# Efficient

1. 访问结构上的一些操作使解密只用一次配对，从而提高效率
2. 可验证外包：用承诺验证外包正确性；实现通用结构。（外包）
3. 密文大小和密钥大小之间的Tradeoff
4. 存疑。

# Generic

1. 将CPA安全的ABE转换为标准模型下CCA安全ABE的通用转换。（安全性证明）

# KP-ABE

1. 提出了一个accountable authority（负责任的授权中心）的KP-ABE方案，且可以实现黑箱跟踪。（责任追踪）
2. ABE转换成Attribute Based Encryption with Keyword Search (ABEKS)方案的通用方式。（交叉学科：关键字搜索）
3. 一个在标准模型下实现CCA2语义安全的直接KP-ABE方案，且实现了密文的有效性验证。（安全性证明）
4. 提出了一个属性带权值的KP-ABE方案（功能）
5. 提出一个密文通过广播时间间隔性的发送的KP-ABE方案。（功能）
6. 将KP-ABE应用到基于云计算的物联网应用中的一种方法。（应用）
7. 提出了一个快速加解密（避免指数运算）高效的KP-ABE（效率）

# policy or access

1. 提出了一个双策略（KP and CP）的ABE方案.
2. 提出了一个第三方撤销的CP-ABE方案。（间接撤销）
3. 构建两种转化：把ABE方案转化为其对偶判定的ABE方案；把普通ABE方案转化为双策略ABE方案。
4. 把ABE 方案应用到无限传感器网络中（应用）
5. 把LSSS技术应用到ABE访问控制策略中。
6. 驳论，纠正之前方案的缺陷（细节）。

# constant ciphertext

1. 固定密文长度的ABE加密方案。
2. 固定密文长度的ABE加密方案。
3. 固定密文长度的ABE加密方案。
4. CP-ABE固定密文方案应用于轻量级设备中。
5. 构建基于LSSS的高效KP-ABE方案。
6. 具有完全安全并且能够更快解密的具有恒定密文长度的CP-ABE方案。

# Delegation

7. 提出了具有委托性能的代理重加密ABE方案。

8. 基于可验证性代理的电路密文策略ABE加密方案。

# Traceable

9. 可追踪解密设备（黑盒追踪）的CP-ABE方案。

10. 可追踪的CP-ABE方案，方案具有全安全、抗合谋、黑盒追踪、支持LSSS的特性。

11. 可追踪（白盒）的CP-ABE方案。

12. 可追踪（白盒）的CP-ABE方案。方案具有公共审计（针对责任权威）的特性。

# CP-ABE

13.第一个CP-ABE方案。

14.可证明安全（CCA）的CP-ABE方案。

15. 支持有界多项式大小的任何访问结构（包括非单调）的CP-ABE方案。

16. 更快的加密/解密算法和缩短的密文大小的CP-ABE方案（效率）

17. 支持LSSS的高效CP-ABE方案（经典CP-ABE方案）。

18. 提出了一种没有配对运算的CP-ABE方案。

19.支持更多属性关系（< > 等）的CP-ABE方案。

20.存疑。

# Revocation

1. 建立一个有效的支持用户永久撤销的公钥加密方案（即时、混合撤销）
2. 建立一个在直接撤销模型下能实现细粒度属性撤销的KP-ABE方案（直接撤销、属性撤销）
3. 建立一个高效撤销的CP-ABE方案.(效率)
4. 1的扩展版本
5. 分层ABE下的用户撤销方案。
6. 建立一个KP-ABE变种加密体制，且具有直接撤销、代理撤销、可验证性的特性。
7. 建立一个混合撤销的ABE（HR-ABE）方案，可以选择进行直接撤销或间接撤销。
8. 建立一个支持电路访问策略的直接撤销ABE方案，且具有有限数量密文、秘钥的强制撤销功能。（功能）
9. 提出一个实用性的ABE方案，该方案综合了黑箱跟踪、直接撤销、Large Universe。

# Multi-authority

1. 第一次提出多权威ABE方案（带有中心权威）
2. 提出不含中心权威的基于门限共享策略的多权威ABE方案。
3. 提出可验证的多权威ABE方案。
4. 多权威可撤销属性方案。
5. 存疑
6. 不含中心权威的多权威加密方案，并具有:任何字符串可以被当做属性，同一个属性可以被使用多次的特性。
7. 多权威外包ABE方案。
8. 全安全，且证明不需随机预言机的多权威ABE方案。
9. 把ABE方案应用到健康数据管理中。总方案具有：白盒追踪、可撤销、多权威加密、分层等特性。

# Survey

1. 驳论，纠正之前方案的缺陷（细节）。
2. 建立ABE与可验证计算的关系，提出一种协议：包含公共代理和公共验证的特性。
3. 对比各种ABE方案的实际（如rejection rate）性能。
4. 建立一个KP-ABE方案，方案具有直接撤销、代理撤销、可验证特性。

# Secure function

1. 建立一个可追踪秘钥滥用源的KP-ABE方案（可追踪）。

# Others

1. 建立一个支持用集合表达属性的CP-ABE方案，实现了用户有限制的结合自己的属性进行解密的功能。（功能）
2. 建立一个支持任意属性状态（属性不仅只有两个状态—有或者无—）和关系动态管理的ABE方案。（功能）
3. 建立一个具有黑盒追踪、隐藏策略功能的CP-ABE方案。（追踪，隐藏策略）。
4. 建立一个多权威属性基加密方案。该方案能够限制授权机构，使其只能发送能够让接收者解密的指定加密数据。（功能）
5. 在分布式ABE方案的基础上增加一个break-glass功能：即在紧急情况下通过改变访问控制策略来访问数据。（功能，审计）
6. 建立一个full安全的ABE方案；建立一个full安全的谓词加密方案（安全性）
7. 把CP-ABE方案应用到网页服务器中。（应用）
8. 把CP-ABE方案应用到EBS系统（应用）
9. 形式化提出分层ABE的含义，构建了一个高效分层ABE.（分层）
10. ABE的一篇综述
11. 建立一种灵活的ABE,具有“loose”功能：把一个策略下的加密信息（密文）转移到另一个策略下加密。转移过程不需要原策略对应的秘钥且（区别于代理重加密）且与策略和密文本身无关。（功能，代理重加密的拓展）
12. 建立一个ABE方案能够抵御恶意KGC(解决秘钥托管问题)，同时使其公钥、密文长度和原ABE方案相当。（但引入了一个第三方dealer）（密钥托管）。
13. 把ABE和可搜索加密方案结合起来，实现可搜索加密方案的细粒度访问（交叉）
14. 利用ABE加密体制建立一套灵活、安全的个人健康记录系统。ABE方案需实现便捷的秘钥管理、灵活的访问控制、高效的密钥撤销（应用）
15. 把经典CP-ABE方案在实际移动端平台进行仿真。（应用）。