软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(6):1299−1315 [doi: 10.3724/SP.J.1001.2011.03993]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

属性基加密机制*

苏金树, 曹 丹+, 王小峰, 孙一品, 胡乔林

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Attribute-Based Encryption Schemes

SU Jin-Shu, CAO Dan+, WANG Xiao-Feng, SUN Yi-Pin, HU Qiao-Lin

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: luckycaodan@gmail.com

Su JS, Cao D, Wang XF, Sun YP, Hu QL. Attribute-Based encryption schemes. *Journal of Software*, 2011,22(6):1299−1315. http://www.jos.org.cn/1000-9825/3993.htm

Abstract: Attribute-Based encryption (ABE) scheme takes attributes as the public key and associates the ciphertext and user's secret key with attributes, so that it can support expressive access control policies. This dramatically reduces the cost of network bandwidth and sending node's operation in fine-grained access control of data sharing. Therefore, ABE has a broad prospect of application in the area of fine-grained access control. After analyzing the basic ABE system and its two variants, Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), this study elaborates the research problems relating to ABE systems, including access structure design for CP-ABE, attribute key revocation, key abuse and multi-authorities ABE with an extensive comparison of their functionality and performance. Finally, this study discusses the need-to-be solved problems and main research directions in ABE.

Key words: ABE; access control policy; revocation; key abuse; multi-authorities

摘 要: 由于属性基加密(attribute-based encryption,简称 ABE)机制以属性为公钥,将密文和用户私钥与属性关联,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带来的网络带宽和发送结点的处理开销.因此,ABE 在细粒度访问控制领域具有广阔的应用前景.在对基本 ABE 机制及其两种扩展:密钥-策略 ABE(KP-ABE)和密文-策略 ABE(CP-ABE)进行深入研究、分析后,针对 ABE 中的 CP-ABE 机制访问结构的设计、属性密钥撤销、ABE 的密钥滥用、多授权机构等难点问题进行了深入探讨和综合分析,对比了现有研究工作的功能及开销.最后讨论了 ABE 未来需进一步研究的问题和主要研究方向.

关键词: ABE;访问控制策略;密钥撤销;密钥滥用;多机构

中图法分类号: TP393 **文献标识码**: A

随着互联网和分布式计算技术的发展,在分布开放的计算环境中进行数据共享和处理的需求越来越多.资源提供方需要制定灵活可扩展的访问控制策略,从而控制数据的共享范围,也需要在与用户的通信过程中保证

* 基金项目: 国家高技术研究发展计划(863)(2009AA01A403-2); 国家重点基础研究发展计划(973)(2009CB320503)
收稿时间: 2010-08-25; 定稿时间: 2011-01-31
CNKI 网络优先出版: 2011-03-07 17:14, http://www.cnki.net/kcms/detail/11.2560.TP.20110307.1714.000.html

数据的机密性.大规模分布式应用也迫切需要支持一对多的通信模式,从而降低为每个用户加密数据带来的巨大开销.传统的基于公钥基础设施(public key infrastructure,简称 PKI)的加密机制能够保护数据机密性,但是存在 3 个重大缺陷:一是资源提供方必须获取用户的真实公钥证书,否则无法加密;二是资源提供方需要用接收群体中每个用户的公钥加密消息,并将密文分别发送给相应的用户,导致处理开销大和占用带宽多的问题;三是广播加密[1−3]技术虽然部分解决了效率问题,却要求资源提供方在加密前获取用户列表,这会产生另外两个次生问题:分布式难以一次获取接收群体的规模与成员身份;分布式应用列举用户身份会损害用户隐私.

为了解决第 1 个重大缺陷,Shamir[4]和 Boneh 等人[5]提出并实现了基于双线性对技术的身份基加密(identity-based encryption,简称 IBE)机制,直接使用用户的身份作为公钥,使得资源提供方无需在线查询用户的公钥证书.Sahai 和 Waters[6]在 IBE 技术的基础上提出属性基加密(attribute-based encryption,简称 ABE)机制,实现基于属性的加解密,能够进一步解决第 2 个和第 3 个重大缺陷.ABE 机制具有以下 4 个特点:一是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;二是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;三是 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;四是 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 机制的高效性、抗串谋性和策略表示灵活性使得它在细粒度访问控制[7−9](审计日志、付费电视系统等)、定向广播[7]、组密钥管理[10,11]、隐私保护[8,12,13]等领域具有良好的应用前景.

最初提出的基本 ABE 机制[6]仅能支持门限访问控制策略.为了表示更灵活的访问控制策略,学者们进一步提出密钥-策略 ABE(KP-ABE)[7]和密文-策略 ABE(CP-ABE)[14]两类 ABE 机制.ABE 机制的复杂性导致其本身仍存在一些需要解决的重要问题:(1) CP-ABE 机制中的策略由消息发送方制定,使得系统公钥设计的复杂性与策略复杂性相关,限制了访问结构的设计;(2) ABE 机制中用户密钥与属性相关,属性的动态性增加了密钥撤销的开销和难度;(3) ABE 机制中用户私钥由授权机构产生,且用户私钥与用户的隐私信息(如 ID)无关,造成了授权机构和用户都可能泄露用户私钥,无法分清密钥泄露的责任;(4) 多机构 ABE 能够分担授权机构的责任,也满足分布式应用的多机构协作的需求,对 ABE 的设计也提出了挑战.针对以上提到的 4 个问题,ABE 机制已成为近年来学者们研究的热点,并在密码和安全协议领域的期刊和学术会议上发布了不少好的研究成果.

本文对当前研究成果进行归纳分析和总结,第 1 节给出本文符号和术语定义,详细阐述基本 ABE,KP-ABE 和 CP-ABE,并指出 ABE 中的难点问题.针对这些难点问题,第 2 节分析比较 CP-ABE 访问结构设计的与门、树和线性秘密共享机制(linear secret sharing scheme,简称 LSSS)矩阵技术.第 3 节阐述 ABE 的 3 种属性撤销机制,即间接撤销、直接撤销以及混合撤销模式的主要算法.第 4 节对比分析防止密钥滥用的 CP-ABE 和 KP-ABE 技术.第 5 节分别介绍多机构 ABE 中采用与不采用中央授权机构的系统结构.最后进行总结,并指出 ABE 的未来可能研究方向.

1 ABE 机制

ABE 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,例如:校园网中的学生具有院系、学生类别、年级、专业等属性;教师具有院系、职称、教龄等属性.群体就是指具有某些属性值组合的用户集合.例如,计算机学院本科生就是指院系属性值为计算机学院、学生类别属性值为本科生的一个群体.

ABE 使用群体的属性组合作为群体的公钥,所有用户向群体发送数据使用相同公钥.上例中,{计算机学院,本科生}作为向计算机学院本科生发送密文的公钥.而私钥由属性授权机构根据用户属性计算并分配给个体.

1.1 术语定义

本文用到的符号见表 1.ABE 机制通过访问结构表示策略,以双线性对为技术基础,并基于各种数学难题和假设构建安全性.下面分别给出本文基本概念的形式化定义.

定义 1(访问结构[15]). 假定$\{P_1,P_2,\ldots,P_n\}$是参与方的集合, $P=2^{\{P_1,P_2,\ldots,P_n\}}$.访问结构$\mathbb{A}$是$\{P_1,P_2,\ldots,P_n\}$的非空子集,即$\mathbb{A}\subseteq P\backslash\{\varnothing\}$.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 $C\in\mathbb{A}$.

定义 2(双线性对[5]). 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$e(f^a,h^b)=e(f,h)^{ab}$,称映射 $e:G_1\times G_1\to G_2$ 是双线性的;(2) 非退化性:$\exists f\in G_1$,使 $e(f,f)\neq 1$;(3) 可计算的:$\forall f,h\in G_1$,存在一个有效的算法计算 $e(f,h)$.注意:$e(*,*)$是对称操作,即 $e(f^a,h^b)=e(f,h)^{ab}=e(f^b,h^a)$.

定义 3(计算 Diffie-Hellman(CDH)问题[16]). 随机选择 $a,b\in Z_q^*$,给定三元组(g,g^a,g^b),计算 g^{ab}.

定义 4(判定双线性 Diffie-Hellman(DBDH)问题[16]). 随机选择 $a,b,c\in Z_q^*,R\in G_2$,给定元组(g,g^a,g^b,g^c,R),判断等式 $e(g,g)^{abc}=R$ 是否成立.

定义 5(判定线性(D-Linear)问题[17]). 随机选择阶为 q 的群 G 的生成元 g,f,v,随机选择指数 $a,b\in Z_q,R\in G$,给定元组(g,f,v,g^a,f^b,R),判断等式 $v^{a+b}=R$ 是否成立.

定义 6(选择密文攻击(IND-CCA)游戏[16]). 敌手和受挑战者进行如下交互:(1) 受挑战者对加密方案进行系统建立,输出公私钥对,并将公钥交给敌手;(2) 敌手可以向受挑战者进行一些解密询问,受挑战者解密密文,返回结果给敌手;(3) 敌手选择两个明文M_0,M_1,然后发送给受挑战者.受挑战者投掷一个公平硬币 $b\in\{0,1\}$,对明文 M_b 加密,得到密文 C^*并发送给敌手;(4) 敌手可以继续向受挑战者进行一些同步骤(2)中的解密询问,但询问密文不能为 C^*;(5) 最后,受挑战者必须回答 0 或者 1(记为 b'),作为对密文 C^*的猜测.

若 $b'=b$,则敌手在该游戏中获胜.敌手在游戏中的优势定义为 $\Pr[b'=b]-1/2$.

