**基于属性访问控制**

**基于属性访问控制模型**

ABAC（Attribute-Based Access Control）基于属性的访问控制的基础元素是相关实体的属性，包括主体属性、客体属性、上下文环境属性和动作属性等，每一类都有多个属性名和属性值构成，并共同组成访问控制请求和策略。

（S、O、E、AC），其中S（subject）代表主体、O（object）代表客体、E（environment）上下文环境、AC（action）代表动作。ABAC模型的授权由用户（主体）、资源（客体）、上下文环境和动作属性共同决定，把与访问控制相关的时间、空间、位置、隶属关系、行为、历史交互等信息作为属性综合考虑，通过全面细致的表达能力进行细粒度、复杂、动态的访问授权，增强了访问控制的有效性、灵活性和可拓展性，适用于云计算等开放性较强的分布式计算环境。

**基于属性加密机制**

ABE（Attribute-Based Encryption）基于属性加密机制属于公钥加密机制，其面向的解密对象是一个群体，而不是单个用户。实现这个特点的关键是引入了属性概念。属性是描述用户的信息要素，群体就是指具有某些属性值组合的用户集合。

ABE具有以下四个特点：

1）资源提供方仅需根据属性加密消息，无需关注群体中成员的数量和身份，降低了数据加密开销并保护了用户隐私；

2）只有符合密文属性要求的群体成员才能解密消息,从而保证数据机密性；

3）ABE机制中用户密钥与随机多项式或随机数相关，不同用户的密钥无法联合，防止了用户的串谋攻击；

4）ABE 机制支持基于属性的灵活访问控制策略，可以实现属性的与、或、非和门限操作。

ABE的高效性、抗串谋性和策略表示灵活性使得该机制可以解决传统加密机制存在的缺陷。在细粒度访问控制（审计日志、付费电视系统等）、定向广播、组密钥管理、隐私保护等领域具有良好的应用前景。

**1．基本ABE机制**

ABE访问控制系统的参与实体包括授权机构和用户。授权机构监管属性并为用户颁发属性密钥，用户分为消息发送方和接收方。系统中的每个属性用散列函数映射到中，密文和用户密钥都与属性相关。该机制支持基于属性的门限策略，即只有用户属性集与密文属性集相交的元素数量达到系统规定的门限参数时才能解密。

主要包括四种算法：Setup、KeyGen、Encrypt、Decrypt。

1. Setup：授权机构执行，输出系统公钥PK和主密钥MK。

选择y,,…,∈,系统公钥PK为e，主密钥MK为（y,,…,）。

1. KeyGen：授权机构执行，生成用户U的私钥SK。

随机选一个（d-1）次多项式p，令p(0)=y，用户私钥SK为

1. Encrypt:发送方执行，生成密文。

用属性集加密消息M∈。随机选择s∈,密文为（,EMeM，）

1. Decrypt：接收方执行，生成明文M。

若|∩|>d，则选择d个属性i∩，计算e(,)= e，再用拉格朗日插值找到= e= e，得到M=E/。

上述机制中,KeyGen算法采用Shamir门限秘密共享机制,将秘密y嵌入到SK的各个构件中,实现门限策略；SK与随机多项式p有关,使得不同用户无法结合私钥实施串谋攻击。Encrypt算法采用双线性对加密消息,并且密文构件与属性相关,从而规定了解密必须的属性；随机数s可以防止多次加密情况下用户首次解密成功即可解密后续密文的问题。在上述基本ABE机制中，PK与系统属性数目线性相关,幂运算次数和双线性对数目较多。

基本ABE机制只能表示属性的“门限”操作，且门限参数由授权机构设置，访问控制策略并不能由发送方决定。而现实中大多数系统或应用需要按照灵活的访问控制策略支持属性的与、或、门限或非操作等，实现发送方在加密时规定访问控制策略。基本的ABE机制无法满足上述情况，因而在此基础上进一步改进得到CP-ABE机制和KP-ABE机制。

**2．KP-ABE机制**

KP-ABE机制（Key Policy ABE）密钥策略基于属性加密机制是用户密钥采取树结构描述访问策略,树的叶节点集合为。密文与属性集相关,只有满足,用户才能解密密文。

