文章编号：2096-1472(2017)-03-38-04

基于属性加密的研究初探

陈继飞，相恒玉，李敬炜
（宿迁学院信息工程学院，江苏 宿迁 223800）

摘　要：针对云计算中存在的安全问题，2005年Sahai和Waters提出了属性基(ABE)加密思想。本文对当前取得的主要成果进行了较详细分析。首先，阐述了KP−ABE和CP−ABE的研究成果，其次，详述了分层属性基加密(HABE)的优点以及不足，系统分析了在云平台上针对属性撤销的所取得的成果，并且根据属性基加密机制(ABE)本身所带来的秘钥滥用问题，分析了学者们所提出的解决方法−可追责任的属性基加密机制，最后，指出了属性加密未来可能的研究方向。

关键词：基于属性加密；访问控制策略；追责；安全
中图分类号：TP309　　**文献标识码**：A

A Brief Study of Attribute-Based Encryption

CHEN Jifei,XIANG Henyu,LI Jingwei
(*Institute of Information and Engineering*,*Suqian College*,*Suqian* 223800,*China*)

Abstract: In view of the security problems in cloud computing,Sahai and Waters put forward the idea of Attribute-Based Encryption (ABE) in 2005.This paper gives a detailed summary of the main results achieved in current studies.Firstly,the paper expounds Key-Policy Attribute-Based Encryption (KP-ABE)and Ciphertext-Policy Attribute-Based Encryption (CP-ABE).Secondly,the advantages and disadvantages of Hierarchical Attribute-Based Encryption (HABE) are described in detail.Thirdly,the paper analyzes the achievements in attribute revocation on cloud platforms.According to the abuse of keys caused by ABE,the paper analyzes the accountable ABE mechanism proposed by some scholars.Finally,the paper points out the possible future research directions of ABE.

Keywords: Attribute-Based Encryption (ABE);access control policy;accountability;security

1 引言(Introduction)

近年，云计算极大减少了用户软硬件、人力资源投资，因此受到人们的广泛支持和使用。然而在给人们带来便捷的同时，不可避免的引起了很多安全问题，许多国内外的学者对此进行了研究，并取得到了很好的成果。Sahai与Waters[1]提出了属性的概念，以访问控制结构作为策略，使得加解密更加灵活。因此，安全的属性基加密机制(ABE)，受到了人们的关注。

由于传统的基于公钥基础设施(PKI)的加密机制能够很好的对用户数据的数据进行加密，然而在三个方面仍存在问题；(1)在对数据进行加密前，资源提供方必须要确保公钥证书的真实性；(2)数据加密的开销较大和所占的网络带宽多；(3)分布式很难一次就接收群体的规模与成员的身份；用户的隐私得不到很好的保护。

基于上面存在的问题，由参考文献[2]和参考文献[3]提出的基于身份加密(IBE)，很好的解决了上述第一个问题。2005年，Sahai和Waters[1]基于IBE提出了属性基(ABE)加密。属性基加密可以实现一对多的通信，以及细粒度的访问控制。目前，关于属性基加密已经取得了一些重要的成果，主要集中在以下几个方面。

第一，在对访问控制策略的研究上面。早期的ABE访问控制策略，仅仅能够支持“门限”的策略，十分的不灵活，而现实中的应用需要按照灵活的访问控制策略支持属性“与”“或”“非”“门限”等操作，因此很多学者对此进行了相关研究。第二，早期的基于身份的密码学里面只有一个单独私钥生成器(PKG)，这导致了私钥生成器的负担，而在基于分层的身份加密(HIBE)中，虽然在某种程度上面解决了单独私钥生成器(PKG)的负担问题，但是当机密数据在云共享平台上面传播时，采用的系统不仅仅需要支持细粒度的访问控制策略，而且在性能上，拓展性也需要很高的要求。第三，在ABE中，由于属性的引入，造成了密钥的撤销难度加大。第四，由于在ABE机制中，密钥滥用现象尤为严重，而导致密钥滥用现象的原因是难以归责到哪个用户和授权机构上面。

本文针对已经取得的主要成果进行了比较系统的归纳与总结，为此我们先给出一些基本的概念和术语。第2节给出本

基金项目：大学生实践创新项目；江苏省教育厅自然科学基金(14KJD520006)；宿迁学院重点科研基金项目(2016KY04)；宿迁学院教改项目(SQC2016JG11).