若在上面的交互中,敌手不能进行任何解密询问,则此游戏称为选择明文攻击(IND-CPA)游戏.对于一个加密方案,如果任意概率多项式时间(PPT)的敌手在上述游戏中的优势是可忽略的,则称该加密方案是 IND-CCA 安全,简称 CCA 安全.对应选择明文攻击游戏,称为 IND-CPA 安全,简称 CPA 安全.CPA 安全是公钥加密机制的最基本要求,CCA 安全是公钥加密机制更强的安全性要求.目前所提出的 ABE 方案基本上都是 CPA 安全,但很多达不到 CCA 安全.

Table 1 Notations

表 1 符号说明

Notation	Definition	Notation	Definition
G_i	Group or operation in *group*(*exponentiation*,*multiplication*) (i=1,2), g is a random generator of G_1	Z_q	*Group*$\{0,\ldots,q-1\}$ under multiplication modulo q. q is a prime
C_e	e operation, e denotes bilinear pairing	n	Number of attributes in system
N'	$N'=\sum_{i=1}^{n}n_i$ is the total number of possible value of attributes, where attribute i has n_i possible values	A_C	Attributes with ciphertext C
AA_k	The kth authority, $k\in\{1,\ldots,N\}$, N denotes the number of authorities	A_k	Attributes managed by AA_k
S	Least interior nodes satisfying an access structure(include the root)	A_u	Attributes of user u
L_*	Bit-Length of element in *	$\|*\|$	Number of elements in *

1.2 ABE基本机制

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.Sahai 和 Waters[6]提出基本 ABE(fuzzy IBE),系统中的每个属性用散列函数映射到 Z_q^* 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.例如,图书馆中某论文的属性集为{计算机,安全,英文,博士},且该论文的属性加密门限参数为 2,则属性集为{计算机,路由,博士}的用户可以访问该论文,而属性集为{机械,博士}的用户无法访问该论文.

基本 ABE 机制包括 4 种算法:Setup,Extract,Encrypt,Decrypt.系统初始化时根据安全参数运行 BDH 参数生成器[5],产生两个阶为素数 q 的群 G_1,G_2,以及双线性对 $e:G_1\times G_1\to G_2$.d 为门限参数.

(1) Setup(d):授权机构执行,选择 $y,t_1,\ldots,t_n\in Z_q$,系统公钥 PK 为 $(T_1=g^{t_1},\ldots,T_n=g^{t_n},Y=e(g,g)^y)$.主密钥 MK

为$(y,t_1,\ldots,t_n)$.

(2) KeyGen:授权机构执行,生成用户 u 的私钥.随机选择一个$(d-1)$次多项式 p,令 $p(0)=y$,用户私钥 SK 为

$$\{D_i=g^{p(i)/t_i}\}_{\forall i\in A_u}.$$

(3) Encrypt:发送方执行,用属性集 A_C 加密消息 $M\in G_2$.随机选择 $s\in Z_q$,密文为

$$(A_C,E=Y^sM=e(g,g)^{ys}M,\{E_i=g^{t_is}\}_{\forall i\in A_C}).$$

(4) Decrypt:接收方执行.若$|A_u\cap A_C|>d$,则选择 d 个属性 $i\in A_u\cap A_C$,计算 $e(E_i,D_i)=e(g,g)^{p(i)s}$,再用拉格朗日插值找到 $Y^s=e(g,g)^{p(0)s}=e(g,g)^{ys}$,得到 $M=E/Y^s$.

上述机制中,KeyGen 算法采用 Shamir 门限秘密共享机制[18],将秘密 y 嵌入到 SK 的各个构件 D_i 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 E_i 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.Pirretti 等人[19]和 Baeky 等人[20]提出了性能更优的算法.

基本 ABE 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.而许多现实应用需要按照灵活的访问控制策略支持属性的与、或、门限和非操作,实现发送方在加密时规定访问控制策略.由于基本 ABE 无法支持灵活的访问控制策略,Goyal 等人[7]提出由接收方制定访问策略的 KP-ABE 机制,支持属性的与、或、门限操作.Bethencourt 等人[14]提出由发送方规定密文的访问策略的 CP-ABE 机制.图 1 和图 2 分别说明了 KP-ABE 和 CP-ABE 的工作流程.

KP-ABE 机制[7]如图 1 所示,用户密钥采取树结构描述访问策略 $A_{u\text{-}KP}$,树的叶节点集合为 A_u.密文与属性集 A_C 相关,只有 A_C 满足 $A_{u\text{-}KP}$,用户才能解密密文.KP-ABE 与基本 ABE 机制的区别在于 KeyGen 和 Decrypt 算法.KeyGen 算法仍采用秘密共享机制,采取自顶向下的方式为树中每个节点 x 定义一个次数比节点的门限值小 1 的随机多项式 p_x,令 $p_x(0)=p_{parent(x)}(index(x))$,其中,$parent(x)$表示 x 的父节点,$index(x)$表示 x 的父节点给 x 的编号.而根节点 r 的 $p_r(0)=y$,使得主密钥 y 分散到对应于叶节点的私钥构件 D_i 中.Decrypt 算法对访问策略树自底向上采用递归过程解密每个节点,得到恢复明文所需的秘密值.图 1 中,A_C 满足策略 $A_{u1\text{-}KP}$,解密需计算的树中内部节点集合 S 为{AND}.

由于共享机制不支持属性的“非”操作,Ostrovsky 等人[21]采用 Naor 和 Pinkas[22]的广播撤销机制实现表示“非”的 KP-ABE 机制,策略表示更加灵活.但是该机制的密文和用户密钥大小,加解密开销都翻倍.Lewko 和 Waters[17]改进 OSW07[21]的算法,缩短系统公钥长度,但增加了密文长度.

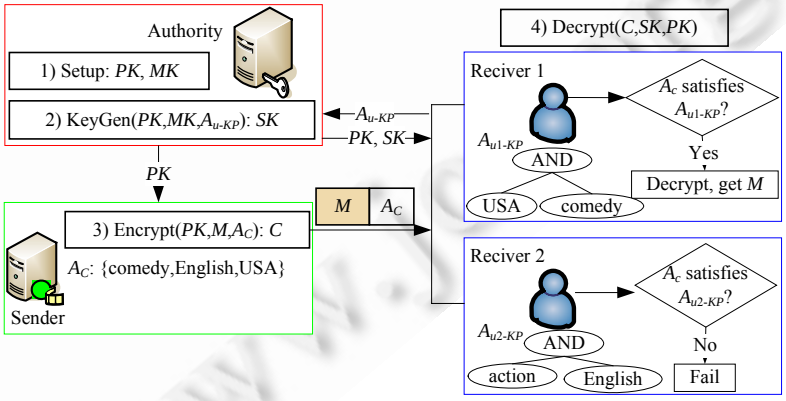

Fig.1 KP-ABE illustration

图 1 KP-ABE 机制示意图

CP-ABE 机制[14]如图 2 所示,密文采取树结构描述访问策略 $A_{C\text{-}CP}$,实现由消息发送方决定的访问控制策略.

CP-ABE 中,用户密钥与属性集 A_u 相关,只有 A_u 满足 $A_{C\text{-}CP}$,用户才能解密密文.CP-ABE 与基本 ABE 的算法不同,且 *PK* 和 *MK* 的长度与系统属性数目无关.CP-ABE 的 KeyGen 算法采用两级随机掩码方式防止用户串谋,用户私钥构件与第 2 级随机数相关.Encrypt 算法中,访问树的实现方式与 KP-ABE[7]的 KeyGen 算法相似,区别是 $p_r(0)=s$,并且叶节点对应密文构件 E_i.Decrypt 算法与 KP-ABE[7]类似,但双线性对操作数目翻倍.图 2 中,A_{u1} 满足 $A_{C\text{-}CP}$,解密需计算的树中内部节点集合 *S* 为{OR,2-of-3,AND}.Ostrovsky 等人[21]也可以实现表示"非"的 CP-ABE 机制.

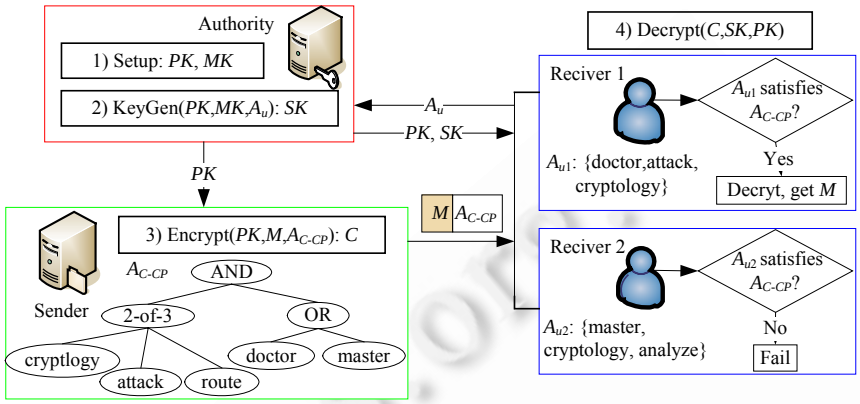

Fig.2 CP-ABE illustration

图 2 CP-ABE 机制示意图

上述 3 种 ABE 算法在复杂性假设、策略灵活性和适用范围方面有着明显的差别.基本 ABE[6]和 KP-ABE[7]均采取 DBDH 假设,而 CP-ABE[14]采取一般群模型.基本 ABE 仅表示门限策略,适用于对策略要求简单的应用.KP-ABE 和 CP-ABE 机制支持复杂策略,适用于细粒度数据共享的应用.KP-ABE 机制中,用户规定对接收消息的要求,适用于查询类的应用,如付费电视系统、视频点播系统、数据库访问等;而 CP-ABE 机制中,发送方规定访问密文的策略,适合访问控制类应用,如社交网站的访问、电子医疗系统等.3 种基本机制的比较见表 2.

