doi:10.11959/j.issn.1000-436x.2017085

支持安全外包计算的无线体域网数据共享方案

张维纬[1,2]，张育钊[1,2]，黄焯[1,2]，张茹[3]，杨义先[3]
（1. 华侨大学工学院，福建 泉州 362021；2. 工业智能化技术与系统福建省高校工程研究中心，福建 泉州 362021；
3. 北京邮电大学信息安全中心，北京 100876）

摘 要：如何有效保护无线体域网（WBAN）中数据共享时的数据安全是一个亟待解决的关键问题。传统的CP-ABE机制具有“一对多”的数据安全通信功能，适用于WBAN中的访问控制，但运算复杂度高且不支持属性撤销。充分考虑WBAN节点资源的有限性和用户属性的动态性，提出一种在标准模型下CPA安全、支持属性撤销、加密和解密安全外包计算的CP-ABE方案。与已有的方案相比，提出的方案在保证安全性的同时，终端的运算负担大为减少，且可以实时、细粒度地撤销用户属性。

关键词：无线体域网；安全共享；外包计算；属性基加密；属性撤销
中图分类号：TP309 **文献标识码**：A

Data sharing scheme supporting secure outsourced computation in wireless body area network

ZHANG Wei-wei[1,2], ZHANG Yu-zhao[1,2], HUANG Chao[1,2], ZHANG Ru[3], YANG Yi-xian[3]
(1. College of Engineering, Huaqiao University, Quanzhou 362021, China;
2. Fujian Provincial Academic Engineering Research Centre in Industrial Intellectual Techniques and Systems, Quanzhou 362021, China;
3. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: How to effectively protect the security of data sharing in WBAN was a key problem to be solved urgently. The traditional CP-ABE mechanism had a "one to many" data security communication function which was suitable for access control in WBAN, but it had high computational complexity and did not support attribute revocation. Fully considering of limitations on computation and storage of sensor nodes and dynamic user attribute in WBAN, a CP-ABE scheme was proposed which was provably secure against CPA under the standard model and supported attributes revocation, outsourced encryption and decryption. Compared with the proposed schemes, the computation burden on senor nodes is greatly reduced and the user’s attribution can be revoked immediately and fine grained while meeting the demand of its security in the proposed scheme.

Key words: wireless body area network, security sharing, outsourced computation, attribute-based encryption, attribute revocation

1 引言

无线体域网（WBAN, wireless body area network）通过分布在人体体表或植入人体体内的无线传感器或设备采集人体的生理和行为数据，并将这些实时获取的数据进行学习和挖掘，对发病进行预警或在病发的紧急情况下采取及时的报警措施，同时，也可将发病过程中重要的生理信息保存以供后续快速的诊断治疗[1]。WBAN能广泛应用于远程医疗、老人看护等领域，具有广阔的应用前景[2]。据

收稿日期：2016-12-19；**修回日期**：2017-03-02
基金项目：华侨大学科研基金资助项目（No.13BS415）；泉州市科技计划基金资助项目（No.2014Z112）；福建省自然科学基金资助项目（No.2015J05125）；国家自然科学基金资助项目（No.61372107）
Foundation Items: Research Foundation of Huaqiao University (No.13BS415), Science and Technology Development Foundation of Quanzhou City (No.2014Z112), The Natural Science Foundation of Fujian Province (No.2015J05125), The National Natural Science Foundation of China (No.61372107)

著名的国际数据公司 IDC 发布的报告，2015 年在中国用于健康医护的可穿戴设备市场价值为 38 亿美元，预测在 2015~2020 年期间以 11.1%的速度增长，有望突破 64 亿美元。

但与传统的传感器网络不同，WBAN 收集的是更为敏感和隐私的个人健康信息。一方面，只有被授权的医生才能获取，医生根据获得的信息给出及时、准确的诊疗反馈。另一方面，在移动医疗社交网络中，个人健康信息也经常共享于同一个社交群体，患有同种疾病的病人间共享信息以提供病情交流与精神支持。然而，大数据技术发展无法避开的事实是数据安全问题[3]，WBAN 在数据共享时也面临着一系列安全与隐私的巨大挑战，尤其是在无线信道传输个人极端隐私的健康信息时，如何保证这些信息免遭非法访问是亟待解决的、具有挑战性的问题[4]。

在 WBAN 中，如果患者的个人健康信息被滥用，可能造成严重的后果[5~7]。保护 WBAN 数据共享时隐私和安全的一种方法是对传感节点采集的数据先进行加密再传输。传统的对称密码和公钥密码体制并不适用于加密传感节点众多和“一对多”通信的 WBAN 数据。一个典型的 WBAN 的应用需求如下。人体分布着一系列计算和存储资源受限的传感器收集体征数据，并将这些数据安全地传输给授权的医生或朋友圈共享。在此场景中，患者不必指定具体哪个医生、专家或朋友能共享他的健康数据，他只需要描述允许共享数据的终端用户属性[6,8]，如{外科医室 and 主任医生 or（护士 and 工龄大于 10 年）}。属性基加密（ABE，attribute-based encryption）机制[9~12]是以属性为公钥，将密文和用户私钥与属性进行关联，能够灵活地表示访问控制策略。ABE 机制中的可信属性机构为每个具有权限的用户赋予一定的属性，并根据该属性为每个用户生成对应的解密私钥。若用户想要正确解密密文时，必须拥有属性私钥而且其属性必须满足访问结构。ABE 机制“一对多”加密的高效性、抗串谋性和策略表示灵活性非常适用于 WBAN 中数据共享的细粒度访问控制[7]。

为了实现对患者长时间实时监控，一方面，WBAN 中的传感节点必须满足低能耗和低运算复杂度的要求，传感节点的加密算法的运算量不能太大。另一方面，考虑到 WBAN 终端用户可能大量使用移动终端设备接收和处理数据，而移动设备的计算和存储资源同样受限，解密也必须满足轻量级运算的要求。因此，传统的 ABE 机制一般无法直接应用于 WBAN 中。首先，ABE 机制的加密和解密算法复杂度高。在 ABE 机制中，加密算法和解密算法包含大量的指数和双线性运算，而且密文长度和加解密的计算复杂度随访问结构复杂度的增加而增加。大量复杂的运算对于计算资源受限的节点终端设备并不适用。其次，传统的 ABE 机制无法实现属性撤销。在 WBAN 中，用户的属性集通常是动态变化的，如患者指定的医院科室发生变化、医生的类别改变或属性密钥泄露等可能需要解决系统属性撤销、用户撤销或用户属性撤销等。

基于此，本文提出将 ABE 机制中加密和解密复杂运算以及属性的细粒度撤销安全外包云服务提供商运算的方案，实验结果和分析表明了本文方案的高效性和安全性。通过方案的实施，充分发挥云计算平台的计算和存储优势，降低传感节点设备的运算负担，保护用户内容共享的隐私和安全。

2 相关研究

为了在满足灵活的访问策略的同时保证数据的机密性，Sahai 等[9]首次引入了 ABE 的概念。在此基础上，Goyal 等[10]提出了密钥策略的 ABE 机制(KP-ABE)，即密钥与访问策略相关，密文与属性相关，只有密文的属性满足密钥的访问策略时才能解密密文。针对 KP-ABE 在数据共享应用中的一些不足，Bethencourt 等[11]采用树形结构表示灵活的访问策略，提出了密文策略的 ABE 机制 (CP-ABE)。在 CP-ABE 中，密文与访问策略相关，密钥与属性集合相关，只有密钥的属性满足密文的访问策略时才能解密密文。CP-ABE 更加适用于云计算的数据共享访问策略，但该方案的安全性是基于通用群组模型，如何进一步提高 CP-ABE 的安全性是其需要进一步公开解决的问题。基于此，Waters 等[12]采用线性秘密共享方案访问策略和基于具体的困难问题假设提出了更高效、更安全的 CP-ABE 方案。

安全和隐私已成为设计和大规模推广 WBAN 应用首要考虑的关键问题。针对此问题的研究大多集中在 WBAN 环境中数据的机密性、完整性、访问控制、可追踪性、可撤销性和不可否认性等方面。ABE 机制被认为非常适用于保护 WBAN 中数据的机密性和满足数据发送方按照设定的访问策略共享数据。文献[7,13]采用 KP-ABE 机制加密无线传

