Attribute-based encryption for cloud computing access control: A survey

单击此处添加副标题

前言与引入

- ABE全称Attribute-Based Encryption，译为属性基加密

  允许数据的所有者根据用户的属性集合来定义访问策略，只有满足策略的用户才可以解密数据

- 分为KP-ABE （基于密钥策略属性基加密）和CP-ABE （基于密文策略属性基加密），这篇**论文主要讲了CP-ABE的分类**

文章结构

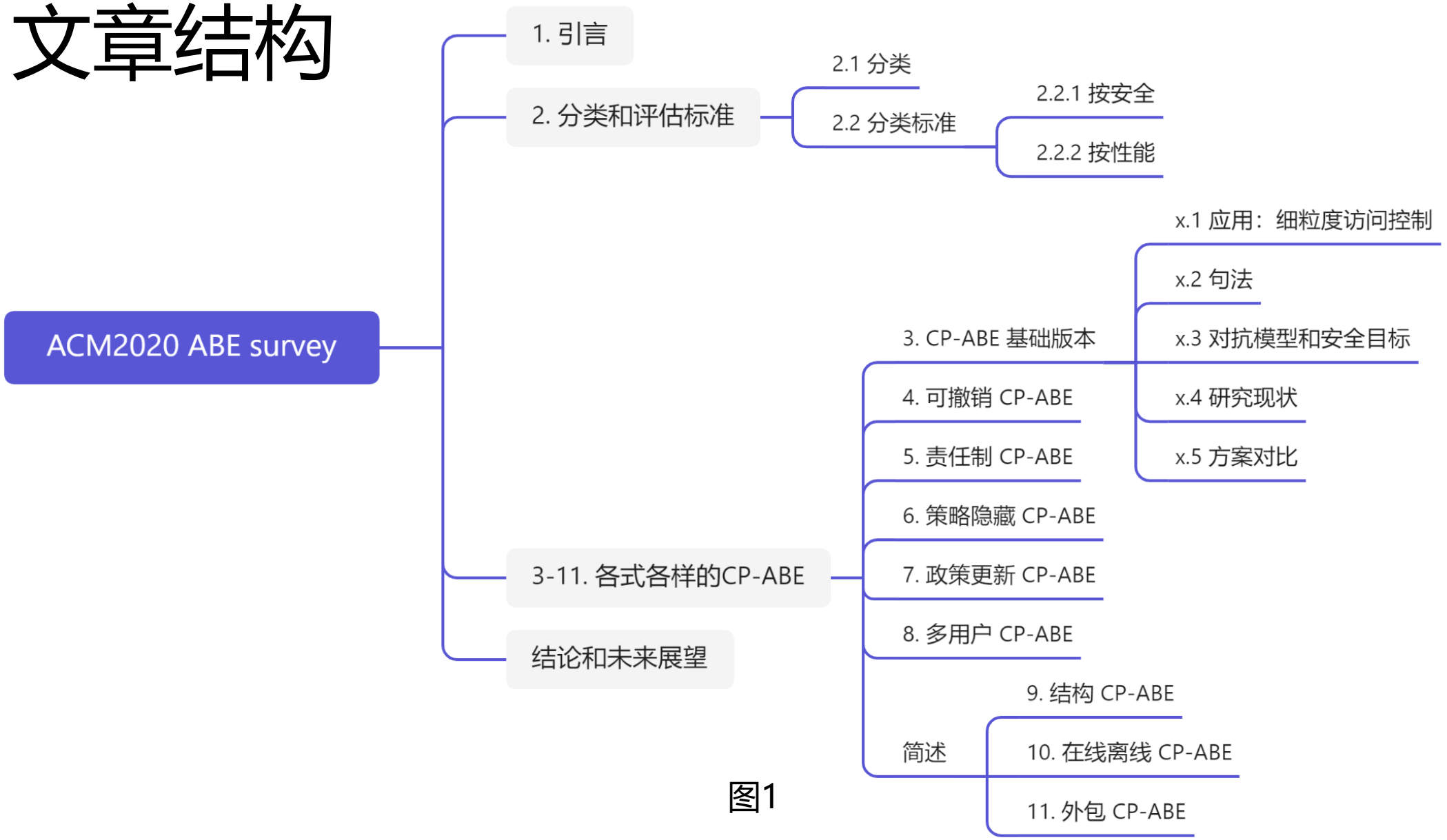
ACM2020 ABE survey
1. 引言
2. 分类和评估标准
2.1 分类
2.2 分类标准
2.2.1 按安全
2.2.2 按性能
3-11. 各式各样的CP-ABE
3. CP-ABE 基础版本
x.1 应用：细粒度访问控制
x.2 句法
x.3 对抗模型和安全目标
x.4 研究现状
x.5 方案对比
4. 可撤销 CP-ABE
5. 责任制 CP-ABE
6. 策略隐藏 CP-ABE
7. 政策更新 CP-ABE
8. 多用户 CP-ABE
9. 结构 CP-ABE
简述
10. 在线离线 CP-ABE
11. 外包 CP-ABE
结论和未来展望