文需要用到的符号和术语定义，第3节详细阐述基本的ABE，KP−ABE和CP−ABE的发展，第4小节详细阐述了分层的属性基加密机制(HABE)的发展，第5小节阐述了两种属性基属性的撤销机制(间接撤销机制,直接撤销机制)的发展，本文重点介绍的是间接撤销机制，第6小节阐述的是关于ABE中的责任认定，第7小节指出属性基加密以后可以进一步研究的方向，第8小节对属性基加密的各个部分进行了总结

下面给出一些基于属性加密(ABE)常用的基本概念和定义。

2　基本术语和定义(Basic terms and definitions)

双线性对：映射$e:G_1\times G_1\to G_2$若满足下列特征就是双线性对：(1)双线性：$\forall a,b\in Z_q$，$\forall f,h\in G_1$，都有$e\left(f^a,h^b\right)=e\left(f,h\right)^{ab}$，(2)非退化性：$\exists f\in G_1$，使$e\left(f,f\right)\neq 1$，(3)可计算的：$\forall f,h\in G_1$，存在一个有效的算法计算$e\left(f,h\right)$，注意：$e\left(*,*\right)$是对称操作，$e\left(f^a,h^b\right)=e\left(f,h\right)^{ab}=e\left(f^b,h^a\right)$。

访问结构：假定$\left\{P_1,P_2,...,P_n\right\}$是参与方的集合，$P=2^{\{P_1,P_2,...,P_n\}}$，访问结构$A$是$\left\{P_1,P_2,...,P_n\right\}$的非空子集，即$A\subseteq P\setminus\left\{\varnothing\right\}$。若访问结构$A$是单调的，$\forall B,C$，若$B\in A$且$B\subseteq C$，那么$C\in A$。

当前属性基机密的研究内容主要是围绕访问控制策略，分层的属性基加密机制(HABE)，属性的撤销机制，以及可追责的属性基加密的机制等方面，本文的重点综述内容如图1所示，图1是本文对属性基加密机制(ABE)的研究内容的分类，主要描述了属性基加密(ABE)的研究进展。

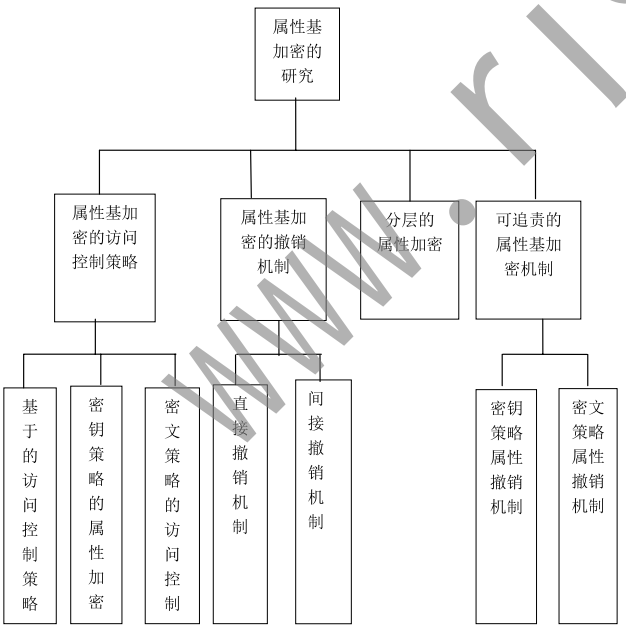

图1 当前属性基加密研究主要方向

Fig.1 The main direction of the current research on attribute based encryption

3　关于访问控制策略的研究(Research on access control policy)

自从属性基加密机制(ABE)被提出之后，该加密机制主要采用了密文或者密钥结合了访问控制策略，大大提高了加密策略的灵活性，可以作为信息共享平台下的加密方式。但是，早期的ABE访问控制较为单一，仅仅支持门限的访问控制策略，门限策略就是指的是用户属性集与密文的属性集相交的元素达到门限参数时，这时候用户就能够解密了。比如说，在一个考场里面，每个学生的属性集为{姓名，学号，准考证号，学生证号}，如果这里的门限参数是4，那么符合{姓名，学号，准考证号，学生证号}的学生就可以考试，而{姓名，学号，准考证号}的学生就不能参加考试，从上面的例子可以看出，门限的访问控制策略的灵活性还不完备，并没有很好的兼容一对多的云平台。为了解决这一问题，学者们引入了密文策略(CP−ABE)和密钥策略(KP−ABE)的机制。

