

典型的CAD模型由各种特征$\{F_i\}$（一组模型特征）组成，如图4（a）所示。基于一系列约束和草图$\{S_i\}$（一组模型特征草图）创建特征，这两个约束和草图都确定了模型形状。如果将变形方法应用于特征和基准，则CAD模型的有效性将受到影响。我们采用基于草图的变形方法来隐藏CAD模型的机密信息。草图S_i由草图元素和约束元素组成。每个草图S_i具有表示为$(x_{i,1}, x_{i,2})$或$(x_{i,1}, x_{i,2}, x_{i,3})$的草图点，并将其合成为草图矩阵$\mathbf{S}_\mathrm{M}$。

我们使用变换矩阵$\mathbf{T}_\mathrm{M}$实现参数变形。选择矩阵$\mathbf{T}_\mathrm{M}$的参数后，我们将n的值从0逐渐增加，直到草图通过$\mathbf{T}_\mathrm{M}$变形不会破坏模型约束。通过将$\mathbf{S}_\mathrm{M}$乘以$\mathbf{T}_\mathrm{M}$可以得到一个新的草图矩阵$\mathbf{S}_{\mathrm{M}'}$，如式（1）所示。

这种变形方法对于CAD模型来说是鲁棒且灵活的，因为可以根据加密矩阵$\mathbf{T}_\mathrm{M}$将草图恢复为原始形状，并且还可以轻松地将CAD模型恢复为原始状态。

$$\underbrace{\begin{bmatrix} x_{1,1} & x_{1,2} \\ \vdots & \vdots \\ x_{n,1} & x_{n,2} \end{bmatrix}}_{\mathbf{S}_\mathrm{M}} \times \mathbf{T}_\mathrm{M} = \underbrace{\begin{bmatrix} x_{1,1'} & x_{1,2'} \\ \vdots & \vdots \\ x_{n,1'} & x_{n,2'} \end{bmatrix}}_{\mathbf{S}_{\mathrm{M}'}} \tag{1}$$

二维和三维特征的转换矩阵定义如下：

$$\mathbf{T}_{\mathrm{M}2\times2} = \begin{bmatrix} a_{1,1} \cdot \eta^n & a_{1,2} \cdot \lambda^n \\ a_{2,1} \cdot \lambda^n & a_{2,2} \cdot \eta^n \end{bmatrix}$$

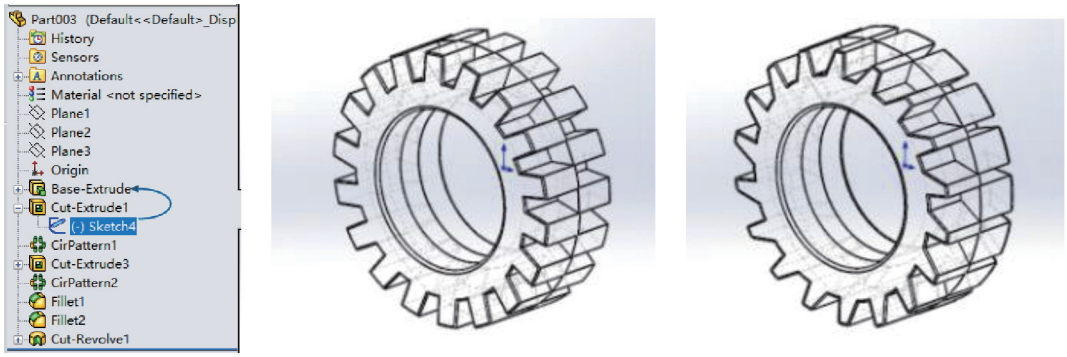

图4. Part003的特征草图变形的示例。（a）SolidWorks中Part003的FeatureManager；（b）原始Part003；（c）变形的Part003。

$$\mathbf{T}_{M3\times3}=\begin{bmatrix} a_{1,1}\cdot\eta^n & a_{1,2}\cdot\lambda^n & a_{1,3}\cdot\lambda^n \\ a_{2,1}\cdot\lambda^n & a_{2,2}\cdot\eta^n & a_{2,3}\cdot\lambda^n \\ a_{3,1}\cdot\lambda^n & a_{3,2}\cdot\lambda^n & a_{3,3}\cdot\eta^n \end{bmatrix}$$

式中，$a_{i,j}$表示在0.9和1.1之间随机选择的一个十进制数；η和λ是两个系数，满足$0<\eta,\lambda<1$；n是从0开始的整数。图4对变形进行了说明。图4（a）中，Cyt-Extrude1是一个私有功能，不能与其他人共享。我们用变换矩阵修改其Sketch4，以获得变形的Part003，如图4（c）所示。

4.2.2. CAD-CP-ABE 方案

CK管理方案是基于双线性映射定义和CP-ABE加密策略的，它由4个功能组成：Setup、KeyGen、Encrypt和Decrypt。

（1）(PK, MSK) ← Setup(1^k)。此功能输入安全参数k和素数p，并输出公共密钥（PK）和主控SK（MSK）。

（2）(SK) ← KeyGen(PK, MSK, S)。此函数输入PK、MSK和一个用户S的一组属性，并为属性集S生成SK。

（3）(ACT) ← Encrypt(PK, CK, AT)。此函数输入PK、CK和一个含有所有属性的集合AT，并输出CK的ACT。

（4）(ck_i ($i\in[1, num]$)) ← Derypt(PK, ACT, SK)。该功能输入用户的PK、ACT文件和SK文件。SK由S描述。如果S满足AHAT的访问结构，则ck_i ($i\in[1, num]$)可以解密部分或全部CK。然后，使用相应的CK，即ck_i解密相应的文件m_i ($i\in[1, num]$)，其中num表示所有CK的数量。

4.3. 系统安全的协同设计过程

安全的共同设计过程包括以下步骤：

（1）变形私有特征。对于数据所有者（D）拥有的CAD装配模型M_0，将使用基于变形的方法隐藏装配内部零部件的私有形状特征（F_i）。共享之前，将M_0转移到新的CAD装配模型M中。