Table 2 Comparision of basic ABE, KP-ABE and CP-ABE

表 2 基本 ABE,KP-ABE 和 CP-ABE 的比较

System	Ciphertext	User's secret key	Encrypt	Decrypt	Policy
Basic ABE[6]	$\|A_C\|L_{G_1}+L_{G_2}$	$\|A_u\|L_{G_1}$	$\|A_C\|G_1+2G_2$	dC_e+2dG_2	Threshold
KP-ABE[7]	$\|A_C\|L_{G_1}+L_{G_2}$	$\|A_u\|L_{G_1}$	$\|A_C\|G_1+2G_2$	$\|A_C\|C_e+2\|S\|G_2$	And, or, threshold
CP-ABE[14]	$(2\|A_C\|+1)L_{G_1}+L_{G_2}$	$(2\|A_u\|+1)L_{G_1}$	$(2\|A_C\|+1)G_1+2G_2$	$2\|A_u\|C_e+(2\|S\|+2)G_2$	And, or, threshold

1.3 ABE难点问题与研究内容

算法的正确性和安全性、密钥管理、可扩展性是安全协议研究的核心问题.ABE 机制采用访问结构表示访问策略,而策略的灵活性会导致访问结构的复杂.当前的 KP-ABE 实现了复杂的访问结构,支持灵活的访问策略,并基于 DBDH 假设达到 CPA 安全.而 CP-ABE 中策略的灵活性使得系统公钥设计复杂,限制了访问结构的设计.ABE 系统中,属性的动态性增加了密钥撤销的复杂性;且属性密钥与用户标识无关,导致无法预防和追踪非法用户持有合法用户的私钥(盗版密钥).而大规模的分布式应用需要 ABE 机制支持多机构协作,以满足可扩展性、容错性的需求.这些因素给 ABE 的研究带来了挑战,主要包括以下几个方面:

(1) CP-ABE 机制访问结构设计难.KP-ABE 的系统公钥以及与复杂访问结构相对应的用户私钥都由授权机构生成,密文的解密只由授权机构控制.而 CP-ABE 的系统公钥由授权机构产生,访问结构由加密者设计,密文的解密由授权机构与加密者共同控制.因此在 CP-ABE 中,访问结构的复杂度增加了系统公钥设计的复杂性,从

而增加了采用标准的复杂性假设证明机制安全性的难度,使访问结构的设计受限;

(2) 属性密钥撤销开销大.ABE 中,用户密钥与属性相关,而系统的动态变化经常引起属性失效或从属关系变更,因而 ABE 属性密钥的撤销成为研究重点.ABE 的属性密钥撤销分为 3 种情况:整个用户的撤销、用户的部分属性撤销和系统属性的撤销.撤销用户需作废该用户的密钥,而不影响未撤销的用户;撤销用户的某个属性,不能影响具备该属性其他用户的权限;系统属性撤销影响具有该属性的所有用户.ABE 中,属性与用户的多对多关系增加了支持上述 3 种撤销需求的属性密钥撤销机制的设计难度;

(3) ABE 的密钥滥用.ABE 中,用户私钥只与用户属性相关,而与用户的任何特定信息无关,无法防止盗版密钥的产生.除了用户会泄露自己的私钥外,掌握所有用户私钥的授权机构也可能透露合法用户的私钥.故在出现盗版密钥时,无法确定是用户还是授权机构泄露了私钥,责任追究困难.盗版密钥难预防和难界定责任,使 ABE 机制中的密钥滥用问题尤为突出,难以解决;

(4) 多机构下的用户授权.基本 ABE 属于单授权机构情形,不能满足大规模分布式应用对不同机构协作的需求;授权机构必须完全可信,违背了分布式应用要求信任分散的安全需求;授权机构管理系统中所有属性,为用户颁发密钥,工作量大,成为系统的性能瓶颈.多授权机构 ABE 不仅能够满足分布式应用的需求,而且可将单授权机构的信任和工作量分散到系统的所有授权机构上,故研究多机构情况下的 ABE 是必要的.但是,每个授权机构独立颁发密钥和用户密钥准确性的需求,给多机构 ABE 的研究带来了挑战.

当前,ABE 的研究工作分为 ABE 机制、ABE 的撤销机制、ABE 的可追责性以及多授权机构 ABE 机制,重点研究内容如图 3 所示.根据图 3 中研究内容的分类,下面主要分析 ABE 的研究进展.

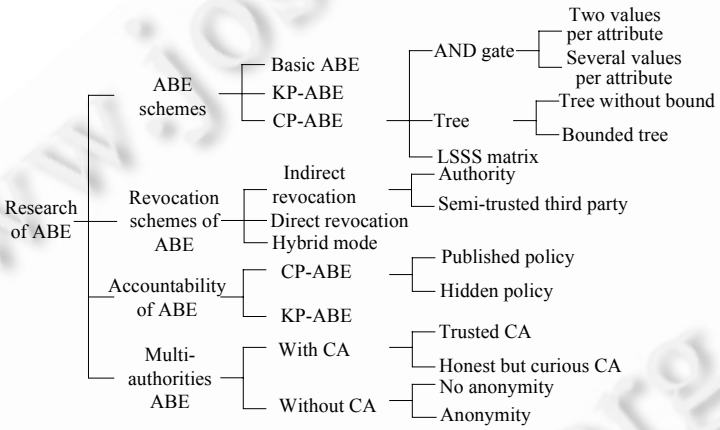

Fig.3 Research of ABE

图 3 ABE 研究内容

2 CP-ABE 的访问结构设计

CP-ABE 机制中,加密者控制访问策略,策略越复杂,系统公钥设计得也越复杂,机制的安全性证明越困难.为达到标准复杂性假设下的 CPA 安全,CP-ABE 的主要研究工作都集中于表示访问策略的访问结构的设计.根据采取的访问结构不同,CP-ABE 的研究工作分为“与”门、访问树和 LSSS 矩阵 3 类.

2.1 “与”门访问结构

Cheung 和 Newport[10]采用“与”门表示访问策略,首次在 DBDH 假设下证明 CP-ABE 机制的安全性.之后,Nishide 等人[23]和 Emura 等人[24]在 CN07[10]的基础上分别实现了策略的隐藏和效率的提高.

CN07[10]最先基于 DBDH 假设构建 CPA 安全的 CP-ABE 机制,并采用 CHK[25]技术扩展到 CCA 安全.引入文字 $\underline{i}$ 表示属性 i 与其非$\neg i$,访问结构为文字上的与门,不出现在与门中的系统属性用无关紧要表示.Setup 算法中,随机选择 $y,t_1,\ldots,t_{3n}\in Z_q$ 作为主密钥,系统公钥中的 T_k 由 3 部分组成,分别对应属性在与门中为正、非

和无关紧要的情况.KeyGen 算法为每个系统属性 i 选择一个随机数 r_i,令 $r=\sum_{i=1}^{n} r_i, \tilde{D}=g^{y-r}$;并根据 i 与用户属性集 A_u 的关系生成密钥构件 $D_i=g^{r_i/t_i}(i\in A_u)$ 或 $D_i=g^{r_i/t_{n+i}}(i\notin A_u)$;然后计算 $F_i=g^{r_i/t_{2n+i}}$,组成用户私钥 $SK=(\tilde{D},\{D_i,F_i\}_{i\in\{1,\ldots,n\}})$.Encrypt 算法选择随机数 s 加密消息,并根据系统属性 i 与密文属性集 A_C 的关系生成密文构件 $E_i=T_i^s$ ($i\in A_C$ 且 $\underline{i}=i$)或 $E_i=T_{n+i}^s$ ($i\in A_C$ 且 $\underline{i}=\neg i$),而 $i\notin A_C$ 时,$E_i=T_{2n+i}^s$.Decrypt 算法根据 A_C 中每个属性与 A_u 的关系选择私钥构件进行解密运算.但访问结构仅实现了属性的"与"和"非"操作,并且 PK 和密文的大小以及加/解密时间都与系统属性数目线性相关,效率低.

基于 DBDH 和 D-Linear 假设,Nishide 等人[23]提出抗串谋的、策略隐藏的 CP-ABE 机制.系统属性有多个候选值.访问结构采用"与"门,每项可以是对应属性候选值集合的一个子集.发送方根据访问结构中各项对系统属性取值的不同要求产生两部分密文构件,Decrypt 算法根据用户属性集中各项的值选择相应的密文构件解密,从而隐藏密文策略.采取 BW07[26]技术使接收方获取解密成功与否的消息,但增加了密文和用户密钥长度以及解密开销.Emura 等人[24]基于 DBDH 假设,采用与 NYO08[23]相同的访问结构,首次提出密文长度不变的 CP-ABE 机制,提高了算法效率.上述两种算法仅支持属性的与操作.

2.2 树访问结构

提出 CP-ABE 机制的 BSW07[14]采用树结构表示灵活的访问控制策略,但其安全性证明仅基于一般的群假设.为了在 DBDH 假设下实现策略灵活的 CP-ABE 机制,Goyal 等人[27]和 Liang 等人[28]采用有界树结构.Ibraimi 等人[29]采用一般的访问树结构,消除了界限条件的约束.

Goyal 等人[27]基于 DBDH 假设提出有界的密文-策略属性基加密(BCP-ABE),提供一种将 KP-ABE 转换为 CP-ABE 的方法,支持任何有界多项式大小的访问公式(包括与、或和门限操作).主要技术与 GPSW06[7]类似.Setup 算法规定参数(d,c),d 为访问树最大高度,c 为树中非叶节点的子女节点最大数目.同时,构造一棵(d,c)-通用访问树 T_u,然后根据 T_u 生成 PK 和 MK.安全性证明中,(d,c)控制了攻击者的询问能力.Encrypt 算法将(d,c)-有限访问树 T 转换为(d,c)-有限标准访问树 T_n,然后构造 T_n 到 T_u 的映射,最后根据映射完成加密.但是,标准型转换添加了大量非叶节点,增加了加密开销.T 的叶节点高度越不整齐,系统效率越低,因此该方法实际并不可行.