KP−ABE：首先，由接收方制定策略的KP−ABE方案是由Goyal[4]在2006年首次提出，该方案虽然弥补了早期ABE在单一的访问控制策略这一方面的不足，使得它可以支持了“门限”“与”和“或”中的约束，但是该访问控制策略中不支持“非”的操作，这使的该访问控制策略在利益冲突的场景下存在很大的局限性。Ostrovsky[5]等人在2007年的广播撤销机制方案中加入了“非”的支持，很好的弥补了上面的不足，并且使得KP−ABE的访问控制策略能够支持非单调的访问结构。该访问结构不仅很好的支持了KP−ABE而且也的支持CP−ABE。Lewko和Waters[6]改进了OSW07[5]的算法，将系统中公钥的长度缩短了，但使得密文的长度增加了，解密的开销也增加了。

CP−ABE：2007年，在KP−ABE方案基础上，Bethencourt等人[7]提出第一个基于属性加密的密文策略(CP−ABE)。但是该策略只能够在通用群模型里面被证明，由于这方面的不足，Chenung和Newport[8]通过对该方案进行改进，首次提出了选择明文攻击的CP−ABE方案，该方案可以在标准模型下面被证明，Goyal等人[9]改进了之前的只能够支持很有限的访问结构的CP−ABE方案，使其安全性的证明也不仅仅局限于通用群模型，该方案在门限的基础上引进了访问树，访问树受限的大小在系统建立时被确定。

Bobba等人[10]通过提出了密文−策略属性集加密，改进了密钥中表达用户属性的灵活性。

Emura等人[11]通过改进之前的CP−ABE方案，提出了一个密文长度是恒定的CP−ABE的方案，除此以外，在计算双线性对的时间开销上面也是恒定的。但是，在这个方案中，访问策略不支持通配符。另外，在访问控制策略上面也不是很灵活。所以该解密方案不能够很好的被运用到一对多的平台上面来。Zhou和Huang等人[12]提出一个将密文的长度减小到固定值的方案，该方案被证明是选择明文攻击安全下的。

4　分层属性基加密(Hierarchical attribute based encryption)

在基于身份加密(IBE)方案下，由于私钥生成器(PKG)的负荷过重，而在像云计算这样的大型的信息共享平台中，

这种单独的私钥生成器(PKG)存在很大的局限性，因为PKG不只有计算上面的开销，还需要验证身份，建立安全的信道来传输私钥，这带来了很多不安全的因素和额外的开销。在这种情况下，私钥生成器(PKG)一旦被敌手攻破，所有用户的安全就得不到保证，为了在性能，安全上面做进一步的提高，Boneh等人[13]提出的身份基加密方案(HIBE)部分解决了PKG负担过重等难题。但是由于机密文件在云服务器上面共享的时候,使得用户对其安全性能的要求也不断的提高，为此Wang等人[14]通过将HIBE与CP−ABE相结合，在云服务器上实现了某企业的共享机密方案，但由于Wang等人[14]的方案中用到了大量的双线性对的操作，这就使得此方案的时间开销较大，Li等人[15]对其树分层的结构对其进行了改进，使得ABE的效率有了巨大的提高。Lewko和Waters等人[6]的方案改进了之前基本模式的HIBE最大分层需要最初被确定下来的不足，使得基本模式的HIBE变得更加灵活。Wang等人[16]之后另辟蹊径，他们利用分层的身份基加密方案(HIBE)与KP−ABE方案相结合，改变了传统的粗粒度的访问控制策略，使其具有了完全授权以及高性能等方面的优点。

5 具有属性撤销功能的ABE(ABE with attribute revocation function)

在基本ABE的数据共享系统中，属性的撤销机制就显得十分重要了，实际上，不同的用户可能有相同的属性，也可能有不同的属性,比如,在A学校,B班级有两个学生分别是C、D，因此，“学校A”与“班级B”是学生Alice,与学生Bob的相同的属性，如果学生Alice退出A学校，那么属性权威中心将会撤销Alice“学校A”与“班级B”这两个属性,而不会改变Bob的属性值。

针对属性的动态性增加了密钥撤销的开销和难度的问题，而在ABE中，分别有两种撤销方案：间接撤销、直接撤销。而间接撤销模式是各个学者们主要研究的方面。

直接撤销：在直接撤销机制中，通过将用户标识作为属性的一种，密文与撤销用户标识的“非”联系起来，然而这也将密文和用户私钥的大小增加了，使得加解密的开销变大了，Attrapadung等人[17]通过引入广播ABE的撤销机制，使得撤销的开销变小，他们的思路方案是结合了KP−ABE与CP−ABE的优点。