（2）构造一个装配体MT。D将构造一个装配体MT，如图3所示。

（3）制定加密过程。M的文件（即明文）将通过加密算法用CK = {ck_1, ..., ck_i, ...}加密为模型密文M' = {m'_1, ..., m'_i, ...}。D将首先生成一个AHAT，然后通过CAD-CP-ABE方案中的加密功能（即CAD-CP-ABE加密过程）为CK= {ck_1, ..., ck_i, ...}计算ACT文件。

（4）共享数据文件。D将装配体MT、M'和CK ACT文件上传到CSP。装配体MT分别存储在云服务器A上。M'和ACT存储在云服务器B上。

（5）验证结构完整性。协同设计者（U）可以向CSP发送一组文件，该CSP将装配体MT与其他共享文件一起存储在云服务器中。该服务器将返回一组哈希值以进行完整性验证。

（6）获得明文。U将其身份属性发送给受信任的授权中心以检索SK。ACT文件中的密文元素与SK组合以评估CK。然后，用CK对加密的模型文件M'解密。

5. CAD-CP-ABE 方案的详细过程

5.1. CAD-AP-ABE 方案的层次访问结构构造

图5（a）中的访问结构T1基于CP-ABE方案来解密源文件m1。每个非叶节点都是一个阈值节点，并且每个叶节点都与属性关联。根节点代表一个源文件。阈值为num1/num2，其中num1表示“需要满足条件的节点数”，而num2表示“子项总数”。

对于CAD装配模型结构，如图5（b）所示，较少用户将访问较高级别的节点。如果将属性节点插入模型

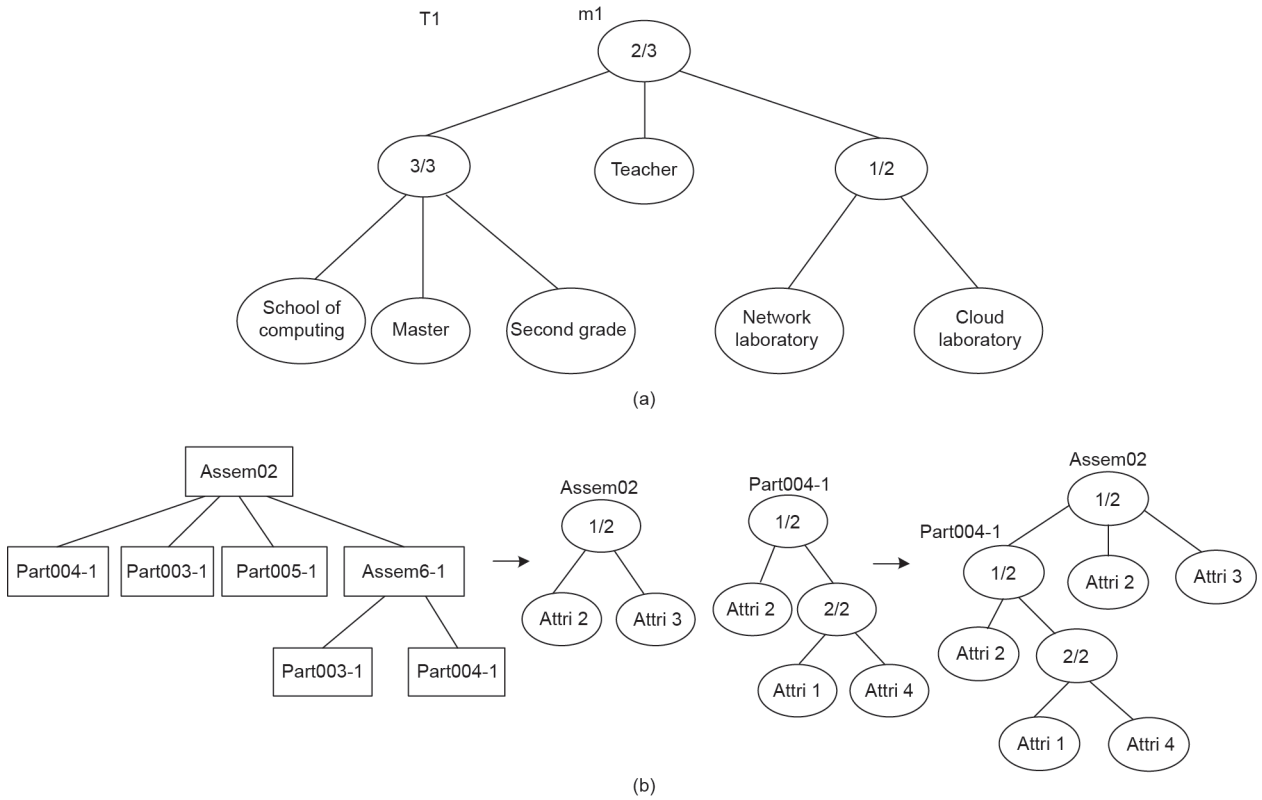

图5. CP-ABE方案中的访问结构示例。（a）访问结构树的示例。T1是m1的访问结构。（b）Assem02和Part004的分层访问结构。Attri：属性节点（attribute node）。

结构，则重复的属性节点将增加不必要的开销，如图5（b）所示。同时，重复的装配体节点也将增加开销。

因此，我们在方案中指定以下规则来生成AHAT：

（1）提取用于AHAT生成的集成装配模型结构。

（2）将结构分为组成节点和隐藏节点。由于节点2和节点3表示相同的属性，因此，如果它们具有相同的父节点1，或者如果节点2的父节点是节点3的祖先，则将节点2及其子节点设置为AHAT中的隐藏节点。

（3）为装配中的每个零部件插入属性节点和（或）阈值节点，以构造AHAT。为了降低AHAT的复杂性，有必要修剪属性结构。如果任何装配体节点与其父/祖先节点具有相同的访问属性结构，则切断这些属性并更改访问结构。

身份属性按层次结构定义如下：总工程师、副总工程师、项目工程师、工程师和助理工程师。对应的属性集合为AT = {1, 2, 3, 4, 5}。例如，我们将三个公司C1、C2和C3列为公司属性，并将它们的值分别定义为6、7和8。总属性设置为AT = {1, 2, 3, 4, 5, 6, 7, 8}。