图1

2.1 分类

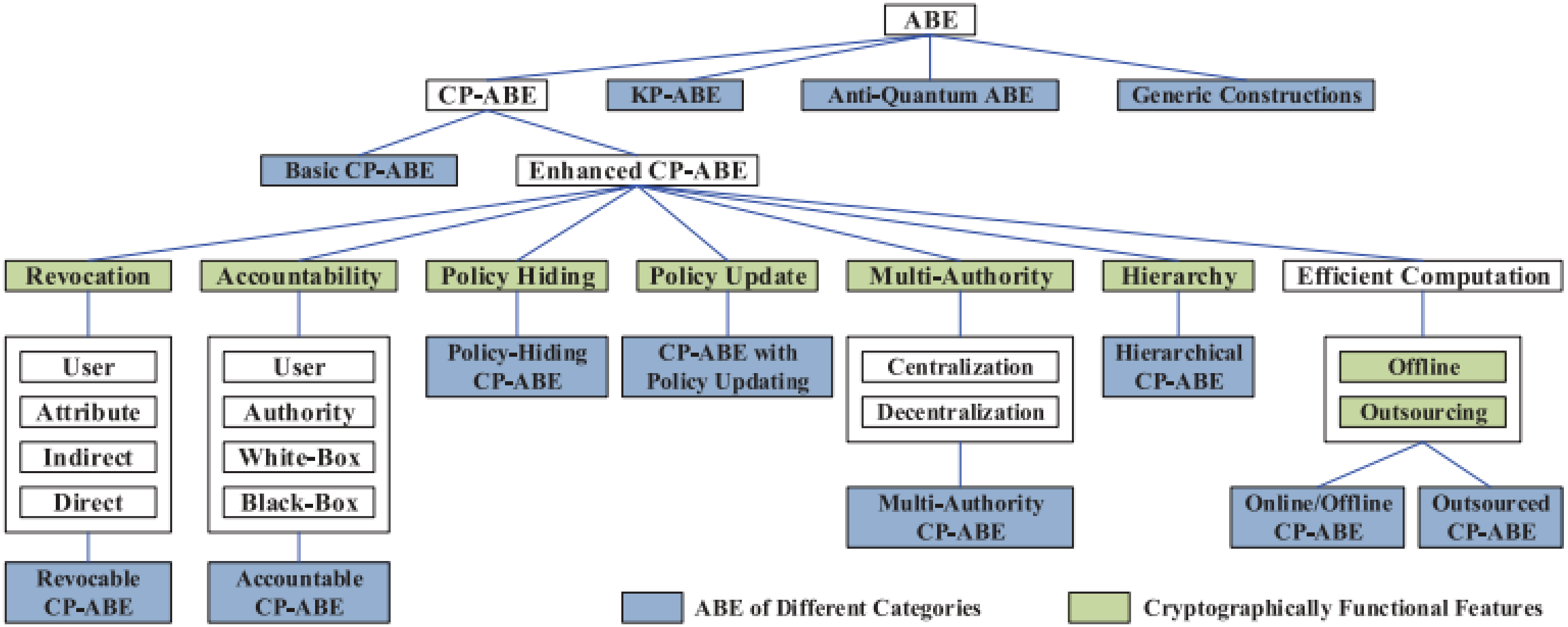
ABE
CP-ABE
KP-ABE
Anti-Quantum ABE
Generic Constructions
Basic CP-ABE
Enhanced CP-ABE
Revocation
Accountability
Policy Hiding
Policy Update
Multi-Authority
Hierarchy
Efficient Computation
User
Attribute
Indirect
Direct
User
Authority
White-Box
Black-Box
Policy-Hiding CP-ABE
CP-ABE with Policy Updating
Centralization
Decentralization
Hierarchical CP-ABE
Offline
Outsourcing
Revocable CP-ABE
Accountable CP-ABE
Multi-Authority CP-ABE
Online/Offline CP-ABE
Outsourced CP-ABE
ABE of Different Categories
Cryptographically Functional Features