KP-ABE中共享的数据与属性关联，每个用户都有一棵访问控制策略树，当共享数据的属性满足用户的访问控制策略树时，用户就可以访问共享数据。引入访问树结构并将用户的密钥表示成一棵访问树，实现属性间的逻辑与和逻辑或操作，拓展密钥策略逻辑表达能力。

KP-ABE的缺陷，加密方式依赖于KGC（密钥生成中心）是否分发正确的密钥给正确的用户，不能完全控制加密策略，一旦共享数据被重加密，系统所有的用户都需要修改私钥才能访问，开销巨大。

**3．CP-ABE机制**

CP-ABE（Ciphertext Policy ABE）密文策略基于属性加密机制是密钥采用树结构描述访问控制策略，实现由消息发送方决定的访问控制策略。用户密钥与属性集相关，只有满足，用户才能解密密文。

CP-ABE中用户的私钥与属性关联，每一个共享的数据有一棵访问控制策略树，树中每个中间节点包括一个与门或一个或门，叶子节点对应属性，只有当用户的属性集满足访问控制策略树结构时，才可以利用这些属性私钥进行计算获得解密密钥，从而访问共享的数据。

CP-ABE机制能够灵活地表示访问控制策略，从而极大地降低了数据共享细粒度访问控制引发的巨大开销，当前云计算环境下应用最为广泛。

CP-ABE的缺陷，由于用户的属性集合是简单集合，在实际应用中对于复杂环境的密文策略制定上存在不足，尤其是对于数值类型的属性，只能将一个密钥对应到一个数值或一个数值区间上。

**4．总结**

1）基本ABE机制与KP-ABE机制均采用DBDH假设，CP-ABE采用一般群组模型；

2）基本ABE机制只适用于简单的门限策略，KP-ABE和CP-ABE适用于复杂策略；

3）基本ABE受限于自身机制的不足，在云计算环境下的应用较为少见，更适用于基于门限策略的简单场景。

4）KP-ABE由接收方制定对发送方的策略，适用于查询类应用，如付费电视系统、视频点播系统、数据库访问等；

5）CP-ABE由发送方制定访问密文的策略，适合控制类应用，如社交网站、电子医疗系统等

**ABE机制的难点问题**

**1．CP-ABE机制的访问结构设计困难**

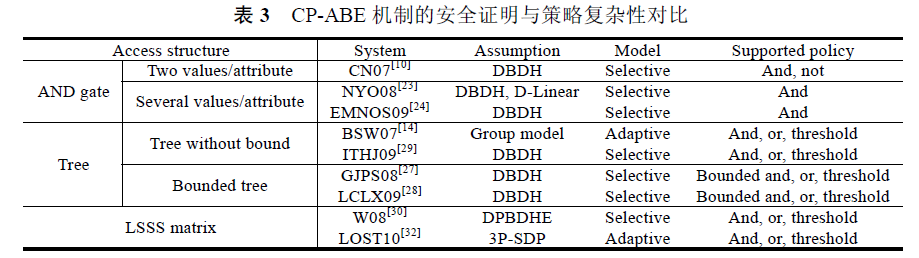
当前存在的三种主流CP-ABE结构设计方案，“与”门、访问树和LSSS矩阵。

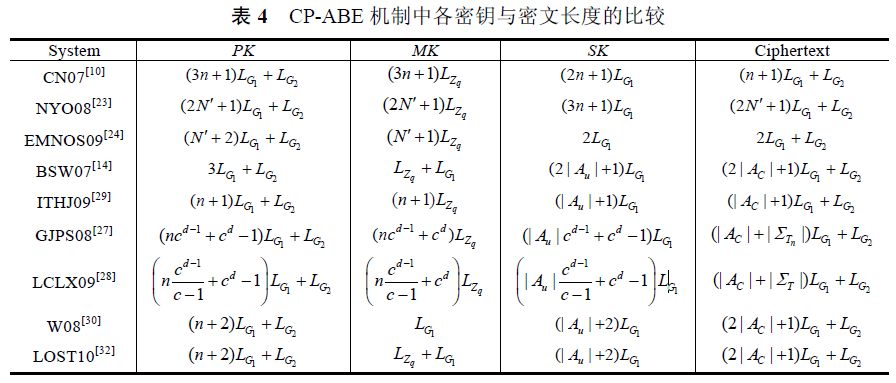
“与”门：系统属性有多个取值，访问结构采用“与”门，每项可以对应一个属性取值的子集，发送方根据各个属性的不同要求产生两部分密文构件，解密时根据用户属性集中的取值情况选择相应的密文构件解密，从而隐藏密文策略。这种机制仅支持属性的“与”操作，应用范围较小。