如图6所示，存在一个描述访问结构并包含几个访问级别的AHAT。AHAT和节点的术语和功能如下：

(x, y)：此二进制表示AHAT中的非隐藏节点。x代表节点的行（从上到下），y代表节点的列（从左到右）。例如，在图6中，节点Assem02的二进制是(1, 1)，节点Part005-1的二进制是(2, 1)，并且级别3上的属性3的二进制是(3, 5)。

$\mathrm{num}_{(x, y)}$：HAT中(x, y)子级集合中非隐藏节点的数量。如图6中的$\mathrm{num}_{(2, 2)} = 2$。

$k_{(x, y)}$：非隐藏节点(x, y)的阈值，其中$0 < k_{(x, y)} \leqslant \mathrm{num}_{(x, y)}$。如果$(x, y)$是叶节点，则$k_{(x, y)} = 1$。例如，$k_{(1, 1)} = k_{(2, 2)} = 2$。

parent(x, y)：AHAT中节点(x, y)的父级。例如，图6中的parent(5, 1)= (4, 3)。

att(x, y)：与AHAT中的叶节点(x, y)关联的属性。

index(x, y)：返回与节点(x, y)关联的唯一值。对于给定密钥，索引值以任意方式唯一地分配给AHAT中的节点。

5.2. CK 的加密和解密过程

DBDH是一个双线性参数生成器。假定数据所有者与num个响应的CK（$\mathrm{CK} = \{\mathrm{ck}_1, \ldots, \mathrm{ck}_{\mathrm{num}}\}$）共享文件。此外，在CAD-CP-ABE方案中使用了两个哈希函数$H_1: \{0,1\}^* \rightarrow G_0$和$H_2: \{0,1\}^* \rightarrow G_{\mathrm{T}}$。

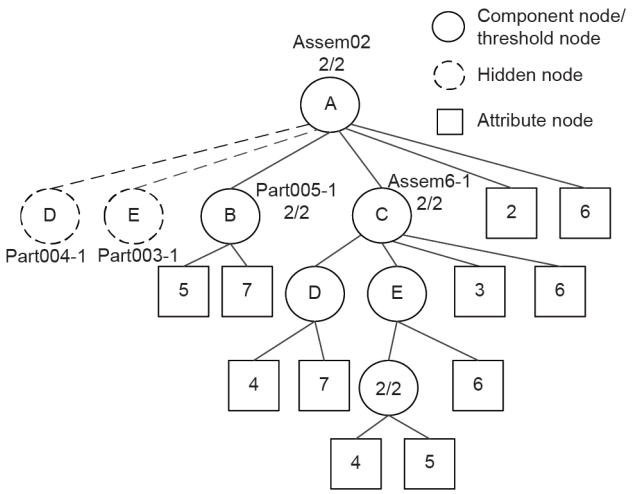

图 6. AHAT是装配模型的集成层次访问结构。

Setup(1^k)：权限在安全参数k和随机数$\alpha, \beta \in Z_p$内执行此功能。DBDH将输出PK和MSK，分别如式（2）和式（3）所示。

$$\mathrm{PK} = \{G_0, g, h = g^{\beta}, e(g,g)^{\alpha}\} \tag{2}$$

$$\mathrm{MSK} = \{g^{\alpha}, \beta\} \tag{3}$$

KeyGen(PK, MSK, S)：授权机构使用一个用户S的一组属性执行此功能，并创建SK，如式（4）所示，其中$r \in Z_p$且 $r_j \in Z_p$是为该用户随机选择的。D是正常的关键参数，D_j和D_j'是属于属性j的关键参数。D、D_j和D_j'组成SK。

$$\mathrm{SK} = \left\{D = g^{(\alpha+r)/\beta}, \forall j \in S : D_j = g^{r} \cdot H_1(j)^{r_j}, D_j' = g^{r_j}\right\} \tag{4}$$

在所提出的方法中，一个用户的属性集具有两个元素：职位属性和公司属性。因此，S通常是两个元组。

Encrypt(PK, CK, A)：数据所有者为$\mathrm{CK} = \{\mathrm{ck}_1, \ldots, \mathrm{ck}_{\mathrm{num}}\}$选择num个随机数$\{s_1, \ldots, s_{\mathrm{num}}\} \in Z_p$，并为所有组成节点($i$ = 1, 2, ..., num)计算C_i和C_i'，如式（5）所示。C_i和C_i'是属于ck_i的关键参数。

$$C_i = \mathrm{ck}_i \cdot e(g,g)^{\alpha s_i},\ C_i' = h^{s_i} \tag{5}$$

以自上而下的方式为每个非隐藏节点生成具有多项式规则的多项式$q_{(x,y)}$，如下所示：

（1）从根节点开始。

（2）$q_{(x,y)}$的度为$k_{(x,y)-1}$。

（3）如果(x, y)是组成节点，则$q_{(x,y)}(0) = s_i$。否则，$q_{(x,y)}(0) = q_{\mathrm{parent}(x,y)}(\mathrm{index}(x,y))$。$q_{(x,y)}$的其他多项式信息是随机选择的。

对于每个叶节点，数据所有者将计算$C^1_{(x,y)}$和$C^2_{(x,y)}$，如式（6）所示。$C^1_{(x,y)}$和$C^2_{(x,y)}$是用于解密节点(x, y)的两个关键参数。

$$C^1_{(x,y)} = g^{q_{(x,y)}(0)},\ C^2_{(x,y)} = H_1(\mathrm{att}(x,y))^{q_{(x,y)}(0)} \tag{6}$$

对于每个组成节点，数据所有者计算$C_{(x,y),l}$，如式（7）所示，其中子项子集是$\{\mathrm{child}_1, \ldots, \mathrm{child}_l, \ldots\}$。$C_{(x,y),l}$是在父节点和子节点之间使用的关键参数。

$$C_{(x,y),l} = e(g,g)^{\alpha \cdot q_{\mathrm{child}_l}(0)} \cdot H_2(e(g, C'_{\mathrm{child}_l}) \cdot e(g,g)^{\alpha \cdot q_{(x,y)}(0)}) \tag{7}$$

数据所有者输出集成的ACT文件，如式（8）所示。

$$\mathrm{ACT} = \left\{\mathrm{AHAT}, C_i, C_i', C^1_{(x,y)}, C^2_{(x,y)}, C_{(x,y),l}\right\} \tag{8}$$