感网络中节点数据的加密密钥，方案中密文与访问结构分别与属性和密钥相关，只有满足访问结构并且具有属性私钥的用户才能解密数据，方案具有细粒度的访问控制功能，但数据的访问策略并不是由数据拥有者制定，在实际应用中具有一定的局限性，此外，由于 KP-ABE 的运算代价高，对无线传感网络的运算、存储和电池的续航能力提出了更高的要求。针对此问题，Picazo-sanchez 等[14]提出了采用具有固定密钥长度和轻量级运算的 CP-ABE 机制[15]以实现保护 WBAN 中数据的机密性和为数据拥有者提供数据共享的访问策略，但该方案解密运算的代价仍然很高。

由于在 WBAN 中人体传感器和用户终端计算和存储资源受限，因此，传感器和用户终端的加密和解密计算应是轻量级的。针对 ABE 机制解密计算复杂度高的问题，Green 等[16]首次提出了将 ABE 机制中解密算法外包计算的方案。该方案把 Waters 等[12]提出的 ABE 机制中的属性私钥分为 2 个部分。一部分通过安全信道传输给终端用户，并由用户安全保管；另一部分作为转换密钥交由第三方代理服务器持有。当代理服务器接收到用户的转换请求后，通过转换密钥将密文转换成用户私钥可以简单解密的密文，而在转换过程中，代理服务器无法获知关于密文所对应的明文的任何有用信息。用户收到转换的密文后，通过简单的计算就能获取明文。该方案将用户终端计算复杂度大的 ABE 解密算法外包给云服务提供商执行，能有效减轻终端设备解密计算的负担。但 ABE 机制的加密算法同样需要执行大量的模指数运算。

为此，Asim 等[17]提出了将部分加密和解密算法分别委托给 2 个代理服务器计算的方案，虽然该方案移动终端设备的解密计算只需要执行 2 次模指数运算，但加密计算仍然需要执行与用户属性个数相同的模指数运算。当用户属性个数庞大时，加密计算的代价依然很高。Zhou 等[18]首次在基于访问策略树的 ABE 机制[11]上提出了加密算法外包计算的方案。该方案在原始访问策略树的根节点上增加一个“与”门及另外一个属性，增加的这个属性相关运算在用户移动终端运行，把原始访问策略树的其他复杂加密运算交给云计算平台执行。解密算法外包计算则采用文献[16]的方案。通过加密和解密算法的外包计算，该方案可以为用户移动终端分别节省 90%和 99%的加密和解密运算量。

Zhou 等[19]提出了在移动云环境下加密和解密外包计算且支持属性撤销的 CP-ABE 方案，该方案数据拥有者首先使用公钥部分加密数据，并将部分加密的密文、访问结构和撤销列表发送给加密代理，加密代理对数据进行完全加密得到密文供移动终端下载。当移动终端请求下载共享数据时，加密代理将密文发送给解密代理对密文进行部分解密，再将部分解密的密文发送给移动终端进行完全解密。方案中，数据拥有者的部分加密和移动终端的部分解密都是轻量级的运算，而加密和解密代理执行的运算则是复杂、耗时的运算。

文献[17~19]将 ABE 机制中大部分的加密或解密运算外包给云服务提供商执行，终端设备只需要进行少量复杂度低的计算，大大减轻终端设备的运算负担，但这些方案的安全模型只是基于通用群组模型，而不是具体困难问题假设模型。通用群组模型是一种理想化的安全模型，其具有与随机预言模型一样的缺点，即存在某些方案在通用群组模型下达到可证明安全，但具体实现时却是不安全的[20,21]。而基于具体困难问题假设的标准模型的安全性形式化证明只依赖于方案所基于的单向陷门函数等特性的困难性，其具有比通用群组模型更高的安全性[12]。在数据共享方案中，加解密部分外包计算意味着数据拥有者对数据的操作失去了控制，因此，在实际应用中需要具有更高安全性的基于具体困难问题假设的标准安全模型。

受文献[17,19]的启发，本文提出了 WBAN 中将复杂的加密和解密运算分别安全外包计算的数据共享方案。借鉴文献[12]构造具体困难问题假设的方法，将文献[18]扩展的访问策略树变换成线性共享矩阵以构造更加安全的加密外包计算算法。解密外包则参考了文献[16]的方法，即将属性私钥分为 2 个部分，第一部分由终端用户安全持有，第二部分转换密钥传送给解密代理提供商。提出的方案将复杂度高的加密和解密运算安全外包计算，并能对属性进行实时、细粒度地撤销。通过方案的实施，人体传感节点只要进行轻量级的加密运算就可实现细粒度地控制数据的访问共享，终端用户的解密运算也是轻量级的。此外，方案中大量复杂度高的算法外包计算时不必假设云服务提供商完全可信。方案分析表明，与现有的方案相比，本文方案在安全性和计算效率上更具优势。

3 预备知识

3.1 双线性运算

令群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 是 2 个乘法有限循环群，它们的阶为素数 p，双线性运算 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$ 满足如下 3 个条件[22]。

1) 双线性：$\forall g,h\in\mathbb{G}_1,\forall a,b\in\mathbb{Z}_p$，均有 $e(g^a,h^b)=e(g,h)^{ab}$ 成立，其中，a、b 表示模为 p 的任意整数；

2) 非退化性：存在 $g,h\in\mathbb{G}_1$，使 $e(g^a,h^b)\neq 1_{\mathbb{G}_2}$ 成立，其中，$1_{\mathbb{G}_2}$ 表示群 $\mathbb{G}_2$ 的单位元；

3) 可计算性：存在一个有效的算法使对于 $\forall g,h\in\mathbb{G}_1$ 均可计算 $e(g,h)$。

3.2 访问结构

设 $P=\{P_1,P_2,\cdots,P_n\}$ 是由 n 个参与者组成的集合，访问结构 $\mathbb{A}$ 是 P 的一个非空子集，即 $\mathbb{A}\subseteq 2^P\setminus\{\varnothing\}$，其中，$2^P$ 表示 P 的所有子集组成的集合。若访问结构 $\mathbb{A}$ 是单调的，则 $\forall B,C$，若 $B\in\mathbb{A}$ 且 $B\subseteq C$，那么 $C\in\mathbb{A}$[23]。

3.3 访问控制策略树 *T*

令 T 表示具有访问结构的树，树的每个非叶子节点表示一个由其子节点和门限值描述的门限，如果 num_x 表示节点 x 的子节点数量，k_x 是节点 x 的阈值，则 $0<k_x\leqslant num_x$。当 $k_x=1$ 时，门限是“或”门，当 $k_x=num_x$ 时，门限是“与”门。树的每一个叶子节点 x 由属性和一个门限值 $k_x=1$ 描述[11]。

3.4 线性秘密共享方案 LSSS

一个关于参与者集合的秘密共享方案 $\prod$ 在 $\mathbb{Z}_p$ 上是线性的，则该方案满足以下 2 点[22]。

1) 所有参与者的分享额构成 $\mathbb{Z}_p$ 上的一个向量。

2) 存在一个 ℓ 行 n 列的矩阵 $\boldsymbol{M}$，称作 $\prod$ 的分享生成矩阵，对于 $i=1,2,\cdots,\ell$，函数 $\rho(i)$ 表示 $\boldsymbol{M}$ 第 i 行所标记的参与者。设列向量 $\vec{\boldsymbol{v}}=(s,y_2,\cdots,y_n)\in\mathbb{Z}_p$，其中，$s\in\mathbb{Z}_p$ 是需要共享的秘密，$y_2,\cdots,y_n\in\mathbb{Z}_p$ 是随机选取的，则向量 $\boldsymbol{Mv}$ 表示 $\prod$ 对秘密 s 的 ℓ 个分享份额，$(\boldsymbol{Mv})_i$ 是第 i 个分享份额，它属于参与者 $\rho(i)$。

根据文献[22]对 LSSS 的定义，LSSS 具有线性重构特性。即若 $\prod$ 是一个关于访问结构的线性秘密共享方案，$S\in\mathbb{A}$ 是一个授权集合，定义 $I\subseteq\{1,2,\cdots,l\}$ 为 $I=\{i:\rho(i)\in S\}$，则可以在多项式时间内找到一组常数 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，如果 $\{\lambda_i\}$ 是对秘密 s 的有效分享，则等式 $\sum_{i\in I}\omega_i\lambda_i=s$ 成立。