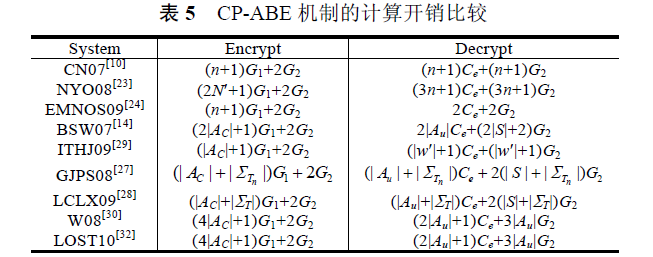
访问树：采用有界树/无界树的形式设计访问结构，由与、或节点组成的l叉树（l>1）。

LSSS矩阵：设置LSSS矩阵M(l\*n)，l表示策略属性集内属性数量，n表示属性向量的最大长度，可支持任何单调的访问公式表示策略。

三种方案的具体实现方法的对比如下：







**2．属性密钥撤销开销大**

ABE机制内，密钥往往与属性相关，而开放式环境下属性的动态性较大，因而密钥的撤销是一个难点。

ABE中的属性撤销分为为用户撤销、用户属性撤销和系统属性撤销3种情况。撤销用户时，直接作废该用户的所有权限；撤销用户属性时，需保证该用户失去该属性对应的权限,而具有该属性的其余用户仍具备此权限；撤销系统属性时，所有与该属性相关的用户都受影响，执行起来比较简单。

主要存在间接撤销、直接撤销和混合撤销三种模式。间接撤销模式下，授权机构周期性对密钥进行更新，当前未撤销的用户才能更新密钥，间接使已撤销的用户的密钥不再有效。直接撤销模式下，发送者在加密消息时规定撤销列表，直接撤销属性密钥。混合撤销模式是将上述两种模式的优点进行结合。

**3.密钥滥用**

**A**BE机制下，用户私钥只与属性相关，因而存在严重的安全隐患，且很难追究是用户还是授权机构泄露了私钥。

可追责的CP-ABE机制，用户通过可信第三方——公钥证书中心注册得到自己的证书公钥，然后向授权机构申请属性私钥，解密密钥内包含了与证书公钥对应的私钥，仅用户知道。证书的密钥机密性高于授权机构颁发的属性私钥。

可追责的匿名CP-ABE机制，将用户标识嵌入属性私钥来阻止用户之间非法共享密钥。

无滥用KP-ABE机制，采用根为“与”门的访问树，用户具有唯一标识，标识的每一位都作为属性嵌入到用户私钥中，这些属性称为标识相关属性，其余属性为普通属性。

**4.多机构下的用户授权**

针对分布式应用，可能存在多机构协作的授权机制，一方面ABE机制要求授权机制完全可信，另一方面分布式应用要求信任分散，二者存在矛盾。

多机构ABE系统包括多个属性授权机构（AA），每个AA都有一个主密钥，所有AA的主密钥之和构成整个系统的主密钥。用户向AA请求密钥，需要具备相应的属性。如果AA的主密钥相同，当用户具有足够多的属性，就可能重构系统主密钥，同时不同的多个用户也可以通过串谋恢复出系统主密钥，存在极大的安全隐患。如果AA的主密钥不同，则存在解密困难，开销巨大等问题。采用全局唯一标识符（GID）可以防止用户串谋，采用CA（Central Authority）可以保证解密的正确，当前的研究主要分为有CA的多机构ABE和无CA的多机构ABE两种。