Decrypt(PK, ACT, SK)：用户需要由S描述的PK和SK来解密ACT。

对于叶节点(x, y)，我们将DecryptNode(ACT, SK, (x, y))定义为式（9），其中$j = \mathrm{att}(x, y)$，且如果$j \notin S$，则DecryptNode(ACT, SK, (x, y)) = null。

$$\begin{aligned}\mathrm{DecryptNode}(\mathrm{ACT}, \mathrm{SK}, (x,y)) &= \frac{e(D_j, C^1_{(x,y)})}{e(D_j', C^2_{(x,y)})} \\ &= \frac{e(g^r \cdot H_1(j)^{r_j}, g^{q_{(x,y)}(0)})}{e(g^{r_j}, H_1(\mathrm{att}(x,y))^{q_{(x,y)}(0)})} \\ &= e(g,g)^{rq_{(x,y)}(0)}\end{aligned} \tag{9}$$

对于每个装配体/阈值节点，我们定义DecryptNode(ACT, SK, (x, y))，如式（10）所示，其中z是(x, y)的属性/阈值子集，$S_{(x,y)}$是AHAT中(x, y)的任意$k_{(x,y)}$大小的属性/阈值子集，$S'_{(x,y)} = \{\mathrm{index}(z) : z \in S_{(x,y)}\}$，以及val=index($z$)。

$$\begin{aligned}F_{(x,y)} &= \prod_{z \in S'_{(x,y)}} F_z^{\Delta \mathrm{val} S'_{(x,y)}(0)} = \prod_{z \in S'_{(x,y)}} (e(g,g)^{rq_z(0)})^{\Delta \mathrm{val} S'_{(x,y)}(0)} \\ &= \prod_{z \in S'_{(x,y)}} (e(g,g)^{rq_{(x,y)}(\mathrm{val})})^{\Delta \mathrm{val} S'_{(x,y)}(0)} = \prod_{z \in S'_{(x,y)}} e(g,g)^{rq_{(x,y)}(0)}\end{aligned} \tag{10}$$

由于装配体(x, y)的随机数s_i与其父级的随机数无关，因此z不能作为装配体节点。

接下来，$e(g,g)^{\alpha s_i}$可以通过式（11）进行计算，其中i是组成节点(x, y)的编号。

$$F'_{(x,y)}=\frac{e(C'_i,D)}{F_{(x,y)}}=\frac{e(h^{s_i},g^{(\alpha+r)/\beta})}{e(g,g)^{rq_{(x,y)}(0)}}=e(g,g)^{\alpha s_i},\ i\in[1,\mathrm{num}] \quad (11)$$

由于父文件需要使用所有子文件，因此(x, y)有权解密所有子文件。$F_{(x,y),l}$是解密的中间参数。我们可以使用式（12）为AHAT中的装配体节点(x, y)计算装配体child_l的$F_{(x,y),l}$。

$$F_{(x,y),l}=\frac{C_{(x,y),l}}{H_2[e(g,C'_l)\cdot F_{(x,y)}]}=e(g,g)^{\alpha q_{\mathrm{child}_l}(0)},\ l=1,2,\ldots \quad (12)$$

然后，通过执行式（13）解密相应的CK，即ck_i，其中i是组成节点(x, y)的编号。

$$\mathrm{ck}_i=\frac{C_i}{F'_{(x,y)}}=\frac{\mathrm{ck}_i\cdot e(g,g)^{\alpha s_i}}{e(g,g)^{\alpha s_i}},\ i\in[1,\mathrm{num}] \quad (13)$$

最后，使用ck_i解密相应的文件。

5.3. CAD-CP-ABE 方案的安全性证明

5.3.1. 安全性模型

在该方案中，用户的SK与属性集相关联，而ACT与访问结构相关联。我们方案的安全模型应该抵抗CPA。敌手A1和挑战者B1之间的CPA安全博弈要求A1挑选一个挑战性结构AT*，并且A1可以要求获得所有不满足AT*子结构的SK。

（1）初始化。A1在AT*处选择一个具有挑战性的结构并将其交付给B1。

（2）设置。B1运行Setup(1^k)算法并且发送PK给A1。

（3）查询阶段。A1选择一系列属性集（S, ..., S_w, $\forall i\in[1, w], S_i\notin$AT*）来重复地为SK询问B1。B1通过运行KeyGen(PK, MSK, S_i)算法来回答这些提问。

（4）挑战。A1选择两个长度相等的信息，即m_0和m_1作为挑战。然后B1随机选择一个比特$\mu\in\{0, 1\}$以及带有访问结构AT*的密文m_μ。最后，B1将密文ACT*交付给A1。

（5）查询阶段2。与查询阶段1相同。

（6）预测。A1输出一个预测比特$\mu'\in\{0, 1\}$。如果$\mu'=\mu$，A1赢得安全性博弈；否则博弈失败。A1赢得CPA博弈的好处被定义为$\mathrm{Adv}_{\mathrm{A1}}^{\mathrm{CPA}}(1^k)=|\Pr[\mu'=\mu]-1/2|$。

定义3： 如果没有概率多项式时间敌手A1能够赢得安全博弈，则CAD-CP-ABE方案对CPA是安全的。

5.3.2. 方案的安全性证明

定理1： 假设DBDH的假设在$<G_0, G_T>$成立，那么任何多项式敌手都不能有选择地破坏该方案。

证明： 假设敌手A1在选择性安全博弈中以不可忽视的优势$\varepsilon=\mathrm{Adv}_{\mathrm{A1}}^{\mathrm{CPA}}(1^k)$来反对我们的构建。挑战者B1能够以不可忽略的概率（$\varepsilon/2$）来区分DBDH元组D_{bdh}和随机元组D_{rand}。令e: $G_0\times G_0\to G_T$是一个高效可计算双线性映射，其中G_0是具有带着一个生成器g的素数阶p。挑战者随机选取参数$(a, b, c)\in Z_p$，随机值$\mu\in\{0, 1\}$，以及随机元素$\theta\in_R G_T$。如果$u=0$，那么挑战者B1设置$(g, A, B, C, T)=(g, g^a, g^b, g^c, e(g,g)^{abc})\in D_{\mathrm{bdh}}$；否则挑战者设置$(g, A, B, C, T)=(g, g^a, g^b, g^c, \theta)\in D_{\mathrm{rand}}$。ACT根据式（8）计算。