Liang 等人[28]改进了 BCP-ABE[27]机制,跳过中间标准型的转化,直接构造新的 T_u.T 直接映射到 T_u,缩短了系统公钥、用户私钥和密文的长度,提高了加/解密算法的效率.在 T 的叶节点高度不整齐时,效果显著.另外,该机制采用 DBDH 假设和不可伪造的一次签名(one time signature,简称 OTS)技术,扩展为 CCA 安全.

Ibraimi 等人[29]基于 DBDH 假设,提出一种新思路实现支持属性的与、或和门限操作的 CP-ABE 机制.首先实现一个基本 CP-ABE 机制,访问结构为由与、或节点组成的 l 叉树(l>1).Encrypt 算法采用模加机制赋值给与节点的子女节点,直接将秘密值赋给或节点的子女节点.用户的私钥与一个随机数相关,能够防止用户串谋.然后采用 Shamir 的门限秘密共享技术[18]扩展基本 CP-ABE 机制,得到支持属性与、或、门限操作的 CP-ABE 机制,其加解密开销低于 BSW07[14].

2.3 LSSS矩阵访问结构

与 GJPS08[27]采取转换方式实现 CP-ABE 不同,Waters[30]首次直接实现强数值假设下支持属性与、或和门限操作的 CP-ABE 机制.采用判定性并行双线性 Diffie-Hellman 指数(decisional Parallel Bilinear Diffie-Hellman Exponent,简称 DPBDHE)[31]假设.采用 LSSS 访问结构[15]$(\boldsymbol{M},\rho)$,其中,$\boldsymbol{M}$ 为 $\ell\times n$ 矩阵.Setup 算法选择随机数 a,$\alpha\in Z_q,h_1,\ldots,h_n\in G_1$,令 $MK=g^{\alpha},PK=(g,e(g,g)^{\alpha},g^{a},h_1,\ldots,h_n)$.KeyGen 选取随机数 t,$SK=(K=g^{\alpha}g^{at},L=g^{t},K_x=h_x^{t}\mid\forall x\in A_u)$.加密算法选择向量 $\vec{v}=(s,y_2,\ldots,y_n)\in Z_q^n$ 产生密钥构件.使用 CHK[25]技术能够扩展为 CCA 安全.但 W08[30]机制的密文长度、加/解密时间都随着访问结构的复杂性线性增长.

Lewko 等人[32]采用双系统加密机制[33,34],首先用完全可行的方法实现 CCA 安全的 CP-ABE 机制.访问结构也采取 LSSS 矩阵,支持任何单调的访问公式表示策略.先构造一次使用 CP-ABE 机制,规定公式中每个属性只能使用一次;然后将一次使用 CP-ABE 机制转换为属性多次使用的 ABE 机制,Setup 算法规定了属性被使用的

最大次数.转换不会增加密钥和密文的大小.与以往 ABE 机制不同,群 G_1,G_2 以 3 个不同素数的乘积作为阶,以这 3 个素数为阶的 G_1 的子群具有正交性.该机制基于 3 个 3 素数子群判定问题(3P-SDP)[34]证明了 CCA 安全.

2.4 分 析

综上所述,CN07[10]首先提出在 DBDH 假设下可证安全的 CP-ABE.W08[30]最先在 DPBDHE 假设下实现支持属性"与"、"或"和"门限"操作的 CP-ABE.LOST10[32]提出可行的 CCA 安全的 CP-ABE.表 3 对比分析了各机制采取的访问结构、支持的策略、安全证明采用的假设和 ID 模型.表 4 比较了各机制中系统公钥、主密钥、用户私钥和密文的长度.其中,密文的长度不计访问结构.表 5 比较了各机制的加解密时间.访问结构为(d,c)-有界树 T[27,28]的情形下($d\geqslant 1,c\geqslant 2$),用$\Sigma_*$表示将树*扩展为子女数目都为 c 的树所增节点集合,则$|\Sigma_{T_n}|>|\Sigma_T|>1$.设 LOST10[32]中 3 个素数分别为 q_1,q_2 和 q_3,则群的阶 $q'=q_1q_2q_3$.ITHJ09[29]中 $w'\subseteq A_u$ 为满足访问结构最小属性集.

Table 3 Comparision of security proof and policy complexity in CP-ABE

表 3 CP-ABE 机制的安全证明与策略复杂性对比

Access structure		System	Assumption	Model	Supported policy
AND gate	Two values/attribute	CN07[10]	DBDH	Selective	And, not
	Several values/attribute	NYO08[23]	DBDH, D-Linear	Selective	And
		EMNOS09[24]	DBDH	Selective	And
Tree	Tree without bound	BSW07[14]	Group model	Adaptive	And, or, threshold
		ITHJ09[29]	DBDH	Selective	And, or, threshold
	Bounded tree	GJPS08[27]	DBDH	Selective	Bounded and, or, threshold
		LCLX09[28]	DBDH	Selective	Bounded and, or, threshold
LSSS matrix		W08[30]	DPBDHE	Selective	And, or, threshold
		LOST10[32]	3P-SDP	Adaptive	And, or, threshold

Table 4 Comparision of size of keys and ciphertext in CP-ABE

表 4 CP-ABE 机制中各密钥与密文长度的比较

System	*PK*	*MK*	*SK*	Ciphertext
CN07[10]	$(3n+1)L_{G_1}+L_{G_2}$	$(3n+1)L_{Z_q}$	$(2n+1)L_{G_1}$	$(n+1)L_{G_1}+L_{G_2}$
NYO08[23]	$(2N'+1)L_{G_1}+L_{G_2}$	$(2N'+1)L_{Z_q}$	$(3n+1)L_{G_1}$	$(2N'+1)L_{G_1}+L_{G_2}$
EMNOS09[24]	$(N'+2)L_{G_1}+L_{G_2}$	$(N'+1)L_{Z_q}$	$2L_{G_1}$	$2L_{G_1}+L_{G_2}$
BSW07[14]	$3L_{G_1}+L_{G_2}$	$L_{Z_q}+L_{G_1}$	$(2\|A_u\|+1)L_{G_1}$	$(2\|A_C\|+1)L_{G_1}+L_{G_2}$
ITHJ09[29]	$(n+1)L_{G_1}+L_{G_2}$	$(n+1)L_{Z_q}$	$(\|A_u\|+1)L_{G_1}$	$(\|A_C\|+1)L_{G_1}+L_{G_2}$
GJPS08[27]	$(nc^{d-1}+c^d-1)L_{G_1}+L_{G_2}$	$(nc^{d-1}+c^d)L_{Z_q}$	$(\|A_u\|c^{d-1}+c^d-1)L_{G_1}$	$(\|A_C\|+\|\Sigma_{T_n}\|)L_{G_1}+L_{G_2}$
LCLX09[28]	$\left(n\frac{c^{d-1}}{c-1}+c^d-1\right)L_{G_1}+L_{G_2}$	$\left(n\frac{c^{d-1}}{c-1}+c^d\right)L_{Z_q}$	$\left(\|A_u\|\frac{c^{d-1}}{c-1}+c^d-1\right)L_{G_1}$	$(\|A_C\|+\|\Sigma_T\|)L_{G_1}+L_{G_2}$
W08[30]	$(n+2)L_{G_1}+L_{G_2}$	L_{G_1}	$(\|A_u\|+2)L_{G_1}$	$(2\|A_C\|+1)L_{G_1}+L_{G_2}$
LOST10[32]	$(n+2)L_{G_1}+L_{G_2}$	$L_{Z_q}+L_{G_1}$	$(\|A_u\|+2)L_{G_1}$	$(2\|A_C\|+1)L_{G_1}+L_{G_2}$

Table 5 Comparision of computational time in CP-ABE

表 5 CP-ABE 机制的计算开销比较

System	Encrypt	Decrypt
CN07[10]	$(n+1)G_1+2G_2$	$(n+1)C_e+(n+1)G_2$
NYO08[23]	$(2N'+1)G_1+2G_2$	$(3n+1)C_e+(3n+1)G_2$
EMNOS09[24]	$(n+1)G_1+2G_2$	$2C_e+2G_2$
BSW07[14]	$(2\|A_C\|+1)G_1+2G_2$	$2\|A_u\|C_e+(2\|S\|+2)G_2$
ITHJ09[29]	$(\|A_C\|+1)G_1+2G_2$	$(\|w'\|+1)C_e+(\|w'\|+1)G_2$
GJPS08[27]	$(\|A_C\|+\|\Sigma_{T_n}\|)G_1+2G_2$	$(\|A_u\|+\|\Sigma_{T_n}\|)C_e+2(\|S\|+\|\Sigma_{T_n}\|)G_2$
LCLX09[28]	$(\|A_C\|+\|\Sigma_T\|)G_1+2G_2$	$(\|A_u\|+\|\Sigma_T\|)C_e+2(\|S\|+\|\Sigma_T\|)G_2$
W08[30]	$(4\|A_C\|+1)G_1+2G_2$	$(2\|A_u\|+1)C_e+3\|A_u\|G_2$
LOST10[32]	$(4\|A_C\|+1)G_1+2G_2$	$(2\|A_u\|+1)C_e+3\|A_u\|G_2$

由表 3 可知:在标准假设下,只有 W08[30]和 ITHJ09[29]支持属性的与、或、门限操作;只有 CN07[10]支持属性

的非操作.由表 4 和表 5 可知:EMNOS09[24]的用户私钥和密文最短、加/解密开销最低;ITHJ09[29]的加/解密开销比 W08[30]低;BSW07[14]的系统公钥和主密钥与系统属性无关,具有最短的系统公钥;W08[30]的主密钥最短.目前的研究工作仍没有实现基于标准数值理论假设的支持属性与、或、门限和非操作的 CP-ABE 机制.