图2

2.2.1 安全评估标准

- 敌手的种类
  - 选择性敌手：攻击者在攻击前选择攻击目标，攻击策略是静态的。（类似于IND-CPA）
  - 自适应敌手：攻击者根据系统反馈不断调整攻击策略，攻击是动态和自适应的。（类似于IND-CCA）
- 安全模型
  - 使用通用群和非通用群
  - 使用标准模型和随机oracle模型
- 复杂性假设
  - ABE的安全往往规约到复杂性假设，简洁形式的复杂性假设下的安全证明更困难

2.2.2 性能评估标准

- 通用标准
  - 系统密钥大小
  - 密文大小
  - 属性密钥大小
  - 计算开销
  - 群的构建（素数群比复合群更安全也更难构造)
- 表达能力（ 定义访问控制策略时的灵活性和精确度)
  - LSSS（线性秘密共享方案）：这是一种比较高效的策略。
  - 树形策略：利用树状结构来定义访问权限。
  - 阈值策略：设定一个阈值，满足一定条件的人才能访问。

3.1 基础CP-ABE 的应用

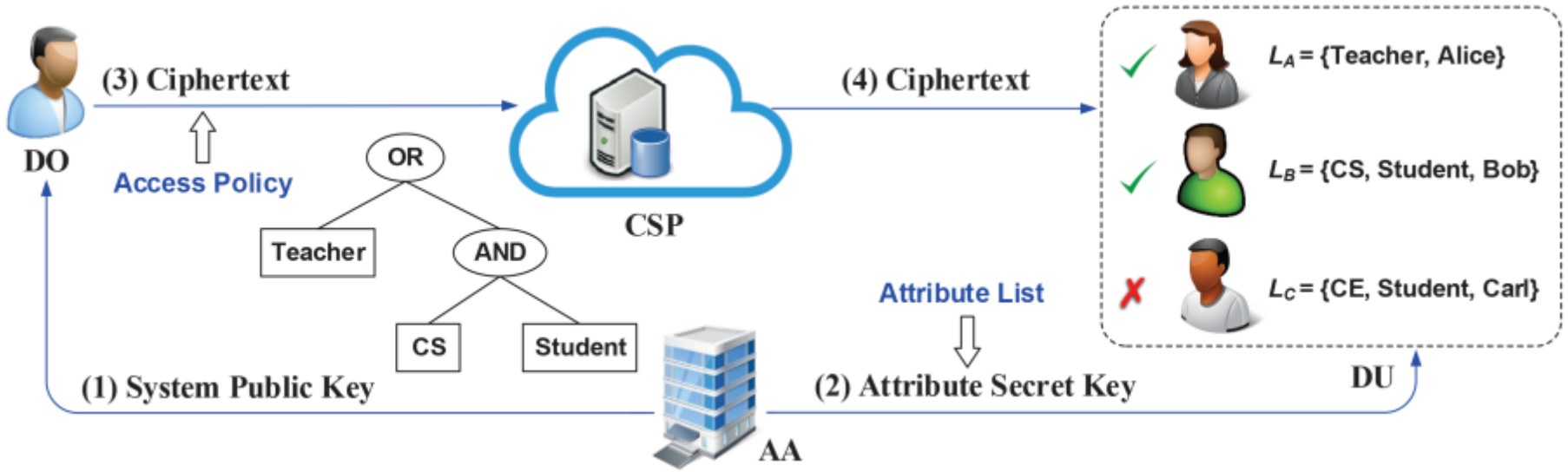

图3

CSP：The Cloud Service Provider，云服务提供者
AA：The Attribute Authority，权威属性机构
DO：The Data Owner，数据所有者，他们定义访问控制策略并加密数据。
DU：The Data User，数据用户，他们基于自己的属性密钥来解密数据，前提是他们的属性与加密时嵌入的访问控制策略匹配。