间接撤销：由于把访问控制的制定权放在了数据拥有者的手里，与KP−ABE相比，CP−ABE更加适用于云计算当中，参考文献[18]首次是给每个属性分配一个有效期，通过每隔一段时间发放属性的更新版本，然后重新颁布给所有用户最新的密钥，来对失效的属性进行撤销，此方法实现起来简单，但仍存在很多问题，在参考文献[18]的方案中，加密方不仅需要和属性撤销机构来协商属性的有效期，而且在属性更新阶段的时候，也需要和用户进行协商，这就使得属性撤销机构的工作量线性的增加。Bethencourt等人[19]提出一种CP−ABE的密钥更新策略解决了密钥存储开销较大的问题。

Ibraimi等人[20]通过引入半可信第三方作为仲裁者解决了属性的即时撤销的难题。

6 具有追责的ABE研究(Research on ABE with accountability)

在ABE加密机制中，密钥滥用问题尤为突出，较为严重的原因是难以判断盗版密钥的来源，目前，盗版密钥的来源主要是用户和授权机构。学者们针对这种密钥滥用现象提出了两种有效的策略,防止密钥滥用的CP−ABE与防止密钥滥用的KP−ABE方案。

防止密钥滥用的CP−ABE：Li等人[21]针对CP−ABE中的密钥滥用问题，提出具有可追踪性的CP−ABE的策略，这种策略很好的用来防止合谋用户之间的密钥共享。

防止密钥滥用的KP−ABE:由于在版权敏感的系统上面密钥滥用攻击过于严重，所以对于KP−ABE的研究就没有防止密钥滥用的CP−ABE那样广泛了。

7 未来研究方向(Future research directions)

在访问控制策略上面，密文的长度随属性数目的增加而线性的增长，属性数目的增加，会造成加解密计算量的开销过大，而在云计算环境中，在对细粒度的访问控制策略上，属性数目过多，密文长度过长都将严重限制属性的访问控制在实际中的应用。所以设计一个简单，高效的CP−ABE或者KP−ABE的访问控制策略就成为未来急需解决的问题了。

针对于第5小节提到的属性撤销方案，还存在着很大的不足，CP−ABE需要在可撤销的，能认定用户责任方面继续完备。并且需要在密文长度,用户私钥长度以及公钥长度都需要缩减并证明其可行性。

在属性基加密的访问控制策略上面，我们可以考虑除了“与”“或”“非”“门限”的操作，是否能够加进来“与或”“异或”等操作，来使得其访问控制策略更加灵活，加解密的效率更高。这些都值得在未来做进一步的研究，同时也要均衡密钥，密文空间等方面的因素。

随着安全事件的频出，人们对可追责的属性基加密也有了更高的要求，但是在这方面的研究还不是太多。

属性基加密(ABE)在移动云环境下的应用前景非常广阔，值得进一步研究。

8 结论(Conclusion)

本文主要描述了属性基加密(ABE)在访问控制策略，分层的属性基加密机制(HABE)，属性撤销机制，以及可追责的属性基机密的内容，由于在容错性，拓展性，以及私钥、密钥的长度和多机构协作方面的需求，导致了ABE本身的复杂性，在属性基加密(ABE)的访问控制策略上面，通过对早期仅能够支持门限的访问控制策略的改进，提出了密文—策略(CP−ABE)与密钥—策略(KP−ABE)的访问控制策略。在对密文—策略(CP−ABE)机制的研究中，总共分为三类：访问树、LSSS矩阵和“与”门。在密钥—策略(KP−ABE)中，改进了基本的ABE仅仅支持门限访问控制的策略，加入

了“与”“或”“非”的访问控制策略使其更加的成熟。而在分层的属性基加密(HABE)中由于传统的基于身份的加密(IBE)以及基于分层的身份加密(HIBE)的不足，所以分层的属性基加密(HABE)被提出，分层的属性基加密在细粒度的访问控制、性能、拓展性、完全授权上面都有巨大的提高。由于ABE机制中用户密钥或者密文与属性相关，这就导致了对过时的属性进行撤销产生了难度，于是学者们提出了两种属性撤销机制一种是直接撤销机制，另一种是间接撤销机制。而对于属性基加密机制中存在的密钥滥用问题，分别是密钥—策略属性撤销机制以及密文—策略属性基撤销机制来解决的，但是主要是通过密文—策略属性基撤销来实现的。

参考文献(References)

[1] Sahai,A.,Waters.Fuzzy Identity-Based Encryption[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques.Springer Berlin Heidelberg,2005:457-473.