3.5 复杂性假设

本文方案的复杂性假设与文献[12]相同，即基于判定性 q-双线性 Diffie-Hellman 指数(q-parallel BDHE, q-parallel bilinear Diffie-Hellman exponent)假设。随机选取 $a,s,b_1,b_2,\cdots,b_q\in\mathbb{Z}_p$，在群 $\mathbb{G}$ 上定义双线性映射 e，且 g 是 $\mathbb{G}$ 的生成元。给定

$$\vec{\boldsymbol{y}}=g,g^s,g^a,\cdots,g^{(a^q)},,g^{(a^{q+2})},\cdots,g^{(a^{2q})}$$

$$\forall_{1\leqslant j\leqslant q}\quad g^{(s\cdot b_j)},g^{\left(\frac{a}{b_j}\right)},,\cdots,g^{\left(\frac{a^q}{b_j}\right)},,g^{\left(\frac{a^{q+2}}{b_j}\right)},\cdots,g^{\left(\frac{a^{2q}}{b_j}\right)}$$

$$\forall_{1\leqslant j\leqslant q,k\neq j}\quad g^{\left(\frac{a\cdot s\cdot b_k}{b_j}\right)},\cdots,g^{\left(\frac{a^q\cdot s\cdot b_k}{b_j}\right)}$$

以及在群 $\mathbb{G}_T$ 中的随机元素 Q，判定 Q 是否等于 $e(g,g)^{a^{q+1}\cdot s}$。

一个概率性多项式时间算法$\mathcal{B}$如果满足

$$|\Pr[\mathcal{A}(\vec{\boldsymbol{y}},Q=e(g,g)^{a^{q+1}s})=0]-\Pr[\mathcal{A}(\vec{\boldsymbol{y}},Q=R)=0]|\geqslant\varepsilon$$

则称算法$\mathcal{B}$能够以优势 ε 求解 $(\mathbb{G},\mathbb{G}_T)$ 中的 q-parallel BDHE 问题，若对于任意 t 时间的算法$\mathcal{B}$，均无法以优势 ε 求解群 $(\mathbb{G},\mathbb{G}_T)$ 中的 q-parallel BDHE 问题，则称群 $(\mathbb{G},\mathbb{G}_T)$ 中的 q-parallel BDHE 假设成立。

4 提出的方案

4.1 设计目标

设计的方案应满足如下目标。

1) 数据共享的安全性。人体传感节点根据访问结构将数据加密后上传到云计算平台供其他用户下载、分析和使用。属性无法满足访问控制策略的终端用户无法解密数据。

2) 细粒度的访问控制。患者可根据需要为采集的体征健康数据的使用设置细粒度的访问控制策略，而且该访问控制策略满足灵活性的要求，只有属性满足访问控制策略的用户才能共享数据。

3) 轻量级的加密和解密运算。人体传感器和用户的终端设备计算能力参差不齐。设计的方案应满足将复杂度高的运算安全外包给云计算平台执行，人体传感器和终端设备分别只负责计算复杂度低的轻量级的加密和解密运算。

4) 外包计算的安全性。在云环境下，云服务提供商是半可信的，即它会正确执行用户的请求操

作，但在这个过程中，会试图非法获取数据或与数据有关的信息。设计的方案应能满足外包给云服务提供商的计算不会泄露关于数据的任何有用信息。

5) 细粒度的属性撤销。在 WBAN 环境下，用户的属性撤销是一种常态，系统要能及时、细粒度地撤销用户的属性，即系统不仅能撤销用户的权限，也能撤销用户的某个属性。

4.2 整体方案

根据方案的设计目标，提出的方案架构如图 1 所示。首先，患者制定共享数据的控制策略，并根据控制策略部分加密采集的密文，密文以 Wi-Fi、Zigbee 或 Bluetooth 的通信方式发送到接入设备并传至云端存储。云端负责部分加密和解密工作。患者的用户可以是医院的医生、紧急救护系统或数据库。这些用户的终端负责轻量的解密运算。权威机构负责为患者和用户生成属性私钥。并通过更新加密密钥的方式实现属性的细粒度撤销。本文用到的符号定义如表 1 所示。

本文方案主要包括以下 6 个功能模块。

1) 云服务提供商

云服务提供商是提供按需的数据存储和计算服务。终端用户可随时随地通过多种不同的设备方便地访问云服务提供商以共享数据。

表 1 相关符号说明

符号	说明
BSN	体域网
ESP	加密服务提供商
DSP	解密服务提供商
AA	权威机构
CSP	云服务提供商
EU	终端用户

2) 人体传感器网络

人体传感器网络包括置于人体内或体表的大量传感器。病患者为传感节点采集的数据制定访问控制策略，传感节点采用 ABE 机制的加密算法加密数据的加密密钥。

3) 终端用户

终端用户包括医生、救护系统、报警系统或医疗大数据分析平台。终端用户通过云服务提供商获取数据。如果终端用户拥有的属性集合满足病患者定义的访问控制策略，并且拥有正确的数据解密密钥，则终端用户可以被授权使用请求的数据。

4) 加密服务提供商

加密服务提供商是云服务提供商提供的加密运算服务。为了减轻数据拥有者使用 ABE 机制加

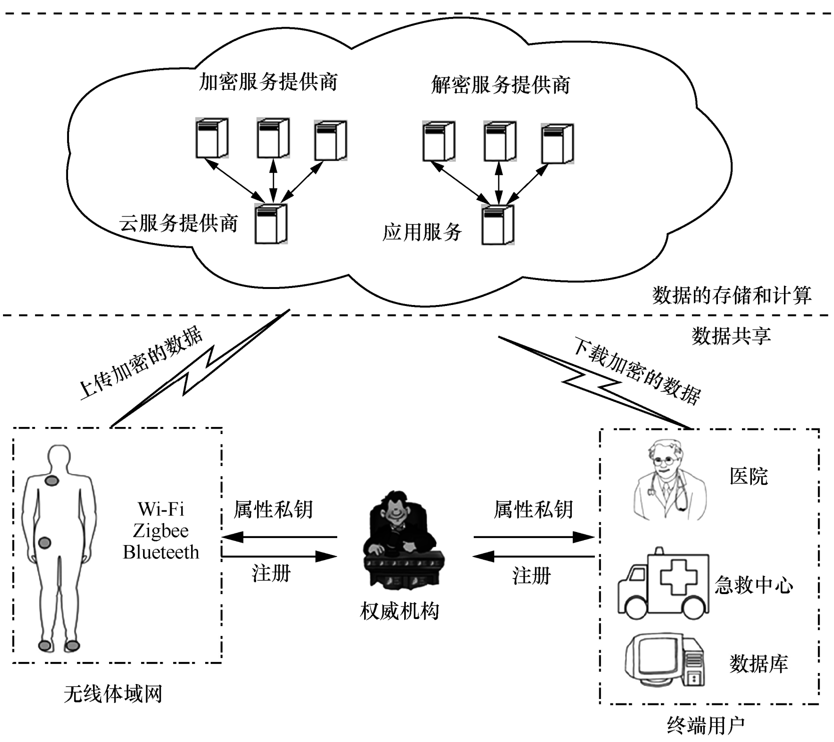


图 1 基于 WBAN 的数据安全共享方案

密数据加密密钥的计算负担，人体传感器将大量复杂度高的运算外包给加密服务提供商运算，加密服务提供商在运算过程中，无法获取关于健康数据加密密钥的任何相关信息。

5) 解密服务提供商

解密服务提供商是云服务提供商提供的解密运算服务。为了减轻终端用户使用 ABE 机制解密数据的计算负担，解密服务提供商将根据数据请求者的请求，部分解密数据加密密钥，执行了大量复杂度高的运算。同样，解密服务提供商在运算过程中，无法获取关于数据加密密钥的任何相关信息。