（1）初始化。敌手A1选择一个具有挑战性的结构AT*并将其交付给B1。

（2）设置。为了提供一个PK给A1，B1随机选择一个数$a'\in Z_p$，并且定义$\partial=a'+ab$。然后计算$e(g, g)^{\partial}=e(g, g)^a\cdot e(g, g)^{ab}$，同时设置$h=g^\beta=g^b$。对于给定的$\beta$，$g^\beta=g^b$。最后B1将PK交给A1。

（3）查询阶段。在这个阶段，A1可以通过向B1提交一个属性集$W_j=\{a_j, a_j\in\mathrm{AT}\}(a_j\notin\mathrm{AT}^*)$来询问SK。随后，B1随机选择一个数字$r'\in Z_p$并设置$r'=r-a$。B1可以获得$D=g^{(\partial+r')/\beta}=g^{(\partial+r-a)/\beta}$。然后，对于每个属性$a_j\in W_j$，B1需要随机选择$r_j\in Z_p$。B1按如下方式，即$D_j=g^{(r-a)}\cdot H_1(j)^{r_j}$，$D_j'=g^{r_j}$构造剩余的SK。最后，B1向A1发送SK。

（4）挑战。A1向B1提交两条长度相等的消息，即mess_0和mess_1。B1随机生成一个比特，$\mu\in\{0, 1\}$。经过AT*下的加密操作，B1以$C'=h^s=g^{\beta c}$, $C=m_\mu\cdot e(g, g)^{\partial s}=m_\mu\cdot e(g, g)^{(a'+ab)c}$计算ACT*。最后，B1将ACT*发送给A1。

（5）查询阶段2。与查询阶段1相同。

（6）预测。A1输出一个预测比特$\mu'\in\{0, 1\}$。如果$\mu'=\mu$，那么B1输出0以显示$(g, A, B, C, T)\in D_{\mathrm{bdh}}$。否则，B1输出1以显示$(g, A, B, C, T)\in D_{\mathrm{rand}}$。敌手A1在与挑战者B1的比赛中获胜的概率计算如下：

如果$(g, g^a, g^b, g^c, T)\in D_{\mathrm{bdh}}$，也就是说$T=g^{abc}$，那么

ACT*是一个有效的密文；在这种情况下，敌手A1的优势是ε。

$\Pr[\mathrm{B1}(g, A, B, C, T) \in D_{\mathrm{bdh}} = 0] = 1/2 + \varepsilon$。

如果$(g, g^a, g^b, g^c, T) \in D_{\mathrm{rand}}$，不等式$\mu' \neq \mu$成立。敌手A1拥有1/2的优势，且与$\mu'$上的分布无关。在这种情况下，敌手A1没有优势。

$\Pr[\mathrm{B1}(g, A, B, C, T) \in D_{\mathrm{rand}} = 0] = 1/2$。

最后，挑战者B1的优势如下：

$$\mathrm{Adv}_{\mathrm{B1}} = 1/2\{\Pr[\mathrm{B1}(g, A, B, C, T) \in D_{\mathrm{bdh}} = 0] + \Pr[\mathrm{B1}(g, A, B, C, T) \in D_{\mathrm{rand}} = 0]\} - 1/2 = 1/2(1/2 + \varepsilon + 1/2) - 1/2 = \varepsilon/2$$

5.4. 理论分析

设C_e为e运算（双线性对）。假设$|A_{\mathrm{a}}|$是属性节点数，A_{c}是将装配体节点作为子节点的装配体节点集，A_{u}是用户U的属性集。

存在k个CK，其中每个节点A_{c}都包含n个装配体节点作为子节点。在CAD-CP-ABE方案中，在生成AHAT的过程中切断了底层构件节点的一些属性节点。因此，当CK的数目固定时，加密时间与k、$n|A_{\mathrm{c}}|$和$|A_{\mathrm{a}}|$有关。

在我们的方法中，$|A_{\mathrm{u}} = 2|$是常数，这使得解密时间独立于叶节点。假设用户U有权访问根节点。因为满足根访问结构的内部节点的最小数量是两个，所以只有两个属性节点。根节点的计算如式（9）所示。解密时间与k和$n|A_{\mathrm{c}}|$有关。

此外，可通过式（8）获得ACT的大小，如表1所示，其中L是元素G_i, $i \in \{0, \mathrm{T}\}$的长度。

表1 CAD-CP-ABE (CK ={ck_1, ..., ck_k})的特征

Feature	Computing equation
Encryption time	$(2\|A_{\mathrm{a}}\| + k)\ G_0 + 2(n\|A_{\mathrm{c}}\| + k)G_{\mathrm{T}}$
Decryption time	$5C_e + (4 + n\|A_{\mathrm{c}}\| + 2k)G_{\mathrm{T}}$
The size of ACT	$(2\|A_{\mathrm{a}}\| + k)L_{G_0} + (n\|A_{\mathrm{c}}\| + k)L_{G_{\mathrm{T}}}$

6. 实验

6.1. 实验仿真

这种方法执行两个加密过程：明文加密和CK加密。对于明文加密，我们使用高级加密系统（AES）算法对装配体文件进行加密和解密。对于CK加密，我们基于Java配对密码（JPBC）库[54]实现了CK的CAD-CP-ABE方案。我们使用A型双线性映射。A型对构造在F_q域上的曲线$y^2 = x^3 + x$上。这种配对是对称的，r阶是$q + 1$的某个素数因子。A型需要两个参数rBits = 160。所有结果都是20个实验的平均值。

6.2. 实验结果

如图7所示，我们使用AES算法对汇编格式进行加密并转换为文本格式，解密过程与加密过程相反。实验验证了一种加密算法在装配体文件上的实用性，加密和解密过程不会破坏内容完整性。

如图8（a）所示，SK的生成时间近似线性。由于每次实验会选择一些新的参数，因此在线性关系中会产生轻微的计算误差。基于Pairing对象使用newElement()方法生成SK的时间低于2 s，整个过程的总时间不超过50 s。我们选择使用newRandomElement()方法加强SK生成的安全性，这会导致额外的时间成本。