[2] Shamir,A.Identity-Based Cryptosystems and Signature Schemes[C].Workshop on the Theory and Application of Cryptographic Techniques.Springer Berlin Heidelberg,1984:47-53.

[3] Boneh,D.,Franklin,M.Identity-Based Encryption from the Weil Pairing[C].Annual International Cryptology Conference. Springer Berlin Heidelberg,2001:213-229.

[4] Goyal,V.,Pandey,O.,Sahai,A.,Waters,B.Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data[C].Proceedings of the 13th ACM Conference on Computer and Communications Security.Acm, 2006:89-98.

[5] Ostrovsky,R.,Sahai,A.,Waters,B.Attribute-Based Encryption with Non-Monotonic Access Structures[C].Proceedings of the 14th ACM Conference on Computer and Communications Security.ACM,2007:195-203.

[6] Lewko,A.,Waters,B.Unbounded HIBE and Attribute-Based Encryption[C].Annual International Conference on the Theory and Applications of Cryptographic Techniques.Springer Berlin Heidelberg,2011:547-567.

[7] Bethencourt,J.,Sahai,A.,Waters,B.Ciphertext-Policy Attribute-Based Encryption[C].Security and Privacy,2007.SP'07.IEEE Symposium on.IEEE,2007:321-334.

[8] Cheung,L.,Newport,C.Provably Secure Ciphertext Policy ABE[C].Proceedings of the 14th ACM Conference on Computer and Communications Security.ACM,2007:456-465.

[9] Goyal,V.,et al.Bounded Ciphertext Policy Attribute Based Encryption[C].International Colloquium on Automata,Languages,and Programming.Springer Berlin Heidelberg,2008:579-591.

[10] Bobba,R.,Khurana,H.,Prabhakaran,M.Attribute-Sets:A Practically Motivated Enhancement to Attribute-Based Encryption[C].European Symposium on Research in Computer Security.Springer Berlin Heidelberg,2009:587-604.

[11] Emura,et al.A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext length[C].International Conference on Information Security Practice and Experience. Springer Berlin Heidelberg,2009:13-23.

[12] Zhou,Z.,Huang,D.On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption[C]. Proceedings of the 17th ACM conference on Computer and Communications Security.ACM,2010:753-755.

[13] Boneh,D.,Boyen,X.Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles[C].International Conference on the Theory and Applications of Cryptographic Techniques.Springer Berlin Heidelberg,2004:223-238.

[14] Wang,G.,Liu, Q.,Wu,J.Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services[C].Proceedings of the 17th ACM Conference on Computer and Communications Security.ACM,2010:735-737.

[15] Li, J.,et al.Enhancing Attribute-Based Encryption with Attribute Hierarchy[J].Mobile Networks and Applications, 2011,16(5):553-561.

[16] Wang,et al.Hierarchical Attribute-Based encryption and Scalable user Revocation for Sharing Data in Cloud Servers[J]. Computers & Security,2011,30(5):320-331.

[17] Attrapadung,N.,Imai,H.Conjunctive Broadcast and Attribute-Based Encryption[C].International Conference on Pairing-Based Cryptography.Springer Berlin Heidelberg,2009:248-265.

[18] Pirretti,et al.Secure Attribute-Based Systems.In:Proc.of the ACM Conf. on Computer and Communications Security. New York:ACM Press,2006:99-112.

[19] Bethencourt,J.,Sahai,A.,Waters,B.Ciphertext-Policy Attribute-Based Encryption[C].Security and Privacy,2007. SP'07. IEEE Symposium on.IEEE,2007:321-334.

[20] Ibraimi,et al.Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application[M].Information Security Applications. Springer Berlin Heidelberg,2009:309-323.

[21] Li,J.,Ren,K.,Kim,K.A2BE:Accountable Attribute-Based Encryption for Abuse Free Access Control[J].IACR Cryptology ePrint Archive,2009:118.

作者简介：

陈继飞(1994-)，男，本科生.研究领域：信息安全与密码学.

相恒玉(1995-)，男，本科生.研究邻域：信息安全与密码学

李敬炜(1996-)，女，本科生.研究领域：信息安全与密码学.