6) 权威机构

权威机构是系统可信的属性机构，为系统生成公钥。权威机构根据用户的属性生成其对应的属性私钥，并通过安全信道为用户颁发属性私钥。

4.3　算法描述

Bethencourt 等[11]提出的 CP-ABE 机制根据秘密共享机制将秘密信息 s 分割成多个部分，并分别嵌入到访问控制策略树每一层级的密文中。访问策略树中各个节点分享到的秘密信息的安全性是相互独立的。在解密过程中，只有拥有秘密信息 s 足够多份额的组成部分才能恢复 s 。换言之，在加密过程中即使攻击者掌握了秘密信息 s 的绝大部分信息，只要缺少其中独立的一部分，在理论上秘密信息 s 仍是安全的。据此，Zhou 等[18]提出基于扩展访问控制策略树的 CP-ABE 机制，方案在原始访问控制策略树中增加一个“与”门和一个由 BSN 进行加密计算的叶子节点，如图 2 所示。其中，T_{ESP} 表示原始的访问树，T 表示扩展的访问树，T 的根节点为“与”门，T_{BSN} 表示 BSN 的访问树。该方案将根据 T_{ESP} 生成密文的计算交给 ESP 执行，根据 T_{BSN} 生成的密文相关运算则由 BSN 完成。由于秘密信息 s 被分割成多个份额，并被分别嵌入到访问树 T_{ESP} 和 T_{BSN} 中，即使 ESP 能通过访问树 T_{ESP} 恢复出关于秘密信息 s 的部分信息，也无法得到完整的 s 。该方案通过扩展访问控制策略树，可以将 CP-ABE 机制中加密算法的大部分运算外包给 ESP 执行，大大减轻 BSN 的运算负担，但 Zhou 等[18]提出的方案是基于访问控制策略树，其整体安全级别与 Bethencourt 等[11]提出的 CP-ABE 机制是相同的。Waters 等[12]提出将访问控制策略树转换为 LSSS，该方案提高了 CP-ABE 机制的安全性。受 Zhou 等[18]提出方案的启发，本文提出基于 LSSS 的加密和解密外包计算且满足属性细粒度撤销的 CP-ABE 机制。

假设 BSN 设置的原始访问控制策略树为 T_{ESP}，根据 Zhou 等[18]的方案构建扩展的访问控制策略树 T，再使用标准的技术[23]将 T 转换为扩展的 LSSS。转换的结果如图 3 所示。其中，访问树 T 中的 ℓ 个叶子节点对应 LSSS 中的 ℓ 行，n 个非叶子节点对应 LSSS 中的 n 列，T 中的访问控制策略树 T_{BSN} 对应 LSSS 中的第一行向量 $\boldsymbol{ATT}_{\mathrm{BSN}}$，$T_{\mathrm{ESP}}$ 对应 LSSS 其他行向量 $\boldsymbol{ATT}_i(i=1,2,\cdots,\ell)$。

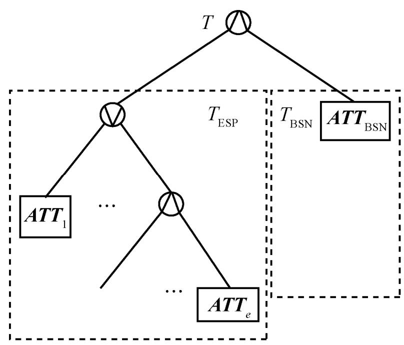


图 2　扩展的访问树

LSSS

$$\begin{array}{c} \boldsymbol{ATT}_{\mathrm{BSN}} \\ \boldsymbol{ATT}_1 \\ \\ \boldsymbol{ATT}_\ell \end{array}\left[\begin{array}{cccc} 0 & 1 & \cdots & -1 \\ 1 & -1 & \cdots & 0 \\ & & & \\ 0 & 1 & \cdots & -1 \end{array}\right]_{\ell\times n}$$

图 3　扩展的 LSSS

基于扩展的 LSSS，本文提出的 CP-ABE 机制由 8 个算法组成。

1) $Setup(1^k)\to(PK,MK)$：该算法由 AA 执行。输入安全参数 1^k，系统参数产生算法输出系统公钥 PK 和主控密钥 MK。

2) $KeyGen(MK,I_{\mathrm{key}},PK)\to(SK,TK)$：该算法由 AA 执行。输入主控密钥 MK、系统公钥 PK 和指定的 I_{key} (某个属性集合 S)，属性私钥产生算法输出属性私钥 SK 和转换解密密钥 TDK。AA 将 TDK 发送给 DSP，并将 SK 通过安全信道发送给 BSN 和 EU。

3) $EncryptBSN(PK,SK,\mathcal{M},I_{\mathrm{enc}})\to(C_{\mathrm{BSN}},TEK)$：该算法由 BSN 执行。输入系统公钥 PK，属性私钥 SK、明文数据 $\mathcal{M}$ 和指定的 I_{enc} (某个访问结构 A)，终端加密算法输出部分加密密文 C_{BSN} 和转换加密密钥 TEK。BSN 将 C_{BSN} 和 TEK 发送给 ESP。

4) $EncryptESP(PK,TEK)\to(CT,MRK)$：算法

由 ESP 执行。输入公钥 PK 和转换加密密钥 TEK，云服务加密算法输出完全加密密文 CT 和属性更新转换密钥 MRK。ESP 存储 MRK，并将 CT 发送给 DSP。

5) $DecryptDSP(PK,CT,TDK) \to (CT')$：输入系统公钥 PK、转换解密密钥 TDK 和密文 CT (对应 I_{enc})，当 $f(I_{\text{key}},I_{\text{enc}})=1$ (表示用户的属性集合满足对应的访问结构)，云服务解密算法输出被部分解密的密文 CT'。

6) $DecryptEU(PK,CT',SK) \to \mathcal{M}$：输入密文 CT'、系统公钥 PK 和属性私钥 SK，如果 $f(I_{\text{key}},I_{\text{enc}})=1$，终端解密算法输出明文数据 $\mathcal{M}$；否则输出错误符号⊥。

7) $ReTKeyGen(PK,MK,\gamma) \to (TDK',PK')$：输入主控密钥 MK、系统公钥 PK 和更新的属性集合 γ ($\gamma \subset S$)，密钥更新算法产生更新后的系统公钥 PK' 和转换密钥 TDK'。

8) $ReEnc(CT,PK',PK,MRK) \to RECT$：输入完全加密的密文 CT、系统原始公钥 PK 和更新的公钥 PK' 以及属性更新转换密钥 MRK，重加密算法输出重加密后的密文 $RECT$。

4.4　安全模型

本文假设所有的外包服务器均是半可信的，即云服务器将严格执行规定的外包存储和计算，但在此过程中会试图获得关于明文的任何有用信息。此外，本文还假设 EU 之间以及 EU、ESP 和 DSP 之间存在共谋攻击以获取明文数据。本文通过敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的游戏定义方案的安全性。在游戏中，敌手首先选择要挑战的访问结构 A^*，敌手可以不断对不满足访问结构 A^* 的属性集合 S 所对应的属性私钥进行查询。

1) 初始化阶段。挑战者 $\mathcal{C}$ 按照图 3 的方法将访问结构 A^* 变换成扩展的 LSSS 矩阵 $\boldsymbol{M}^*$，执行初始化程序 $Setup$，输出系统公钥 PK 并发送给敌手 $\mathcal{A}$。

2) 查询阶段 1。敌手 $\mathcal{A}$ 对与属性集合 $S_1,\cdots,S_{q1}$ 相对应的属性私钥 SK 和转换解密密钥 TDK 进行查询。

3) 挑战阶段。敌手 $\mathcal{A}$ 选择 2 个等长的消息 m_0 和 m_1，并指定访问结构 A^*，要求在查询阶段 1 的所有属性集合 $S_1,\cdots,S_{q1}$ 都不满足访问结构 A^*。挑战者 $\mathcal{C}$ 选择随机数 $b \in \{0,1\}$，针对 $(m_b,\boldsymbol{M}^*)$ 进行加密，并将获得的密文 CT^* 返回给敌手 $\mathcal{A}$。

4) 查询阶段 2。与查询阶段 1 相同，但要求敌手 $\mathcal{A}$ 提交的属性集合 $S_{q1},S_{q2},\cdots,S_q$ 不满足访问结构 A^*。