3 ABE 的属性撤销机制

ABE 中的属性撤销分为用户撤销、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.

根据撤销由机构还是发送方执行,当前 ABE 撤销机制的研究工作分为间接撤销和直接撤销两类.根据 Attrapadung 和 Imai[35]的定义,在间接撤销模式下,授权机构周期性释放密钥的更新,只有未撤销的用户才能更新密钥,从而使已撤销用户的密钥无效.在直接撤销模式下,发送者在加密消息时规定撤销列表,直接实现属性密钥的撤销.间接撤销的优势在于发送者无需获取撤销列表.直接撤销的优势在于所有未撤销用户无需更新密钥,减轻授权机构的负担.AI09b[35]结合两种撤销模式的优点,提出了混合撤销模式.

3.1 间接撤销

ABE 撤销机制的大部分研究工作都采用间接撤销模式.前期的研究由授权机构执行撤销[14,19,36],加密过程都与时间有关,属性只有到期失效时才能撤销;更新阶段,授权机构的工作量大.为减轻授权机构的负担并实现属性的即时撤销,后期工作引入半可信第三方[37,38],但要保证第三方的诚实性.

Pirretti 等人[19]最早提出 ABE 机制属性撤销的办法:每个属性包含一个有效期.授权机构周期性地释放属性的最新版本,并重新颁发所有用户的密钥信息.若删除系统的某个属性,机构停止发布该属性的最新版本,在周期性更新所有用户密钥时,不再颁发与该属性对应的密钥构件.如需撤销某个用户的属性,机构撤销用户私钥中该属性的最新版本.该方法简单,但存在不少缺点:加密方需与机构协商属性有效期;用户需保存每个时间段的密钥,撤销日期的粒度越细,密钥存储开销越大;属性密钥更新阶段,用户与机构在线交互,授权机构的工作量随用户数目线性增长,系统的可扩展性不好;属性也无法在到期前撤销.

为消除加密方与授权机构的协调,并降低用户密钥存储开销,Bethencourt 等人[14]提出一种 CP-ABE 的密钥更新思路.授权机构给每个用户的属性一个终止日期,密文附带时间信息.解密要求用户属性满足密文的访问策略,且终止日期在密文附带的时间之后.但在密钥更新过程中,用户仍需与授权机构在线交互,授权机构的工作量与属性到期的用户数量线性相关.另外,该机制不支持属性的即时撤销.

Boldyreva 等人[36]采用二叉树提出可撤销的 ABE 机制,支持 KP-ABE 中用户的撤销.每个用户与二叉树的叶节点相关,密钥更新数量与用户数量为对数关系.用户密钥分为两部分:一部分与访问结构相关,称为私钥,由授权机构生成;另一部分与时间相关,称为密钥更新,由授权机构公布,对全体用户可见,消除了密钥更新过程中的在线交互.授权机构撤销用户时,停止公布该用户的密钥更新,密文与属性集和时间相关.这种算法具有 KP-ABE 的抗串谋特性,保证了算法的安全性,但不支持属性的即时撤销.

为了实现属性的即时撤销,Ibraimi 等人[37]基于 ITHJ09[29]的 CP-ABE 引入半可信第三方作为仲裁者.仲裁者维持一个属性撤销列表,包括撤销的系统属性和用户属性信息.核心思想是,用户不再持有完整的密钥,而是将密钥分为两份,分别由仲裁者和用户持有.用户私钥与随机生成的用户标识相关,能够防止用户的串谋攻击.解密时,用户将满足访问树的最小属性集,密文和用户标识发送给仲裁者.仲裁者先判断该属性集中是否存在被撤销的属性,若无,则利用掌握的部分用户密钥执行与访问树叶节点相关的解密任务,并将结果返给用户,再由用户完成解密运算;否则,返回错误信号.该机制不需要更新未撤销属性的用户私钥.授权机构在为所有用户生成私钥后即可离线,减轻了授权机构的工作量.仲裁者持有部分密钥并参与解密运算,因此必须诚实,且保持在线.

Yu 等人[38]在 CN07[10]的 CP-ABE 机制基础上引入半信任的代理服务器,采用代理重加密技术,支持可撤销的 KP-ABE.授权机构用版本号标记主密钥的演化版本,初始化时置为 1,系统公钥、密文、用户私钥和代理重密钥都用版本号标记,以表示由主密钥的哪个版本产生.当发生撤销时,授权机构更新主密钥中与被撤销属性对应

的构件,将版本号的值加 1,然后生成新的代理重密钥.代理服务器用最新版本的代理重密钥再加密存储的密文,为所有未被撤销的用户更新密钥.被撤销属性用户的私钥构件的版本号不是最新,无法解密,从而实现属性的即时撤销.该机制将授权机构的部分负担转移到代理服务器,减轻授权机构的工作量,但是代理服务器和授权机构必须在线,而且代理服务器要更新全部未撤销用户的私钥.

3.2 直接撤销

OSW07[21]首次提出 CP-ABE 的直接撤销思想,将用户标识作为一种属性,把被撤销用户标识的"非"与密文关联起来,使得撤销的用户无法解密密文,但是增加了密文和用户私钥的大小.Attrapadung 等人[31]采取同样的思路,减少了撤销的开销,提出 Broadcast ABE 机制,实现 KP-ABE 和 CP-ABE 的直接撤销.设 $W=U\backslash R$,其中:U 为系统中用户的标识集;R 为用户撤销列表,包含了被撤销用户的 ID.密文与 W 相关,而用户私钥与其唯一标识 ID 相关.KP-ABE 中,用与门将 W 与密文属性连接起来;在 CP-ABE 中,用与门将 W 与密文访问策略连接起来.接收者只有满足 $ID\in W$ 且属性与策略匹配时,才能解密密文.

直接撤销模式下,未撤销用户无需周期性更新密钥.发送方加密时规定一个系统属性撤销列表可实现系统属性的撤销.但 OSW07[21]和 AI09a[31]都采用用户标识,仅支持整个用户的撤销,没有解决用户属性撤销的情况,而且增加了系统公钥长度.

3.3 混合模式

Attrapadung 等人[35]充分利用两种撤销模式的优势,采取二叉树,针对 KP-ABE 的撤销问题提出混合可撤销机制 HR-ABE.发送方在加密时可以选择直接或间接的撤销模式.若选择直接模式,则直接规定用户撤销列表 R;若选择间接模式,则选择当前时间 t.HR-ABE 包括两个子系统:直接可撤销的 ABE 和间接可撤销的 ABE.发送方根据所选模式使用相应的子系统.用户密钥与访问结构和唯一标识 ID 相关.每个用户的密钥由来自每个子系统的密钥组成,能够解密以任何模式构造的密文.直接模式下,接收方用密钥即可解密;间接模式下,授权机构在创建更新的密钥时会规定用户撤销列表 R,接收方在时刻 t 后必须从授权机构获取更新的密钥.若密文属性集满足接收方的密钥访问结构且 $ID\notin R$,则解密成功.该方法只解决了用户撤销的问题,无法处理用户属性的撤销;而两个子系统的使用,显著增加了用户密钥长度.

3.4 分 析

上述关于 ABE 撤销机制的研究工作,二叉树[35,36]将密钥更新数量减少为用户的对数级;少数撤销机制无需更新未撤销用户的密钥[21,31,37].表 6 对比分析了上述撤销机制.AA(attribute authority)表示授权机构.对于没有在线方要求的系统,用户通过 AA 的张贴获取更新信息.对于有在线方要求的系统,用户需与在线方交互获取信息.混合模式[35]下,直接模式的执行者为发送方,间接模式的执行者为 AA,撤销速度与执行者相关.由表 6 可知,目前由发送方执行的撤销机制[21,31,35]虽消除了在线约束,实现了即时撤销,但没有解决用户属性的撤销.因而,未来仍需研究无在线交互,达到所有撤销要求,并实现即时撤销的 ABE 撤销机制.

Table 6 Comparision of revocation schemes

表 6 各种撤销机制对比

System	Executor	Online party	Supported schemes		Speed	Revoke		
			KP-ABE	CP-ABE		User	User's attribute	System attribute
PTMW06[19]	AA	AA	Yes	Yes	Expiry	Yes	Yes	Yes
BSW07[14]	AA	AA	/	Yes	Expiry	Yes	Yes	Yes
BGK08[36]	AA	/	Yes	/	Expiry	Yes	/	Yes
IPNHJ09[37]	Third party	Third party	/	Yes	Immediate	Yes	Yes	Yes
YWR10[38]	Third party	Third party, AA	Yes	Yes	Immediate	Yes	Yes	Yes
OSW07[21]	Sender	/	/	Yes	Immediate	Yes	/	Yes
AI09a[31]	Sender	/	Yes	Yes	Immediate	Yes	/	Yes
AI09b[35]	Hybrid	/	Yes	/	Hybrid	Yes	/	Yes

4 责任认定

ABE 中,防止密钥滥用的难点在于定位盗版密钥的来源,即查清是哪个用户或者授权机构所为.目前,盗版密钥责任认定的方案有:(1) 关于 CP-ABE[39,40]机制中的追责性,LRK09[39]将责任定位到用户或授权机构,LRZW09[40]将责任定位到用户,同时实现策略隐藏.(2) 关于 KP-ABE[41]机制中的追责性, YRLL09[41]将责任定位到用户,且发送方隐藏部分属性.