3.2 基础CP-ABE 的句法

- $setup(1^{\lambda}) \rightarrow (PK, MK)$ 由权威属性机构生成系统公钥和私钥（万能钥匙)
- $KeyGen(PK, MK, L) \rightarrow SK_L$ 由权威属性机构生成属性密钥，其中 L 为属性列表
- $Encrypt(PK, M, \mathbb{A}) \rightarrow CT_{\mathbb{A}}$ 由数据所有者生成密文，其中 $\mathbb{A}$ 是策略， M 是为待加密明文
- $Decrypt(PK, CT_{\mathbb{A}}, SK_L) \rightarrow M \ or \ \perp$ 由数据用户解密密文，如果 L 匹配 $\mathbb{A}$ 则正确解密，否则解密失败

3.3 对抗模型和安全目标

- 权威属性机构完全可信，而云服务提供者会诚实地执行系统中的程序但也可能读取密文
- 数据机密性
  - 云服务提供者无法获取明文
  - $L_A| = \mathbb{A}$ 的数据用户无法获取明文
    (| =意为不匹配)
  - $L_B = \mathbb{A}$ 的数据用户可以获取明文

$\mathbb{A}$=((通信工程 AND 教师) OR (计算机科学AND 学生))

则 L_A={通信工程, 学生, 小明} 无法访问

L_B={通信工程, 教师, 小红} 可以访问

图4

- 防串通性

  多个未授权的数据用户和云服务提供者联合，企图结合各自的属性私钥进行解密密文，他们也无法成功解密

  对于 图4 的例子，即便 L_A 和 L_B 联合起来也无法对数据进行访问

3.4 研究现状

列举了19篇，看不过来了>﹏<　　survey工作量好大

贡献者	时间	贡献	安全性
Sahai 和 Waters	2005	利用**秘密共享技术**实现了两种**模糊身份基加密**；实现了**阈值访问控制**，允许使用模糊匹配（例如，允许一些近似的身份信息）	分别依赖于DMBDH和DBDH
Bethencourt	2007	首次提出了一种 **基于树形访问策略** 的CP-ABE解决方案，采用了一种新颖的**属性私钥随机化技术**，实现 **抗串通性**	基于通用群模型，安全性较低
Cheung 和 Newport	2007	使用AND们策略，提供了选择明文攻击安全，但表达能力有限引入 **层次属性** 提升了性能。	IND-CCA安全
Goyal	2008	设计了一种基于树形结构的 CP-ABE 方案，同时解决**表达能力**和**安全性证明**问题；但**效率**低下	IND-CCA安全
Liang	2009	设计了一个新的有限CP-ABE方案，减小了计算负担但仍存在**效率**需要提高和**属性空间**小的问题	依赖于 DBDH
Lewko	2010	新的构造，涉及**复合群体**，但是导致**效率问题**	在三个新的静态假设下能够实现完全安全性

3.5 方案对比

- 计算开销最高效：Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li. 2014. Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts.
- LSSS基础方案中最高效的是：Qutaibah M. Malluhi, Abdullatif Shikfa, and Viet Cuong Trinh. 2017. A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption.
- 完全安全性方案只有
  - Shashank Agrawal and Melissa Chase. 2017. FAME: Fast attribute-based message encryption.
  - Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. 2010. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption.
  - Allison Lewko and Brent Waters. 2012. New proof methods for attribute-based encryption: Achieving full security through selective techniques.

  其中后两篇已在标准模型下证明安全
- 需要同时满足完全安全性、表达能力和解密效率，最优方案为：Shashank Agrawal and Melissa Chase. 2017. FAME: Fast attribute-based message encryption.