5) 猜测阶段。敌手 $\mathcal{A}$ 输出对 b 的猜测 b^*。

在这个游戏中敌手 $\mathcal{A}$ 的优势定义为

$$Adv_{\mathcal{A}}(1^k) = |\Pr[b=b^*] - \frac{1}{2}|$$

定义 1　一个 ABE 方案是 CPA 安全的，如果任何多项式时间敌手在上述的安全模型中的优势是可以忽略的。

4.5　CP-ABE 机制主要算法的具体构造

1) 系统参数产生算法 $Setup(\lambda,U)$

算法的输入是安全参数 λ 及系统的属性个数 U。AA 选择一个阶为素数 p、生成元为 g 的乘法有限循环群 $\mathbb{G}$，然后选择 U 个随机群元素 $h_1,\cdots,h_U \in \mathbb{G}$ 及属性版本随机参数 $V_1,\cdots,V_U \in \mathbb{G}$。再选择随机指数 $\alpha, a \in \mathbb{Z}_p$。

AA 发布的系统公钥 PK 为

$$PK = g, e(g,g)^{\alpha}, g^a, h_1^{V_1},\cdots,h_U^{V_U}$$

AA 设置的主控密钥为 $MSK = g^{\alpha}$。

2) 属性私钥的生成算法 $KeyGen(MSK,S,PK)$

算法的输入是主控密钥 MSK 和用户的属性集合 S。AA 指定扩展的属性为 $\boldsymbol{ATT}_{\text{BSN}}$，并令用户扩展的属性集合为

$$ES = S \cap \{\boldsymbol{ATT}_{\text{BSN}}\}$$

AA 选择随机数 $t,z \in \mathbb{Z}_p$。生成的转换密钥

$$TK = K = g^{\frac{\alpha}{z}} g^{\frac{at}{z}}, L = g^{\frac{t}{z}}, \{K_x\}_{x\in ES} = (h_x^{V_x})^{\frac{t}{z}}$$

AA 将 TK 发送给 DSP 进行密文的部分解密，再通过安全信道将 z 发送给终端用户 BSN 和 EU。BSN 使用 z 构建密文。EU 使用 $SK = z$ 解密密文。

3) 加密算法 $EncryptBSN(PK,SK,\mathcal{M},(\boldsymbol{M},\rho))$

BSN 选择扩展后的 LSSS 访问结构 $(\boldsymbol{M},\rho)$，其中，扩展后的 LSSS 由图 2 的扩展访问树转换得到。假设 $\boldsymbol{M}$ 是一个 $\ell+1$ 行 n 列的矩阵。其中，映射函数 ρ 能将访问结构中的每一个属性与分享生成矩阵 $\boldsymbol{M}$ 的某一行关联起来，其中，第一行与扩展的属性 $\boldsymbol{ATT}_{\text{BSN}}$ 关联。BSN 选择随机列向量 $\vec{\boldsymbol{v}} = (s,y_2,\cdots,y_n) \in \mathbb{Z}_p$，$y_2,\cdots,y_n$ 这些随机数用来分享加密秘密参数 s，计算 $\lambda_i = \boldsymbol{M}_i \vec{\boldsymbol{v}}$，其中，

$i=1,2,\cdots,\ell,\ell+1$，$\boldsymbol{M}_i$ 为矩阵 $\boldsymbol{M}$ 的第 i 行。BSN 使用 λ_1 生成部分密文，对其他的 λ_i 进行盲化处理，其中，$i=2,\cdots,\ell,\ell+1$。令盲化处理后的向量

$$\vec{\boldsymbol{\lambda}}_{\mathrm{ESP}}=(z\lambda_2,z\lambda_3,\cdots,z\lambda_\ell,z\lambda_{\ell+1})$$

BSN 选择随机数 $r_1\in\mathbb{Z}_p$，得到的部分密文

$$C=\mathcal{M}e(g,g)^{\alpha s},C'=g^s,C_1=g^{az\lambda_1}h_{\rho(1)}^{-V_1r_1},D_1=g^{r_1}$$

BSN 将加密后的部分密文 CT_{BSN} 和 $\vec{\boldsymbol{\lambda}}_{\mathrm{ESP}}$ 发送给 ESP 进行完全加密。

4) 加密算法 $EncryptESP(PK,CT_{\mathrm{BSN}},\vec{\boldsymbol{\lambda}}_{\mathrm{ESP}})$

ESP 选择随机数 $r_2,\cdots,r_\ell,r_{\ell+1}\in\mathbb{Z}_p$，然后计算

$$CT_{\mathrm{ESP}}=C_i=g^{az\lambda_i}h_{\rho(i)}^{-V_ir_i},D_i=g^{r_i},\quad i=2,\cdots,\ell,\ell+1$$

ESP 对 CT_{BSN} 和 CT_{ESP} 进行连接操作，得到

$$CT=CT_{\mathrm{BSN}}\wedge CT_{\mathrm{ESP}}$$

其中，“$\wedge$”为连接操作符号。ESP 存储 $MRK=(r_2,\cdots,r_\ell,r_{\ell+1})$，并将 CT 发送给 DSP。

5) 解密算法 $DecryptDSP(PK,CT,TK)$

假设用户扩展的属性集合 ES 满足扩展后的访问结构并定义 $I=\{i:\rho(i)\in ES\}$，其中，$I\subset\{1,2,\cdots,\ell,\ell+1\}$。根据 $LSSS$ 的线性重构特性，能够找出常数集合 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，满足 $\sum_{i\in I}\omega_i\lambda_i=s$，其中，$\{\lambda_i\}$ 是秘密 s 的一组有效分享。DSP 执行的部分解密

$$\begin{aligned}
&\frac{e(C,K)}{\prod_{i\in I}(e(C_i,L)e(D_i,K_{\rho(i)}))^{w_i}}\\
&=\frac{e(g^s,g^{\frac{\alpha}{z}}g^{at})}{\prod_{i\in I}(e(g^{az\lambda_i}h_{\rho(i)}^{-V_ir_i},g^{\frac{t}{z}})e(g^{r_i},h_{\rho(i)}^{\frac{V_it}{z}}))^{w_i}}\\
&=\frac{e(g,g)^{\frac{s\alpha}{z}}e(g,g)^{ast}}{\prod_{i\in I}(e(g^{az\lambda_i},g^{\frac{t}{z}})e(h_{\rho(i)}^{-V_ir_i},g^{\frac{t}{z}})e(g^{r_i},h_{\rho(i)}^{\frac{V_it}{z}}))^{w_i}}\\
&=\frac{e(g,g)^{\frac{s\alpha}{z}}e(g,g)^{ast}}{\prod_{i\in I}(e(g^{az\lambda_i},g^{\frac{t}{z}}))^{w_i}}=\frac{e(g,g)^{\frac{s\alpha}{z}}e(g,g)^{ast}}{\prod_{i\in I}(e(g,g)^{a\lambda_it})^{w_i}}\\
&=\frac{e(g,g)^{\frac{s\alpha}{z}}e(g,g)^{ast}}{e(g,g)^{(at)\sum_{i\in I}\lambda_i\omega_i}}=e(g,g)^{\frac{s\alpha}{z}}
\end{aligned}$$

令

$$\begin{aligned}
CT'&=(C,e(g,g)^{\frac{s\alpha}{z}})\\
&=(\mathcal{M}e(g,g)^{\alpha s},e(g,g)^{\frac{s\alpha}{z}})\\
&=(T_0,T_1)
\end{aligned}$$

DSP 将 CT' 发送给 EU 进行完全解密。

6) 解密算法 $DecryptEU(PK,CT',SK)$

EU 执行解密算法得到共享的明文 $\mathcal{M}$

$$\frac{T_0}{T_1^{sk}}=\frac{\mathcal{M}e(g,g)^{\alpha s}}{(e(g,g)^{\frac{s\alpha}{z}})^{sk}}=\frac{\mathcal{M}e(g,g)^{\alpha s}}{e(g,g)^{s\alpha}}=\mathcal{M}$$