4.1 防止密钥滥用的CP-ABE

LRK09[39]基于 DBDH 和 CDH 假设,提出可追责的 CP-ABE(CP-A^{2}BE)机制,解决了 CP-ABE 中认定用户或授权机构责任性的问题.用户首先通过可信第三方-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.用户的解密密钥包含了与证书公钥对应的私钥,仅用户知道.假设证书中密钥的机密性高于授权机构颁发的属性私钥.用户若共享其解密密钥,会泄露密级更高的证书私钥.盗版密钥追踪算法判断密钥中的证书私钥是否存在相应的有效证书公钥.若存在,说明是持有该证书的用户泄露了其解密密钥;否则,说明是授权机构的不良行为.CP-A^{2}BE 假设盗版设备中有格式规范的解密密钥,只能进行白盒追踪;仅支持属性的“与”操作,表达策略的能力有限;另外,公钥证书中心负责为所有用户颁发证书,工作量大,严重影响系统性能.

为实现策略隐藏以达到接收方匿名性,LRZW09[40]基于 DBDH 和 D-Linear 假设提出可追责的匿名 CP-ABE (CP-A^{3}BE)机制,解决了用户的责任认定问题.其核心思想是,将用户标识嵌入属性私钥来阻止用户之间非法共享密钥.加密算法采取与 NYO08[23]类似的技术实现策略隐藏,达到接收方匿名的效果,使得追踪加密与普通加密算法对于用户来说是不可分辨的.但是,追踪加密算法产生的密文标识域为可疑用户,只有属性集满足密文策略的可疑用户才能解密该消息,从而确定盗版密钥的产生者.CP-A^{3}BE 具有黑盒追踪的特点,即仅观察对某些输入的输出就能追踪盗版设备.该机制支持策略隐藏,保护发送方的隐私,但是显著增加解密密钥和密文的长度,只能表示“与”策略.

4.2 防止密钥滥用的KP-ABE

YRLL09[41]基于 DBDH 和 D-Linear 假设提出无滥用 KP-ABE(AFKP-ABE)机制,解决了 KP-ABE 机制中合法用户与他人分享密钥造成的密钥滥用问题.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.追踪算法将可疑标识对应的标识相关属性与密文关联起来,使得只有可疑标识的用户才能解密追踪密文,从而提供盗版的证据.追踪算法采用与 NYO08[23]类似的技术,在加密时隐藏标识相关属性和部分普通属性,使得盗版设备不能探测追踪行为.AFKP-ABE 以叛徒追踪系统[42]的定义为基础,是黑盒追踪.

4.3 分析

表 7 对比分析了上述 3 种机制.它们都解决了由用户导致的密钥滥用问题的责任认定.LRK09[39]虽可认定授权机构,但假设盗版设备中的密钥格式规范,缺乏可行性.LRZW09[40]和 YRLL09[41]都考虑保护发送方的隐私,但是 YRLL09[41]仅隐藏部分属性.只有 YRLL09[41]支持属性的与、或、门限操作.因而,还需研究策略灵活的可追责的 CP-ABE,以及保护发送方隐私的可追责的 KP-ABE.

Table 7 Comparision of AFKP-ABE, CP-A^{2}BE and CP-A^{3}BE

表 7 AFKP-ABE,CP-A^{2}BE 与 CP-A^{3}BE 的对比

System	Trace property	Trace effect	Key form	Third party	Sender hides	Assumption	Supported policy
CP-A^{2}BE[39]	White-Box	AA, user	Well-Formed	Trusted	/	DBDH, CDH	And
CP-A^{3}BE[40]	Black-Box	User	/	/	Policy	DBDH, D-Linear	And
AFKP-ABE[41]	Black-Box	User	/	/	Part attributes	DBDH, D-Linear	And, or, threshold

5 多机构 ABE

多机构 ABE 系统包含多个属性授权机构(AA)和大量用户.用户向某个 AA 证明自己具有某些该机构管理的属性,请求相应的解密密钥.每个 AA 都有一个主密钥.为保证解密的正确运行,所有 AA 的主密钥之和应为系统的主密钥.但是,如果 AA 用相同的主密钥为每个用户生成私钥,那么具有足够多属性的用户将能够重构 AA 的主密钥,不同用户串谋就可恢复出系统主密钥,从而威胁系统安全性.因而,解密正确性和系统安全性之间存在矛盾,这是多机构 ABE 的研究难点.

目前,关于多机构 ABE 的研究工作都以基本 ABE 机制为基础,采用用户全局唯一标识(GID)[43]来防止用户串谋.根据是否采用中央授权机构(central authority,简称 CA)来保证解密的正确运行,目前的研究分为采用 CA[43,44]的多机构 ABE 和无 CA[45,46]的多机构 ABE 两类.

5.1 采用CA的多机构ABE

基于 BDH 假设,Chase[43]最先采用用户 GID,伪随机函数(PRF)和 CA 解决多机构 ABE 的研究难点,提出多 AA 的 ABE(MA-ABE)机制.MA-ABE 中,系统主密钥为 y_0.AA_k 的私钥由种子 s_k 和 n 个随机数 $t_{k,i}$ 组成,其中,$k\in\{1,\ldots,N\}$,$i\in\{1,\ldots,n\}$.先用 PRF 计算 $y_{k,u}=F_{s_k}(u)$,u 为用户的 GID,然后令随机多项式的 $p(0)=y_{k,u}$,颁发用户私钥构件 $D_{k,i}=g^{p(i)/t_{k,i}}$.$y_{k,u}$ 能够防止不同用户对 AA_k 的串谋攻击.CA 的私钥为$(y_0,\{s_k\}|k=1,\ldots,N)$,可以根据用户的 GID 重构 AA_k 计算的 $y_{k,u}$ 颁发用户私钥部件 $D_{CA}=g^{y_0-\sum_{k=1}^{N}y_{k,u}}$.MA-ABE 的加解密思想与 SW05[6]一致.D_{CA} 帮助用户使用来自多个 AA 的密钥解密消息,使解密独立于 GID.

AA 独立为用户颁发密钥.CA 参与授权,但不知用户属性.系统增加新 AA 时,CA 选择新的系统主密钥和公钥,保存新 AA 的 PRF 种子.所有从新 AA 获取属性私钥的用户必须从 CA 获取新的 D_{CA},但无需从旧 AA 获取私钥构件.缺点是 CA 能够解密用户密文,必须完全可信.另外,用户需要向 AA 提交 GID,使得 AA 之间能够根据 GID 恢复用户的完整轮廓,可能危害到用户隐私.而且,用户属性变更会引起 GID 变更.

为解决 MA-ABE 中 CA 完全可信的问题,Bŏzovíc 等人[44]基于 DBDH 假设提出一种将 CA 视为诚实但好奇的方法:CA 诚实地遵守协议,同时好奇地解密密文.CA 向每个 AA 发送消息,通过反馈得到系统公钥,仅在增加新的 AA 时才为每个用户生成一个私钥,其在初始化阶段的诚实性保证了加密的不可区分性.密钥生成、防止串谋和加解密的思想与 C07[43]类似.

5.2 无CA的多机构ABE

为避免使用 CA 带来的安全脆弱性,Lin 等人[45]采用密钥分发(DKG)和联合的零秘密共享(JZSS)技术[47]解决研究挑战,基于 DBDH 假设提出一种多 AA 的 ABE(threshold MA-FIBE)机制.Setup 算法设置决定系统效率和安全性的常数 m,运行 2 次 DKG 协议产生系统主密钥 a_0 和 b_0,并形成 a_0 与 b_0 的一个(t,N)门限秘密共享,a_0 用于加密,b_0 用于生成用户私钥.AA_k 仅具有 a_0 的份额 $a_{k,0}$ 和 b_0 的份额 $b_{k,m+1}$.运行 m 次 JZSS 协议产生系数 $a_{k,j}$ (j=1,…,m),形成 0 的一个(t,N)门限多项式秘密共享.用户随机选择一个 GID 提交给 AA_k,由 AA_k 验证 GID 有效后,用多项式 $p_k(x)=a_{k,0}+a_{k,1}x+\ldots+a_{k,m}x^m$ 生成用户私钥,其中,$p_k(0)=a_{k,0}+a_{k,1}\mathrm{GID}+\ldots+a_{k,m}\mathrm{GID}^m$.Encrypt 算法将一串 0 作为密文后缀,用以检验解密是否有效.根据 DKG 协议,用户需从至少$(t+1)$个诚实的 AA_k 获得 $p_k(0)$(其中,$t\leqslant n/2$)才能在解密的最后步骤消去 GID,得到 a_0,使解密独立于 GID.该机制最多只能防止 m 个用户串谋,只要串谋用户数目达到$(m+1)$,加密就不安全.增加新 AA 时需要重新初始化整个系统,开销巨大.

Chase 等人[46]提出 Multi-authority ABE 机制解决 LCLS08[45]只能防止 m 个用户串谋的问题,避免了用户向 AA 提交 GID 带来的隐私危害.该机制在初始化阶段执行一次共享,每对 AA(j,k)共享一个 PRF 种子,共需 $O(N^2)$ 个 PRFs,无需 CA 也能保证解密的正确性.每个 AA 最终使用的 PRF 是$(N-1)$个基本 PRFs 的线性组合,每个基本 PRF 的系数为 1 或者−1.累加不同机构的最终 PRF 时,恰当选择加和减,能使这些 PRF 值互相抵消,使得解密最后阶段与 GID 无关,保证了解密能力仅由用户属性决定.只要至少有两个 AA 是诚实的,该机制就是安全的,最多能够容忍$(N-2)$个 AA 被破坏.同时,采用匿名密钥颁发(AKI)协议保护用户隐私,用户与 AA 交互时采用别名,对

AA 隐藏 GID.缺点是增加新 AA 时,初始化阶段执行的 PRF 次数会增加 $O(N)$,系统公钥改变,用户必须向所有的 AA 重新申请密钥,开销随用户数目线性增长.