4.1 可撤销CP-ABE 的应用

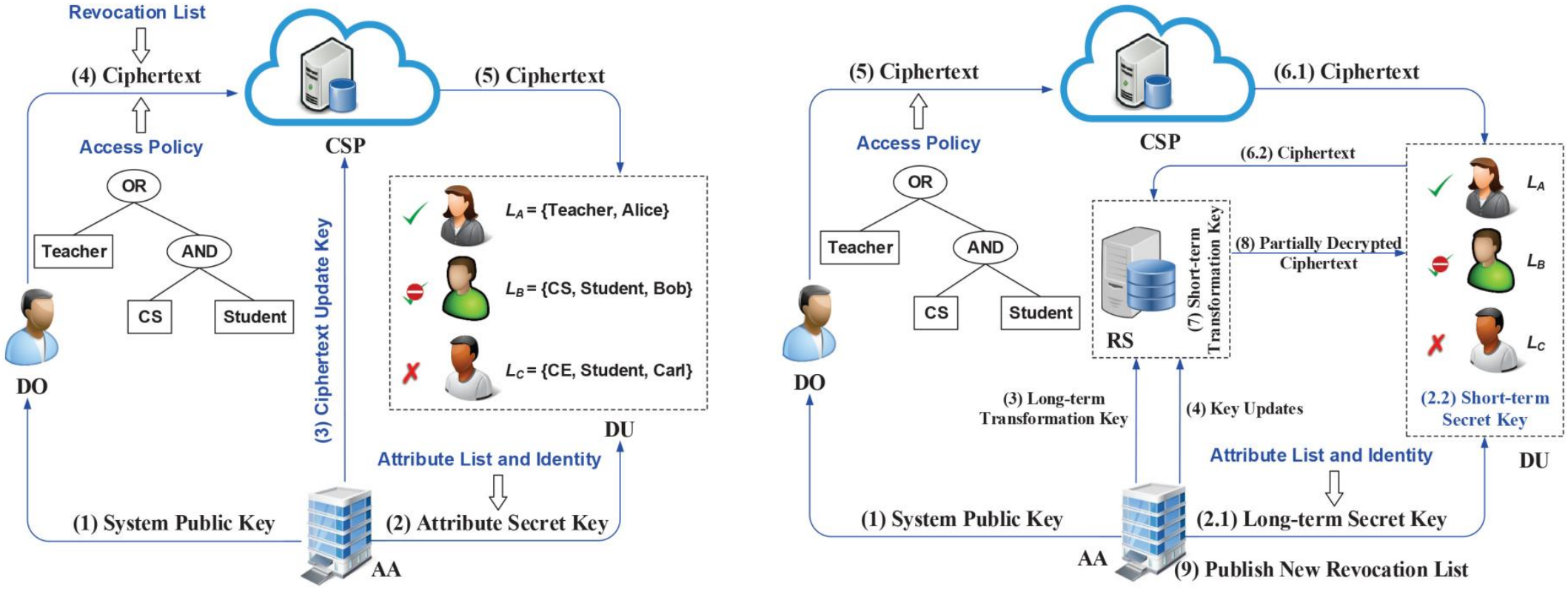

图5

RS：The Entity Revocation Server，实体撤销服务器，不可信，用于启用撤销机制

4.2 可撤销CP-ABE 的句法

- $setup()$ 和 $KeyGen()$ 与初始构造基本相同
- $Encrypt(PK, M, \mathbb{A}, \mathcal{R}) \rightarrow CT_{\mathbb{A}}$ 由数据所有者生成密文，其中 $\mathcal{R}$ 是属性撤销信息（即指定撤销的时间涉及的身份属性）
- $UKeyGen\left(PK, MK, \mathcal{R}^{(k)}\right) \rightarrow (PP^{(k)}, UK^{(k)})$
- $CTUpdate\left(PK, CT_{\mathbb{A}}, UK^{(k)}, \mathcal{R}^{(k)}\right) \rightarrow CT'_{\mathbb{A}}$
- $Decrypt(PK, PP, CT_{\mathbb{A}}, SK_L) \rightarrow M\ or\ \perp$ 由数据用户解密密文，如果 L 匹配 $\mathbb{A}$ 则正确解密，否则解密失败