7) 密钥更新算法 $ReTKeyGen(PK,MRK,\gamma)$

AA 重新选择 W 个属性版本随机参数 $V_1',\cdots,V_U'\in\mathbb{G}$。并公布新的系统公钥

$$PK'=g,e(g,g)^{\alpha},g^a,h_1^{V_1'},\cdots,h_U^{V_U'}$$

AA 根据用户新的属性集合 γ (包含扩展的属性 $\boldsymbol{ATT}_{\mathrm{BSN}}$)更新用户的属性转换密钥

$$TK'=K=g^{\frac{\alpha}{z}}g^{\frac{at}{z}},L=g^{\frac{t}{z}},\{K_x\}_{x\in\gamma}=(h_x^{V_x'})^{\frac{t}{z}}$$

8) 重加密算法 $ReEnc(CT,PK',PK,MRK)$

ESP 收到系统公钥更新的通知后，利用原始的公钥 PK、更新后的公钥 PK' 以及存储的主控密钥 MRK 计算重加密密钥

$$(rk_i=(h_{\rho(i)}^{V_i})^{-r_i}(h_{\rho(i)}^{V_i'})^{r_i}=h_{\rho(i)}^{-r_iV_i+r_iV_i'})_{i=2,\cdots,\ell+1}$$

对密文 C_i 进行重加密计算

$$\begin{aligned}
(C_i'&=C_irk_i=g^{az\lambda_i}(h_{\rho(i)}^{V_i})^{-r_i}h_{\rho(i)}^{-r_iV_i+r_iV_i'}\\
&=g^{az\lambda_i}(h_{\rho(i)}^{V_i'})^{-r_i})_{i=2,\cdots,\ell+1}
\end{aligned}$$

得

$$\begin{aligned}
&CT_{\mathrm{ESP}}'=C=\mathcal{M}e(g,g)^{\alpha s},C'=g^s,\\
&(C_i'=g^{az\lambda_i}(h_{\rho(i)}^{V_i'})^{-r_i},D_i=g^{r_i})_{i=2,\cdots,\ell+1}
\end{aligned}$$

4.6 属性撤销

若 AA 需要撤销用户 EU_i 的某个属性 j (假设用户的属性 j 已过期，需要撤销)，则 AA 首先更新系统公钥，得到新的公钥 PK'。但在为用户 EU_i 生成新的转换密钥 TK' 时，不升级属性 j 对应的私钥构件 K_j。即

$$\{K_x\}_{x\in\gamma,x\neq j}=(h_x^{V_x'})^{\frac{t}{z}}$$

由于 ESP 采用更新的公钥重加密密文，只有转换密钥 TK' 并同时更新才能有效解密密文。

对于未撤销属性的用户来说，由于重加密密文的结构形式与重加密前完全一样，因此，并不会影响 DSP 和 EU 的解密。

5 方案分析

5.1 安全性分析

定理 1 假设群 $(\mathbb{G},\mathbb{G}_T)$ 的 q-parallel BDHE 问

题成立，则敌手$\mathcal{A}$就无法在多项式时间内选择访问结构 A^* 下攻破支持外包加密和解密计算且可间接属性撤销的 CP-ABE 方案。该方案在标准安全模型下是选择性 CPA 安全的。

证明 如果存在一个敌手$\mathcal{A}$可以攻破本文方案，则存在一个挑战者$\mathcal{C}$可以攻破 q-parallel BDHE 问题，即输入$(\vec{y},Q)$，挑战者$\mathcal{C}$可以以不可忽略的优势决定等式$Q=e(g,g)^{a^{q+1}\cdot s}$是否成立。

敌手和挑战者按照如下游戏进行操作。

1) 初始化阶段。敌手$\mathcal{A}$选择访问结构 A^*，并发送给挑战者$\mathcal{C}$。$\mathcal{C}$按照图 3 的方法将访问结构 A^* 变换成扩展的访问结构$(\boldsymbol{M}^*,\rho^*)$，假设$\boldsymbol{M}^*$具有 ℓ^* 行 n^* 列。挑战者$\mathcal{C}$执行初始化程序 $Setup$。

挑战者选择随机数$\alpha'\in\mathbb{Z}_p$，并且通过令$e(g,g)^{\alpha}=e(g,g)^{\alpha'}e(g^{a},g^{a^{q}})$使$\alpha=\alpha'+a^{q+1}$。对于每一个属性 x，选择随机数$z_x,V_x\in\mathbb{Z}_p$。其中，$1\leqslant x\leqslant U$，U 为系统属性的总数。令 X 表示索引值 i 的集合，其中，$\rho^*(i)=x$。挑战者$\mathcal{C}$设置 h_x 为

$$h_x=g^{V_x z_x}\prod_{i\in X}g^{\frac{V_x aM^*_{i,1}}{b_i}}g^{\frac{V_x a^2M^*_{i,2}}{b_i}}\cdots g^{\frac{V_x a^{n^*}M^*_{i,n^*}}{b_i}}$$

如果 $X=\varnothing$，则令$h_x=g^{V_x z_x}$，由于 z_x 为随机数，则 h_x 也是随机数。挑战者$\mathcal{C}$将$PK=g,e(g,g)^{\alpha}$，$g^{a},h_1,\cdots,h_U$ 发送给敌手。

2) 查询阶段 1。在这个阶段，敌手$\mathcal{A}$对与属性集合 S 相对应的属性私钥 SK 和转换解密密钥 TDK 进行查询。假设属性集合不满足访问结构 A^*。挑战者$\mathcal{C}$选择随机数$r,z\in\mathbb{Z}_p$，根据线性共享矩阵的性质，存在一组向量$\vec{\boldsymbol{w}}=(w_1,w_2,\cdots,w_{n^*})\in\mathbb{Z}_p^{n^*}$，使$\boldsymbol{M}_i^*\cdot\vec{\boldsymbol{w}}=\boldsymbol{\vec{0}}$成立，其中，$w_1=-1$，并且对于所有的 i，都有$\rho^*(i)\in S$。

挑战者$\mathcal{C}$令

$$L=g^{\frac{r}{z}}\prod_{i=1,\cdots,n^*}(g^{a^{q+1-i}})^{\frac{w_i}{z}}=g^{\frac{t}{z}}$$

其中，$t=r+w_1a^{q}+w_1a^{q-1}+\cdots+w_na^{q-n^*+1}$。

挑战者$\mathcal{C}$构造 K 的表达式如下

$$K=g^{\frac{\alpha'}{z}}g^{\frac{a\cdot r}{z}}\prod_{i=2,\cdots,n^*}g^{\frac{(a^{q+2-i})w_i}{z}}$$

$$=g^{\frac{\alpha'}{z}}g^{\frac{a^{q+1}}{z}}g^{\frac{-(a^{q+1})}{z}}g^{\frac{a\cdot r}{z}}\prod_{i=2,\cdots,n^*}g^{\frac{(a^{q+2-i})w_i}{z}}$$

$$=g^{\frac{\alpha}{z}}(g^{\frac{r}{z}}\prod_{i=1,\cdots,n^*}g^{\frac{(a^{q+2-i})w_i}{z}})^{a}$$

$$=g^{\frac{\alpha}{z}}L^{a}=g^{\frac{\alpha}{z}}g^{\frac{t}{z}}$$

若属性$x\in S$，但对于任意的$i\in\{1,2,\cdots,l^*\}$，$\rho^*(i)\neq x$，挑战者$\mathcal{C}$使$K_x=L^{z_x}$。否则，由于

$$\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{\frac{a^{q+1}}{b_i}})^{\left(\frac{w_j}{z}\right)\cdot M^*_{i,j}}=1$$