5.3 分 析

上述 4 种多机构 ABE 机制都采用了用户 GID 来防止用户串谋,但用户解密能力都与 GID 无关.C07[43], CC09[46]和 BSSV09[44]充分利用了 PRF 对于敌手而言无法在多项式时间内区分随机选择的函数和真正随机函数的特征.采用 CA 的方法在系统增加新 AA 时,旧 AA 无需更新用户密钥,开销较低.表 8 对比分析了上述机制的性能,其中:容忍度表示系统能够忍受的被破坏机构的最大数目,或恶意用户最大数目;各种协议比较的是生成用户私钥需运行的次数.无 CA 机制容忍度大,对 AA 的可信性要求降低,但安全性依赖于协议.上述系统都以基本 ABE 机制为基础,只能表示门限策略.

Table 8 Performance of multi-authorities ABE

表 8 多机构 ABE 机制性能

System	Tolerance	DKG	JZSS	AKI	AA's secret key	User's secret key	Ciphertext
C07[43]	0 CA	0	0	0	$(n+1)L_{Z_q}$	$(\|A_u\|+1)L_{G_1}$	$(\|A_C\|+1)L_{G_1}+L_{G_2}$
BSSV09[44]	0 CA	0	0	0	$(\|A_k\|+1)L_{Z_q}+nL_{G_1}$	$(\|A_u\|+N)L_{G_1}$	$(\|A_C\|+1)L_{G_1}+L_{G_2}$
LCLS08[45]	m users	2	m	0	$(\|A_k\|+m+2)L_{Z_q}$	$\|A_u\|L_{G_1}$	$\|A_C\|L_{G_1}+L_{G_2}$
CC09[46]	(N–2)AA	0	0	N–1	$(\|A_k\|+N)L_{Z_q}$	$(\|A_u\|+1)L_{G_1}$	$(\|A_C\|+1)L_{G_1}+L_{G_2}$

6 总结及未来研究方向

表 9 根据 ABE 机制中标准假设和策略灵活性的兼顾、撤销机制、可追责性、多机构下 ABE 等难题,分析当前的研究工作已解决哪些问题,从而总结基本 ABE,KP-ABE 和 CP-ABE 机制的上述难题是否都已解决.其中:标准假设指数值理论假设;策略灵活性指支持属性的与、或、门限操作,但是基本 ABE 仅支持属性的"门限"操作;撤销包括用户、用户属性、系统属性的撤销.

由表 9 可知,基本 ABE 的研究工作没有解决用户追责性.KP-ABE 的研究工作都采用 GPSW06[7]的结构,因而除多机构情况,其余难题均解决.CP-ABE 的研究中,解决撤销难题的系统[29]采用解决了标准假设和策略灵活性兼顾难题的系统[30]的结构,但是解决用户追责性难题的系统[39,40]所采用的结构[23]只能表示属性的与操作,因而目前 CP-ABE 的研究仅实现标准假设下策略表示灵活的可撤销的 CP-ABE 机制,未解决用户责任认定和多机构的难题.而每种机制都没有有效解决授权机构追责性难题的方法.

Table 9 Summary the research of ABE

表 9 ABE 研究情况总结

Scheme	Standard assumption	Policy flexibility	Revocation	Accountable user	Multi-authorities
Basic ABE	SW05[6], PTMW06[19], BSZ07[20]	SW05[6], PTMW06[19], BSZ07[20]	PTMW06[19]	/	C07[43], BSSV09[44], LCLS08[45], CC09[46]
KP-ABE	GPSW06[7], OSW07[21], LW10[17]	GPSW06[7], OSW07[21], LW10[17]	PTMW06[19], YWR10[38]	YRLL09[41]	/
CP-ABE	CN07[10], NYO08[23], EMNOS09[24], ITHJ09[29], GJPS08[27], LCLX09[28], W08[30]	BSW07[14], ITHJ09[29], W08[30], LOST10[32]	PTMW06[19], BSW07[14], IPNHJ09[29], YWR10[38]	LRK09[39], LRZW09[40]	/

通过上述策略灵活性、密钥撤销、追责性、多机构情形等方面研究分析,我们认为,ABE 研究中仍存在值得深入研究的问题,主要包括:

(1) 多机构 KP-ABE 与 CP-ABE.目前,多机构 ABE 的工作都研究基本 ABE,而围绕 KP-ABE 和 CP-ABE 的研究并未展开.KP-ABE 和 CP-ABE 在现实应用中的重要性已经得到实践证明,在付费电视系统、组密钥管理、用户隐私保护等领域得到广泛应用,因而多机构 KP-ABE 与 CP-ABE 的研究成为一个急切需求;

(2) 可撤销的能认定用户责任的 CP-ABE 机制.目前的研究已实现标准假设下策略灵活的、可撤销的 CP-ABE 机制[29],但是该机制未解决用户责任认定难题.因而,未来需要研究策略表达能力完备的、可撤销的、能认定用户责任的 CP-ABE 机制;

(3) 授权机构的信任问题.ABE 系统中,授权机构的完全可信给系统带来安全隐患.一旦授权机构被破坏,攻击者可以获取任何用户的密钥,并能解密所有密文.目前,只有 Goyal 等人[48]采取黑盒模式解决 IBE 系统中授权机构完全可信带来的问题,但 ABE 机制中,授权机构的责任认定问题仍无有效的解决办法;

(4) 策略隐藏的 CP-ABE.CP-ABE 机制中,策略体现了发送方的隐私.同时,为了避免用户攻击系统,例如频繁改变行为来获得消息,或基于策略推断重要的消息,也需要隐藏策略.Kapadia 等人[49]提出了隐藏策略的方法,但是不能防止用户串谋,并且引入一个在线的半可信服务器.为防止用户串谋攻击,Yu 等人基于 CN07[10]的构造提出两种匿名 CP-ABE 机制[8,12],但采用了强假设.Nishide 等人[23]首次提出基于 DBDH 和 D-Linear 假设的匿名 CP-ABE 机制实现策略隐藏,但是只能表示属性的与操作.因而,研究标准假设下具备丰富的策略表示能力,同时实现策略隐藏的 CP-ABE 机制,是未来需要研究的一个方向;

(5) 层次化 ABE.实际应用中的授权机构之间通常存在层次关系,属性之间也有层次关系,这使得层次化 ABE 的研究具有现实需求.CN07[10]为提高算法效率,提出将属性分层次的思想.Li 等人[50]使用层次化的 IBE(HIBE)技术和 ABE 中的秘密共享技术,采用树层次结构表示属性间的层次关系,提高了 ABE 的效率,但没有研究更高效的表示属性间层次关系的数据结构.而且上述研究仅处理了属性的层次关系,没有处理多个授权机构间的层次关系,需要研究类似于 HIBE[33,34,51−55]的层次化 ABE 系统;

(6) 双策略 ABE.KP-ABE 和 CP-ABE 机制中的策略只能控制对用户密钥或密文的访问.Attrapadung 和 Imai[56]引入主客观属性和主客观策略的概念,代数结合 CP-ABE[30]和 KP-ABE[7],实现双策略 ABE,使得与密文相关的策略有效保护资源,与用户密钥相关的策略保护用户权限,但是增加了密钥和密文长度.提高双策略 ABE 机制的效率并增加策略的灵活性,是未来研究的方向之一.

致谢 在此,我们向对本文提出宝贵修改意见的评审老师和同行表示衷心的感谢.

References:

[1] Fiat A, Naor M. Broadcast encryption. In: Stinson DR, ed. Advances in Cryptology-CRYPTO'93. Berlin, Heidelberg: Springer-Verlag, 1994. 480−491.

[2] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers. In: Kilian J, ed. Advances in Cryptology-CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 41−62.

[3] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup V, ed. Advances in Crytology-CRYPTO 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 258−275. [doi: 10.1007/11535218_16]

[4] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Advances in Cryptology-CRYPTO'84. Berlin, Heidelberg: Springer-Verlag, 1984. 47−53.

[5] Boneh D, Franklin M. Identity-Based encryption from the weil pairing. In: Kilian J, ed. Advances in Cryptology-CRYPTO 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[6] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer R, ed. Advances in Cryptology-EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 457−473.

[7] Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

[8] Yu SC, Ren K, Lou WJ. Attribute-Based content distribution with hidden policy. In: Proc. of the 4th Workshop on Secure Network Protocols (NPSec). Orlando: IEEE Computer Society, 2008. 39−44. [doi: 10.1109/NPSEC.2008.4664879]

[9] Traynor P, Butler K, Enck W, Mcdaniel P. Realizing massive-scale conditional access systems through attribute-based cryptosystems. In: Proc. of the 15th Annual Network and Distributed System Security Symp. (NDSS 2008). San Diego: USENIX Association, 2008. 1−13.

[10] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 456−465. [doi: 10.1145/1315245.1315302]

[11] Cheung L, Cooley JA, Khazan R, Newport C. Collusion-Resistant group key management using attribute-based encryption. http://eprint.iacr.org/2007/161.pdf

[12] Yu SC, Ren K, Lou WJ. Attribute-Based on-demand multicast group setup with membership anonymity. Computer Networks, 2010, 54(3):377−386. [doi: 10.1016/j.comnet.2009.09.009]

[13] Baden R, Bender A, Spring N, Bhattacharjee B, Starin D. Persona: An online social network with user-defined privacy. In: Proc. of the ACM SIGCOMM 2009 Conf. on Data Communication. New York: ACM Press, 2009. 135−146. [doi: 10.1145/1592568.1592585]

[14] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[15] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Technion: Israel Institute of Technology, 1996.

[16] Liang XH. Research on attribute-based cryptosystem [MS. Thesis]. Shanghai: Shanghai Jiaotong University Press, 2009 (in Chinese).