图8（b）~（d）给出了加密和解密实验结果。如图8（b）所示，我们假设有不同的叶节点，每个叶节点具有两个层次文件。根据AHAT生成规则，CAD-CP-ABE中的叶节点数等于CP-ABE中的$|A_{\mathrm{a2}}|$。如图8（c）所示，存在固定叶节点（$N = 30$）的各种层次文件。图8（b）、（c）表明，结果越来越近似地遵循线性关系。显然，叶片节点的数量对CAD-CP-ABE中的时间成本影响较大。

CK的解密时间从根节点开始计算。在我们的方法中，对于CAD-CP-ABE中的根节点和CP-ABE中的每个装配体节点，只需要满足两个叶节点。当用户U获得文

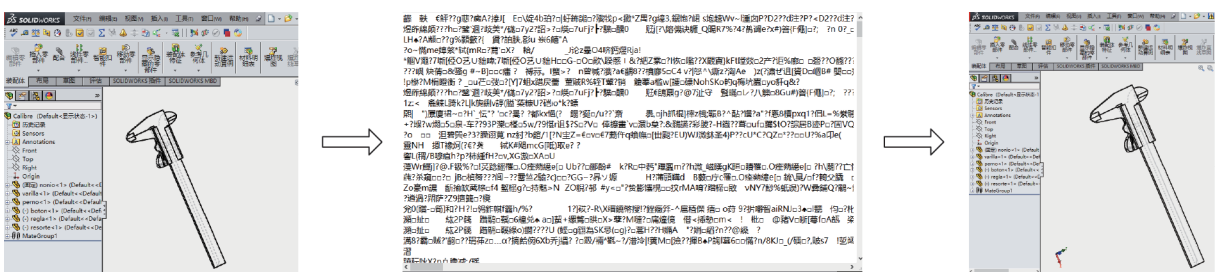

图7. 装配体文件使用AES算法进行加密和解密的示例。

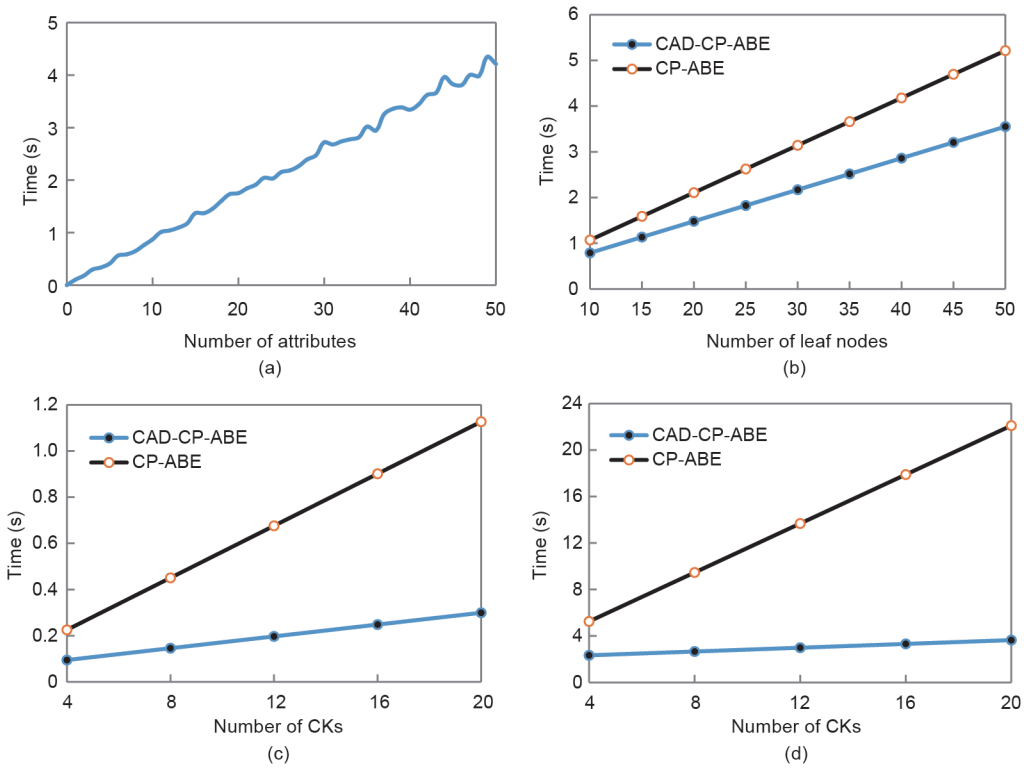

图8. CK加密和解密的实验结果。（a）SK生成时间和所有属性数；（b）两个CK的加密时间成本；（c）30个叶节点的加密时间成本；（d）来自根节点的所有CK的解密时间成本。

件A的CK时，*U*可以通过ACT文件逐层导出文件A下面的所有其他装配体节点的CK。如图8（d）所示，解密时间成本仅与CK的数目有关。实验表明，该方案提高了加密和解密效率。

7. 结论

本文提出了一种层次化的装配体文件共享方法，以保护云设计和制造时代面向外包和协同设计的CAD模型。这种方法结合了ABE方案、结构完整性检查和基于变形的CAD装配模型形状保护。仿真实验表明，该方法在计算效率和灵活性方面是可行的。

对于未来的工作，第一个方向是确定如何将形状加密从基于草图的CAD零件变形扩展到CAD装配变形。第二个方向是采用多核计算技术和优化方法[55–61]，以加速CAD大数据的加密和解密。第三个方向是将建议的方法扩展到其他多媒体数据[62–67]。最后，我们将把一个可搜索的加密方案集成到所提出的方法中[68,69]。