挑战者$\mathcal{C}$令

$$K_x=L^{z_xV_x}\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{\frac{a^j}{b_i}\cdot\frac{r}{z}}\prod_{k=1,\cdots,n^*,k\neq j}(g^{\frac{a^{q+1+j-k}}{b_i}\cdot\frac{w_k}{z}}))^{M^*_{i,j}}$$

$$=L^{z_xV_x}\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{\frac{a^j}{b_i}\cdot\frac{r}{z}}\prod_{k=1,\cdots,n^*,k\neq j}(g^{\frac{a^{q+1+j-k}}{b_i}\cdot\frac{w_k}{z}}))^{M^*_{i,j}}\cdot$$

$$\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{\frac{a^{q+1}}{b_i}})^{\left(\frac{w_j}{z}\right)M^*_{i,j}}$$

$$=(g^{\frac{r}{z}}\prod_{i=1,\cdots,n^*}(g^{a^{q+1-i}})^{\frac{w_i}{z}})^{z_xV_x}\cdot$$

$$\prod_{i\in X}\prod_{j=1,\cdots,n^*}(g^{\frac{a^j}{b_i}\cdot\frac{r}{z}}\prod_{k=1,\cdots,n^*}(g^{\frac{a^{q+1+j-k}}{b_i}\cdot\frac{w_k}{z}}))^{M^*_{i,j}}$$

$$=(g^{z_xV_x}\prod_{i\in X}g^{\frac{V_xaM^*_{i,1}}{b_i}}g^{\frac{V_xa^2M^*_{i,2}}{b_i}}\cdots$$

$$g^{\frac{V_xa^{n^*}M^*_{i,n^*}}{b_i}})^{\frac{r+w_1a^{q}+w_1a^{q-1}+\cdots+w_na^{q-n^*+1}}{z}}$$

$$=h_x^{\frac{V_xt}{z}}$$

3) 挑战阶段。敌手$\mathcal{A}$选择 2 个等长的消息 m_0 和 m_1，并指定访问结构 A^*，要求在查询阶段 1 所有的属性集合$S_1,\cdots,S_{q1}$都不满足访问结构 A^*。挑战者$\mathcal{C}$随机选择$b\in\{0,1\}$，针对(m_b,A^*)进行加密。

挑战者$\mathcal{C}$选择随机数$y_2',y_3',\cdots,y_{n^*}'\in\mathbb{Z}_p^{n^*}$以及$r_1',r_2',\cdots,r_\ell'$，对于所有的$i\in\{1,2,\cdots,n^*\}$，定义 R_i 为集合 S 中所有$k\neq i$但$\rho^*(i)=\rho^*(k)$的元素集合。挑战者$\mathcal{C}$构造的密文 CT^* 如下

$$C=m_be(g^{s},g^{\alpha'})$$

$$C'=g^{s}$$

$$D_i=g^{-r_i'}g^{-sb_i}$$

$$C_i=h_{\rho^*(i)}^{V_i\cdot r_i'}(\prod_{j=2,\cdots,n^*}(g^{a\cdot z})^{M^*_{i,j}y_j'})(g^{b_i\cdot s\cdot z})^{-z_{\rho^*(i)}}\cdot$$

$$(\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{a^j\cdot s\cdot\frac{b_i}{b_k}})^{z\cdot M_{i,j}^*})$$

挑战者$\mathcal{C}$将获得的密文CT^*返回给敌手$\mathcal{A}$。

4) 查询阶段 2。与查询阶段 1 相同，但要求敌手$\mathcal{A}$提交的属性集合$S_{q1},S_{q2},\cdots,S_q$不满足访问结构A^*。

5) 猜测阶段。敌手$\mathcal{A}$输出对b的猜测b^*。如果$b^*=b$，挑战者$\mathcal{C}$输出 0，表示q-parallel BDHE 成立，则$Q=e(g,g)^{a^{q+1}s}$；否则，输出 1，表示$Q=e(g,g)^{\theta}$，其中，θ是一个随机数。

当$Q=e(g,g)^{a^{q+1}s}$时，攻击者获得的是有效的密文，攻击者的优势为

$$\Pr[b=b^*\,|\,Q=e(g,g)^{a^{q+1}s}]=\frac{1}{2}+\varepsilon$$

当$Q=e(g,g)^{\theta}$时，攻击者获得的密文是随机的，并不能获得关于明文的任何有用信息，攻击者的优势为

$$\Pr[b\neq b^*\,|\,Q=e(g,g)^{\theta}]=\frac{1}{2}$$

因此，$|\Pr[\mathcal{A}(\vec{y},Q=e(g,g)^{a^{q+1}s})=0]-\Pr[\mathcal{A}(\vec{y},Q=R)=0]|\geqslant\varepsilon$成立，即假设攻击者能以优势$\varepsilon$求解。

综上分析，假设q-parallel BDHE 成立，那么本文方案在标准安全模型下是选择性 CPA 安全的。证毕。

5.2　效率分析

本文提出的方案对 WBAN 系统的各个参与方都是高效和合理的。首先，BSN 每次进行加密只需要 5 次模指数运算，对于请求共享数据的 EU 来说，解密只需进行 1 次模指数运算，数据共享时的加解密只需要执行轻量级的运算。此外，由于 CSP 的优势在于存储和计算。提出的方案将大部分运算代价高的加密和解密运算交给 CSP 执行，是合理的。当发生属性撤销时，可以细粒度地撤销 EU 的某些属性，但不需要大规模更新未被撤销属性 EU 的私钥。本文方案与文献[7,12,16,18,19]的功能特征比较如表 2 所示，"N"表示无该项功能，"Y"表示具有该项功能。

从表 2 可以看出，传统的 CP-ABE 方案没有外包加密和解密计算以及属性撤销的功能，如文献[12]。文献[7]采用 CP-ABE 机制解决 WBAN 中的数据安全和隐私问题，能实现属性撤销，但没有将终端运算代价高的计算外包。文献[16]和文献[18]分别将解密和加密外包计算，但都没有属性撤销功能。文献[19]实现了复杂的加密和解密计算外包且支持属性细粒度的撤销，但安全模型仅仅是通用群组模型，而本文提出的方案安全模型基于具体的困难假设，安全性更高[12]。

本文提出的方案与文献[12,19]的计算复杂度比较如表 3 所示。假设与加密密文相关的属性个数为ℓ个，用户的属性为η个。在表 3 中，符号"—"表示没有该项运算，t_{P}表示一次双线性运算，t_{E}和t_{T}分别表示在群$\mathbb{G}_1$和群$\mathbb{G}_2$上一次模指数运算。此

表 2　本文方案与其他方案的功能特征比较

方案	外包加密	外包解密	属性撤销	安全模型
文献[7]	N	N	Y	DBDH
文献[12]	N	N	N	q-parallel BDHE
文献[16]	N	Y	N	Generic Group
文献[18]	Y	N	N	Generic Group
文献[19]	Y	Y	Y	Generic Group
本文方案	Y	Y	Y	q-parallel BDHE

表 3　本文方案与文献[12,19]计算复杂度比较

方案	本地加密	外包加密	本地解密	外包解密	安全模型
文献[12]	$(3\ell+1)t_{\mathrm{E}}+t_{\mathrm{T}}$	—	$(2\eta+1)t_{\mathrm{p}}+\eta t_{\mathrm{T}}$	—	d-parallel BDHE
文献[19]	$5t_{\mathrm{E}}+t_{\mathrm{T}}$	$(6\ell+1)t_{\mathrm{E}}$	t_{T}	$(4\eta+3)t_{\mathrm{p}}+(3\eta+4)t_{\mathrm{T}}$	Generic Group
本文方案	$4t_{\mathrm{E}}+t_{\mathrm{T}}$	$(5\ell+1)t_{\mathrm{E}}$	t_{T}	$(2\eta+1)t_{\mathrm{p}}+\eta t_{\mathrm{T}}$	d-parallel BDHE

外，假设外包加密计算也包括所有用户撤销中的转换加密。表 3 的结果表明，文献[12]终端设备的加密和解密运算复杂度随访问结构复杂度的增加而增加，文献[19]和本文方案终端设备的加密和解密运算复杂度都是一个常量，但与文献[19]相比，本文方案总的计算代价少了 $(\ell+1)t_{\mathrm{E}}+(2\eta+4)t_{\mathrm{T}}+(2\eta+2)t_{\mathrm{p}}$，而且本文方案比文献[19]安全性更高。

为了仿真本文算法与已提出算法的运算效率，选择 PBC（pairing-based cryptography）密码库作为仿真工具，仿真实验中双线性运算采用 224 bit 的 MNT 椭圆曲线双线性对。仿真平台是虚拟机上的 ubuntu 操作系统。硬件配置为 Intel I7-6700，CPU@3.40 GHz，内存 1 GB。在仿真实验中，加密的系统属性和解密的用户属性分别从 1~100 个逐一仿真，并且每次仿真的次数为 100 次，最终算法的运行时间取 100 次仿真实验的平均值。