[17] Lewko A, Sahai A, Waters B. Revocation systems with very small private keys. In: Proc. of the IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2010. 273−285. [doi: 10.1109/SP.2010.23]

[18] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612−613. [doi: 10.1145/359168.359176]

[19] Pirretti M, Traynor P, Mcdaniel P, Waters B. Secure attribute-based systems. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2006. 99−112. [doi: 10.1145/1180405.1180419]

[20] Baek J, Susilo W, Zhou J. New constructions of fuzzy identity-based encryption. In: Proc. of the ASIAN ACM Conf. on Computer and Communications Security (ASIACCS 2007). New York: ACM Press, 2007. 368−370. [doi: 10.1145/1229285.1229330]

[21] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 195−203. [doi: 10.1145/1315245.1315270]

[22] Naor M, Pinkas B. Efficient trace and revoke schemes. In: Frankel Y, ed. Proc. of the Financial Cryptography. Berlin, Heidelberg: Springer-Verlag, 2001. 1−20. [doi: 10.1007/978-3-540-68914-0_7]

[23] Nishide T, Yoneyama K, Ohta K. Attribute-Based encryption with partially hidden encryptor-specified access structures. In: Bellovin SM, Gennaro R, Keromytis A, Yung M, eds. Proc. of the Applied Cryptography and Network Security. Berlin, Heidelberg: Springer-Verlag, 2008. 111−129. [doi: 10.1007/978-3-540-68914-0_7]

[24] Emura K, Miyaji A, Nomura A, Omote K, Soshi M. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Bao F, Li H, Wang G, eds. Proc. of the Information Security Practice and Experience (ISPEC 2009). Berlin, Heidelberg: Springer-Verlag, 2009. 13−23. [doi: 10.1007/978-3-642-00843-6_2]

[25] Canetti R, Halevi S, Katz J. Chosen-Ciphertext security from identity-based encryption. In: Advances in Cryptology-EUROCRYPT 2004. Berlin, Heidelberg: Springer-Verlag, 2004. 207−222.

[26] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Proc. of the Theory of Cryptography Conf. (TCC). Berlin, Heidelberg: Springer-Verlag, 2007. 535−554. [doi: 10.1007/978-3-540-70936-7_29]

[27] Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption. In: Aceto L, Damgård I, Goldberg LA, Halldórsson M M, Ingólfsdóttir A, Walukiewicz I, eds. Proc. of the ICALP 2008. Berlin, Heidelberg: Springer-Verlag, 2008. 579−591. [doi: 10.1007/978-3-540-70583-3_47]

[28] Liang XH, Cao ZF, Lin H, Xing DS. Provably secure and efficient bounded ciphertext policy attribute based encryption. In: Proc. of the ASIAN ACM Symp. on Information, Computer and Communications Security (ASIACCS 2009). New York: ACM Press, 2009. 343−352. [doi: 10.1145/1533057.1533102]

[29] Ibraimi L, Tang Q, Hartel P, Jonker W. Efficient and provable secure ciphertext-policy attribute-based encryption schemes. In: Proc. of the Information Security Practice and Experience. Berlin, Heidelberg: Springer-Verlag, 2009. 1−12. [doi: 10.1007/978-3-642-00843-6_1]

[30] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. http://eprint.iacr.org/2008/290.pdf [doi: 10.1007/978-3-642-19379-8_4]

[31] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography-Pairing 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 248−265. [doi: 10.1007/978-3-642-03298-1_16]

[32] Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: Attribute-Based encryption and (hierarchical) inner product encryption. In: Advances in Cryptology-EUROCRYPT 2010. LNCS 6110, Berlin, Heidelberg: Springer-Verlag, 2010. 62−91. [doi: 10.1007/978-3-642-13190-5_4]

[33] Waters B. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In: Halevi S, ed. Advances in Cryptology-CRYTO 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 619−636. [doi: 10.1007/978-3-642-03356-8_36]

[34] Lewko A, Waters B. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Proc. of the 7th Theory of Cryptography Conf. (TCC 2010). Berlin, Heidelberg: Springer-Verlag, 2010. 455−479. [doi: 10.1007/978-3-642-11799-2_27]

[35] Attrapadung N, Imai H. Attribute-Based encryption supporting direct/indirect revocation modes. In: Parker MG, ed. Proc. of the Cryptography and Coding 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 278−300. [doi: 10.1007/978-3-642-10868-6_17]

[36] Boldyreva A, Goyal V, Kumar V. Identity-Based encryption with efficient revocation. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2008. 417−426. [doi: 10.1145/1455770.1455823]

[37] Ibraimi L, Petkovic M, Nikova S, Hartel P, Jonker W. Mediated ciphertext-policy attribute-based encryption and its application. In: Proc. of the 10th Int'l Workshop on Information Security Applications-WISA 2009. LNCS 5932, Berlin, Heidelberg: Springer-Verlag, 2009. 309−323. [doi: 10.1007/978-3-642-10838-9_23]

[38] Yu SC, Wang C, Ren K, Lou WJ. Attribute based data sharing with attribute revocation. In: Proc. of the ASIAN ACM Conf. on Computer and Communications Security (ASIACCS 2010). New York: ACM Press, 2010. 261−270. [doi: 10.1145/1755688.1755720]

[39] Li J, Ren K, Kim K. A^2BE: Accountable attribute-based encryption for abuse free access control. http://eprint.iacr.org/2009/118.pdf

[40] Li J, Ren K, Zhu B, Wan ZG. Privacy-Aware attribute-based encryption with user accountability. In: Proc. of the Information Security Conf. 2009. LNCS 5735, Berlin, Heidelberg: Springer-Verlag, 2009. 347−362. [doi: 10.1007/978-3-642-04474-8_28]

[41] Yu SC, Ren K, Lou WJ, Li J. Defending against key abuse attacks in KP-ABE enabled broadcast systems. In: Proc. of the Security and Privacy in Communication Networks. Berlin, Heidelberg: Springer-Verlag, 2009. 311−329. [doi: 10.1007/978-3-642-05284-2_18]

[42] Boneh D, Sahai A, Waters B. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In: Vaudenay S,ed. Advances in Cryptology-EUROCRYPT 2006. LNCS 4004, Berlin, Heidelberg: Springer-Verlag, 2006. 573−592. [doi: 10.1007/11761679_34]

[43] Chase M. Multi-Authority attribute based encryption. In: Proc. of the Theory of Cryptography Conf. (TCC). Berlin, Heidelberg: Springer-Verlag, 2007. 515−534.

[44] Božović V, Socek D, Steinwandt R, Villányi VI. Multi-Authority attribute based encryption with honest-but-curious central authority 2009. http://eprint.iacr.org/2009/083.pdf

[45] Lin H, Cao ZF, Liang X, Shao J. Secure threshold multi authority attribute based encryption without a central authority. In: Chowdhury DR, Rijmen V, Das A, eds. Proc. of the Cryptology in India-INDOCRYPT 2008. Berlin, Heidelberg: Springer-Verlag, 2008. 426−436. [doi: 10.1007/978-3-540-89754-5_33]

[46] Chase M, Chow SSM. Improving privacy and security in multi-authority attribute-based encryption. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2009. 121−130. [doi: 10.1145/1653662.1653678]

[47] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems. Journal of Cryptology, 2007,20(1):51−83. [doi: 10.1007/s00145-006-0347-3]

[48] Goyal V, Lu S, Sahai A, Waters B. Black-Box accountable authority identity-based encryption. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2008. 427−436. [doi: 10.1145/1455770.1455824]

[49] Kapadia A, Tsang PP, Smith SW. Attribute-Based publishing with hidden credentials and hidden policies. In: Proc. of the 14th Annual Network and Distributed System Security Symp. (NDSS 2007). USENIX Association, 2007. 179−192.

[50] Li J, Wang Q, Wang C, Ren K. Enhancing attribute-based encryption with attribute hierarchy. In: Proc. of the Mobile Networks and Applications. Berlin, Heidelberg: Springer-Verlag, 2010. 1−9. [doi: 10.1007/s11036-010-0233-y]

[51] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model. In: Gilbert H, ed. Advances in Cryptology-EUROCRYPT 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 553−572.

[52] Boneh D, Boyen X, Goh EJ. Hierarchical identity based encryption with constant size ciphertext. In: Cramer R, ed. Advances in Cryptology-EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 440−456. [doi: 10.1007/11426639_26]

[53] Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork C, ed. Advances in Cryptology-CRYPTO 2006. Berlin, Heidelberg: Springer-Verlag, 2006. 290−307. [doi: 10.1007/11818175_17]

[54] Horwitz J, Lynn B. Toward hierarchical identity-based encryption. In: Proc. of the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2002. 466−481.

[55] Yao DF, Fazio N, Dodis Y, Lysyanskaya A. Id-Based encryption for complex hierarchies with applications to forward security and broadcast encryption. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 354−363. [doi: 10.1145/1030083.1030130]

[56] Attrapadung N, Imai H. Dual-Policy attribute based encryption. In: Abdalla M, Pointcheval D, Fouque P A, Vergnaud D, eds. Proc. of the Applied Cryptography and Network Security. Berlin, Heidelberg: Springer-Verlag, 2009. 168−185. [doi: 10.1007/978-3-642-01957-9_11]

附中文参考文献:

[16] 梁晓辉.基于属性的密码系统研究[硕士学位论文].上海:上海交通大学,2009.

苏金树(1962－),男,福建莆田人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络,信息安全.

曹丹(1983－),女,博士生,主要研究领域为网络安全.

王小峰(1982－),男,博士,助理研究员,主要研究领域为网络安全,信息确保和分布式智能计算.

孙一品(1981－),男,博士,助理研究员,主要研究领域为信息安全,隐私保护技术.

胡乔林(1979－),男,博士生,主要研究领域为网络可生存性,虚拟网络.