致谢

本课题得到了国家自然科学基金（62072348）和湖北省科技重大专项（下一代人工智能技术；2019AEA170）的支持。

Compliance with ethics guidelines

Yueting Yang, Fazhi He, Soonhung Han, Yaqian Liang, and Yuan Cheng declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Zhong RY, Xu X, Klotz E, Newman ST. Intelligent manufacturing in the context of industry 4.0: a review. Engineering 2017;3(5):616–30.
[2] Wang L, Chen X, Liu Q. A lightweight intelligent manufacturing system based on cloud computing for plate production. Mob Netw Appl 2017;22 (6):1170–81.
[3] Andreadis G, Fourtounis G, Bouzakis KD. Collaborative design in the era of cloud computing. Adv Eng Softw 2015;81:66–72.
[4] Tao F, Qi Q, Wang L, Nee A. Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: correlation and comparison. Engineering 2019;5(4):653–61.
[5] Chen Y. Integrated and intelligent manufacturing: perspectives and enablers. Engineering 2017;3(5):588–95.
[6] Wu D, Rosen DW, Wang L, Schaefer D. Cloud-based design and manufacturing a new paradigm in digital manufacturing and design innovation. Comput Aided Des 2015;59:1–14.
[7] Cai W, He F, Lv X, Cheng Y. A semi-transparent selective undo algorithm for multi-user collaborative editor. Front Comput Sci 2021;25(3):1–21.
[8] Wang J, Zheng P, Lv Y, Bao J, Zhang J. Fog-IBDIS: industrial big data integration and sharing with fog computing for manufacturing systems. Engineering 2019;5(4):662–70.
[9] Villa A, Taurino T. From industrial districts to SME collaboration frames. Int J