图 4 和图 5 是本文算法与文献[12]加解密算法运行时间的比较，由于本文提出的机制将加解密算法中大量的模指数和双线性运算外包执行，终端仅需少量的运算，并且终端的加解密时间与系统属性和用户属性个数无关，在仿真平台上本文提出的加解密算法的运算时间分别为 22.77 ms 和 10.07 ms。

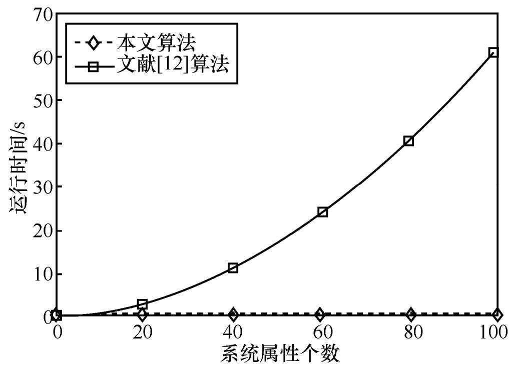


图 4　终端加密运行时间比较

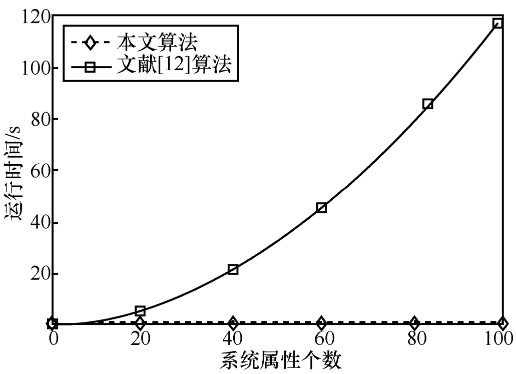


图 5　终端解密运行时间比较

图 6 和图 7 分别是本文算法与文献[19]外包计算的运行时间的比较，从图中可以看出，本文提出算法的运行时间更少，并且属性个数越多，与文献[19]相比本文算法外包计算的效率越高。

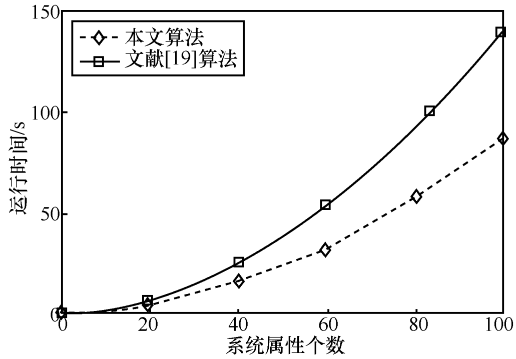


图 6　外包加密运行时间比较

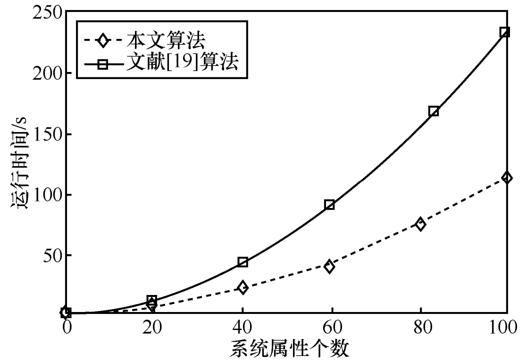


图 7　外包解密运行时间比较

6　结束语

医疗大数据具有很高的利用价值，WBAN 可产生实时、广泛的数据，具有广泛的应用前景。但 WBAN 中数据的安全和隐私性是急需解决的问题。本文提出了一种 WBAN 环境下支持隐私保护的数据共享方案。考虑到 WBAN 中人体传感器和用户终端计算与存储资源受限的因素以及用户属性的动态性，提出将加密和解密安全外包计算、支持属性细粒度撤销的 CP-ABE 机制。通过安全性和效率的分析表明，与现有的方案相比，所提方案的效率和安全性较高，更具实用性。

参考文献：

[1] HUSSEIN M, FRANCIS M B. Optimal relay selection and power control with quality-of-service provisioning in wireless body area networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(8): 5497-5510.

[2] HU F Y, WANG L, WANG S S. A human body posture recognition

algorithm based on BP neural network for wireless body area networks[J]. China Communications, 2016, 13(8): 198-208.

[3] 肖人毅. 云计算中数据隐私保护研究进展[J]. 通信学报，2014, 35(12): 168-177.
XIAO R Y. Survey of privacy preserving data queries in cloud computing[J]. Journal on Communications, 2014, 35(12):168-177.

[4] 董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展，2015, 52(10): 2341-2351.
DONG X L. Advances of privacy preservation in internet of things[J]. Journal of Computer Research and Development, 2015, 52(10): 2341-2351.

[5] LI M, LOU W, REN K. Data security and privacy in wireless body area networks[J]. IEEE Wireless Communications, 2010, 17(1):51-58.

[6] HU C Q, LI H J, HUO Y, et al. Secure and efficient data communication protocol for wireless body area networks[J]. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2(2): 94-107.

[7] TIAN Y, PENG Y B, PENG X G, et al. An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks[J]. International Journal of Distributed Sensor Networks, 2014, 10(11): 1-11.

[8] LIU X Y, ZHU Y S, GE Y, et al. A secure medical information management system for wireless body area networks[J]. KSII Transactions on Internet and Information Systems, 2016, 10(1): 221-237.

[9] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Eurocrypt 2005. Berlin: Heidelberg, 2005:457-473.

[10] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The ACM 13th Conference on Computer and Communications Security. 2006:89-98.

[11] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy. Berkeley, CA: IEEE, 2007: 321-334.

[12] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient and provably secure realization[C]//PKC 2011. Berlin: Heidelberg, 2005: 53-70.

[13] YU S, REN K, LOU W. FDAC: Toward fine-grained distributed data access control in wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(4):637-686.

[14] PICAZO-SANCHEZ P, TAPIADOR J E, PERIS-LOPEZ P, et al. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks[J]. Sensors, 2014, 14(12): 22619-22642.

[15] GUO F, MU Y, SUSILO W, et al. CP-ABE with constant-size keys for lightweight devices[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(5): 763-771.

[16] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//USENIX Security Symposium. Berkeley, CA: USENIX, 2011:523-538.

[17] ASIM M, PETKOVIC M, IGNATENKO T. Attribute-based encryption with encryption and decryption outsourcing[C]//The 12th Australian Information Security Management Conference，Perth, Western Australia, Austria: Edith Cowan University, 2014:21-28.

[18] ZHOU Z B, HUANG D J. Efficient and secure data storage operations for mobile cloud computing[C]//The 8th International Conference on Network and Service Management, Laxenburg, Austria: International Federation for Information Processing. 2012:37-45.

[19] ZHOU S G, DU R Y, CHEN J, et al. FACOR: flexible access control with outsourceable revocation in mobile clouds[J]. China Communications, 2016, 13(4): 136-150.

[20] SHOUP V. Lower bounds for discrete logarithms and related problems[C]//Eurocrypt'97. 1997: 256-266.

[21] MAURER U. Abstract models of computation in cryptography[C]// Cryptography and Coding 2005. 2005: 1-12.

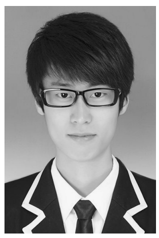
[22] BONEH D, FRANKLIN M. Identity-based encryption from the weil paring[C]//CRYPTO 2001. Berlin: Heidelberg, 2001:213-229.

[23] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Haifa: Israel Institute of Technology, 1996.

作者简介：

张维纬（1982-），男，福建泉州人，博士，华侨大学讲师、硕士生导师，主要研究方向为大数据与云计算安全、物联网安全与密码学等。

张育钊（1963-），男，福建泉州人，华侨大学副教授、硕士生导师，主要研究方向为嵌入式系统安全、物联网技术应用等。



黄焯（1993-），男，福建福州人，华侨大学硕士生，主要研究方向为数据挖掘、云计算安全等。

张茹（1976-），女，山东济南人，博士，北京邮电大学副教授、硕士生导师，主要研究方向为数字水印、数字图像取证与密码学等。

杨义先（1961-），男，四川绵阳人，博士，北京邮电大学教授、博士生导师，主要研究为网络与信息安全、密码学、编码理论等。