Prod Res 2018;56(1–2):974–82.
[10] Tehrani SR, Shirazi F. Factors influencing the adoption of cloud computing by small and medium size enterprises (SMEs). In: Proceeding of International Conference on Human Interface and the Management of Information; 2014 Jun 22–27; Heraklion, Greece. Berlin: Springer; 2014. p. 631–42.
[11] Cheng Y, Bi L, Tao F, Ji P. Hypernetwork-based manufacturing service scheduling for distributed and collaborative manufacturing operations towards smart manufacturing. J Intell Manuf 2020;31(7):1707–20.
[12] Zhang Y, Xi D, Yang H, Tao F, Wang Z. Cloud manufacturing based service encapsulation and optimal configuration method for injection molding machine. J Intell Manuf 2019;30(7):2681–99.
[13] Zhao C, Zhang L, Ren L, Tao F. Simulation platform for transaction processes in cloud manufacturing. Comput Integr Manuf Syst 2016;22(1):25–32.
[14] Demoly F, Roth S. Knowledge-based parametric CAD models of configurable biomechanical structures using geometric skeletons. Comput Ind 2017;92–93:104–17.
[15] Qin F, Gao S, Yang X, Li M, Bai J. An ontology-based semantic retrieval approach for heterogeneous 3D CAD models. Adv Eng Inform 2016;30(4):751–68.
[16] Liang Y, He FX, Zeng X. 3D mesh simplification with feature preservation based on whale optimization algorithm and differential evolution. Integr Comput Aided Eng 2020;27(4):417–35.
[17] Shen W, Li W. Collaboration computing technologies and applications. J Netw Comput Appl 2013;36(6):1577–8.
[18] Li W, Shen W. Collaborative design: new methodologies and technologies. Comput Ind 2008;59:853–4.
[19] Gong W, Wang QS, Chen HQ. Summarization on intelligent manufacturing information security certification feasibility research. Inf Technol Inf 2018;2–3:147–50.
[20] Chang SI, Chang IC, Li HJ, He TH. The study of intelligent manufacturing internal control mechanism by using a perspective of the production cycle. J Ind Prod Eng 2014;31(3):119–27.
[21] Kim H, Yeo C, Lee ID, Mun D. Deep-learning-based retrieval of piping component catalogs for plant 3D cad model reconstruction. Comput Ind 2020;123:103320.
[22] Liu Y, Wang L, Wang XV, Xu X, Zhang L. Scheduling in cloud manufacturing: state-of-the-art and research challenges. Int J Prod Res 2019;57(15–16):4854–79.
[23] Liu Y, Wang L, Wang XV, Xu X, Jiang P. Cloud manufacturing: key issues and future perspectives. Int J Comput Integr Manuf 2019;32(9):858–74.
[24] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceeding of Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2005 May 22–26; Aarhus, Denmark. Berlin: Springer; 2005. p. 457–73.
[25] Miao Y, Ma J, Liu X, Li X, Jiang Q, Zhang J. Attribute-based keyword search over hierarchical data in cloud computing. IEEE Trans Serv Comput 2020;13(6):985–96.
[26] Wan Z, Liu J, Deng RH. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans Inf Forensic Secur 2012;7(2):743–54.
[27] Wang S, Zhou J, Liu JK, Yu J, Chen J, Xie W. An efficient file hierarchy attributebased encryption scheme in cloud computing. IEEE Trans Inf Forensic Secur 2016;11(6):1265–77.
[28] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceeding of 2007 IEEE Symposium on Security and Privacy (SP '07); 2007 May 20–23; Berkeley, CA, USA. New York: IEEE; 2007. p. 321–34.
[29] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. Computer 1996;29(2):38–47.
[30] Oh S, Park S. Task–role-based access control model. Inf Syst 2003;28(6):533–62.
[31] Park J, Sandhu R. Towards usage control models: beyond traditional access control. In: Proceeding of the Seventh ACM Symposium on Access Control Models and Technologies; 2002 Jun; Monterey, CA, USA. New York: Association for Computing Machinery; 2002. p. 57–64.
[32] Park J, Sandhu R. The UCONABC usage control model. ACM Trans Inf Syst Secur 2004;7(1):128–74.
[33] Lampson BW. Protection. Oper Syst Rev 1974;8(1):18–24.
[34] Cera CD, Kim T, Han J, Regli WC. Role-based viewing envelopes for information protection in collaborative modeling. Comput Aided Des 2004;36(9):873–86.
[35] Yao L, Shao J, Sheng G, Zhang G. Research on a security model of data in computer supported collaborative design integrated with PDM system. In: Proceeding of Workshop on Intelligent Information Technology Application (IITA 2007); 2007 Dec 2–3; Zhangjiajie, China. New York: IEEE; 2007. p. 91–4.
[36] Chang H, Kim KK, Kim Y. The development of security system for sharing cad drawings in U-environment. Comput Inf 2008;27(5):731–41.
[37] Speier C, Whipple JM, Closs DJ, Voss MD. Global supply chain design considerations: mitigating product safety and security risks. J Oper Manag 2011;29(7–8):721–36.
[38] Zeng Y, Wang L, Deng X, Cao X, Khundker N. Secure collaboration in global design and supply chain environment: problem analysis and literature review. Comput Ind 2012;63(6):545–56.
[39] Wang Y, Ajoku PN, Brustoloni JC, Nnaji BO. Intellectual property protection in collaborative design through lean information modeling and sharing. J Comput Inf Sci Eng 2006;6(2):149–59.
[40] Cheng H, Li X. Partial encryption of compressed images and videos. IEEE Trans Signal Process 2000;48(8):2439–51.
[41] Nishchal NK, Naughton TJ. Flexible optical encryption with multiple users and multiple security levels. Opt Commun 2011;284(3):735–9.
[42] Huang Z, Liu G, Ren Z, Zeng L. A method of 3D data information encryption with virtual holography. In: Proceeding of Eighth International Symposium on Optical Storage and 2008 International Workshop on Information Data Storage; 2008 Nov 24–27; Wuhan, China. New York: International Society for Optics and Photonics; 2009. p. 71250E.
[43] Kim KC, Yoo SB. Collaborative design by sharing multiple-level encryption files. Concurrent Eng 2014;22(1):29–37.
[44] Chen T, Tsai HR. Ubiquitous manufacturing: current practices, challenges, and opportunities. Robot Comput Integr Manuf 2017;45:126–32.
[45] Cai X, He F, Li W, Li X, Wu Y. Multi-granularity partial encryption method of cad model. In: Proceeding of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD); 2013 Jun 27–29; Whistler, BC, Canada. New York: IEEE; 2013. p. 23–30.
[46] Cai X, Li W, He F, Li X. Customized encryption of computer aided design models for collaboration in cloud manufacturing environment. J Manuf Sci Eng 2015;137(4):040905.
[47] Cai X, Wang S, Lu X, Li W. Parametric encryption of cad models in cloud manufacturing environment. In: Proceeding of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD); 2016 May 4–6; Nanchang, China. New York: IEEE; 2016. p. 551–6.
[48] Cai X, Wang S, Lu X, Li W. An encryption approach for product assembly models. Adv Eng Inform 2017;33:374–87.
[49] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for finegrained access control of encrypted data. In: Proceeding of the 13th ACM conference on Computer and communications security; 2006 Oct; Alexandria, VA, USA. New York: Association for Computing Machinery; 2006. p. 89–98.
[50] Sun X, Zeng Y, Liu W. Formalization of design chain management using environment-based design (EBD) theory. J Intell Manuf 2013;24(3):597–612.
[51] Liu W, Zeng Y. Conceptual modeling of design chain management towards product lifecycle management. In: Chou SY, Trappey A, Pokojski J, Smith S, editors. Global perspective for competitive enterprise, economy and ecology. Berlin: Springer; 2009. p. 137–48.
[52] Zeng Y. Environment-based design (EBD): a methodology for transdisciplinary design. J Integr Des Process Sci 2015;19(1):5–24.
[53] Merkle RC, inventor; The Board of Trustees of the Leland Stanford Junior University, assignee. Method of providing digital signatures. United States patent US 4200770. 1982 Jan 5.
[54] De Caro A, Iovino V. jPBC: Java pairing based cryptography. In: Proceeding of 2011 IEEE Symposium on Computers and Communications (ISCC); 2011 Jun 28–Jul 1; Kerkyra, Greece. New York: IEEE; 2011. p. 850–5.
[55] Hou N, He F, Zhou YCY, Chen Y. An efficient GPU-based parallel tabu search algorithm for hardware/software co-design. Front Comput Sci 2020;14(5):145316.
[56] Gao Y, Gao L, Li X, Wang XV. A multilevel information fusion-based deep leaning method for vision-based defect recognition. IEEE Trans Instrum Meas 2020;69(7):3980–91.
[57] Luo J, He F, Li H, Zeng X, Liang Y. A novel whale optimization algorithm with filtering disturbance and non-linear step. Int J Bio-inspired Comput 2021;16:1–11.
[58] Li H, He F, Chen Y, Pan Y. MLFS-CCDE: multi-objective large-scale feature selection by cooperative coevolutionary differential evolution. Memet Comput 2021;13(1):1–18.
[59] Wang K, Li X, Gao L. A multi-objective discrete flower pollination algorithm for stochastic two-sided partial disassembly line balancing problem. Comput Ind Eng 2019;130:634–49.
[60] Chen Y, He F, Li H, Zhang D, Wu Y. A full migration BBO algorithm with enhanced population quality bounds for multimodal biomedical image registration. Appl Soft Comput 2020;93:106335.
[61] Song W, Lai M, Li X, Song Y, Gao L. A new spectral clustering based on particle swarm optimization for unsupervised fault diagnosis of bearings. In: Proceeding of 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE); 2019 Aug 22–26; Vancouver, BC, Canada. New York: IEEE; 2019. p. 386–91.
[62] Halima I, Laferte JM, Cormier G. Depth and thermal information fusion for head tracking using particle filter in a fall detection context. Integr Comput Aided Eng 2020;27(2):195–208.
[63] Pan Y, He F, Yu H. Learning social representations with deep autoencoder for recommender system. World Wide Web 2020;23(4):2259–79.
[64] Zhang S, He F, Ren W, Yao J. Joint learning of image detail and transmission map for single image dehazing. Vis Comput 2020;36(2):305–16.
[65] Halima I, Laferte JM, Cormier G, Fougères AJ, Dillenseger JL. Depth and thermal information fusion for head tracking using particle filter in a fall detection context. Integr Comput Aided Eng 2020;27(2):195–208.
[66] Quan Q, He F, Li H. A multi-phase blending method with incremental intensity for training detection networks. Vis Comput 2021;37(2):245–59.

[67] Zhang S, He F. DRCDN: learning deep residual convolutional dehazing networks. Vis Comput 2020;36(9):1797–808.
[68] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption. In: Proceeding of 2013 International Conference on Financial Cryptography and Data Security; 2013 Apr 1–5; Okinawa, Japan. Berlin: Springer; 2013. p. 258–74.
[69] Cui J, Zhou H, Zhong H, Xu Y. AKSER: attribute-based keyword search with efficient revocation in cloud computing. Inf Sci 2018;423:343–52.