计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180085
55(7):1409-1420,2018

一种适用于广电网的属性基广播加密方案

李学俊[1] 袁亚文[1] 金春花[2]
[1](西安电子科技大学网络与信息安全学院 西安 710071)
[2](江苏省物联网移动互联技术工程实验室(淮阴工学院) 江苏淮安 223001)
(aluckydd@mail.xidian.edu.en)

An Attribute-Based Broadcast Encryption Scheme Suitable for the Broadcasting Network

Li Xuejun[1], Yuan Yawen[1], and Jin Chunhua[2]
[1](*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071)
[2](*The Laboratory for Internet of Things and Mobile Internet Technology of Jiangsu Province* (*Huaiyin University of Technology*), *Huai'an Jiangsu* 223001)

Abstract In the transitional period, broadcasting network will cooperate with 'cloud channel device' to implement a unified layout and a service cloud platform. However, the opening cloud made the information security protection be hard in the broadcasting network. Attribute-based broadcast encryption technology combines the advantages of broadcast encryption and the attribute-based encryption technologies. It can securely transmit messages to multiple users and achieve flexible ciphertext access control. It is applicable to the broadcasting network which has multi-user and multi-service. However, most of the attribute-based broadcast encryption schemes up to now are not efficient enough and have many shortcomings, such as the long length of ciphertext, the big number of user private keys, the complicated calculation of encryption and decryption, and without weighted-attributes considering. In order to overcome the flaws of the attribute-based broadcast encryption schemes, the contribution of this paper is an efficient attribute-based broadcast encryption scheme for broadcasting network environment. This scheme is based on a classical broadcast encryption scheme, and the sender can choose the receiver set freely, achieving efficient user revocation. Adopt a dynamic weighted threshold access structure and introduce a wildcard mechanism which fixes the length of the broadcast ciphertext and enhance the flexibility of the ciphertext access control. The weighted attributes make the scheme more in line with the actual application environment. We incorporate a mediated attribute-based encryption to achieve outsourced storage and outsourced decryption. By this technology, we can effectively reduce the storage of private keys and computational overhead. Finally, through the security analysis and experimental simulation, we prove our scheme achieves choose plaintext attack (CPA) security safety, and has high efficiency.

收稿日期:2018-02-01;**修回日期**:2018-05-03
基金项目:国家自然科学基金项目(61572460);国家重点研发计划项目(2016YFB0800703);江苏省物联网移动互联技术工程实验室资助项目(JSWLW-2017-011)
This work was supported by the National Natural Science Foundation of China (61572460), the National Key Research and Development Program of China (2016YFB0800703), and the Funding Project of Jiangsu Provincial Internet of Things Mobile Interconnection Technical Laboratory (JSWLW-2017-011).
通信作者:袁亚文(1498072980@qq.com)

Key words broadcasting network; attribute-based broadcast encryption; weighted-attributes; fixed-length ciphertext; low computational overhead; low outsourced decryption; choose plaintext attack (CPA) security

摘 要 广电网在战略转型阶段中,协同"云管端"统一布局,规划服务云平台.但是,云的开放使广电网中信息安全无法得到保证.属性基广播加密技术融合了广播加密和属性基加密技术的优点,可将消息安全传送给多个用户的同时实现灵活的密文访问控制,适用于多用户、多服务的广电网.然而,目前属性基广播加密技术中仍存在一些缺陷,如广播密文长度过大、用户私钥数量过多、加解密计算复杂、访问策略不够灵活以及未考虑属性权重等.针对以上不足,提出一种适用于广电网的属性基广播加密方案.方案基于经典的广播加密方案,发送方可自由选择接收用户集,实现了高效的用户撤销;采用权重门限访问结构并引入通配符机制,实现了广播密文长度固定的同时增强了密文访问结构灵活性,权重思想也使方案更符合现实应用场景;引入一种基于中间人的属性基加密技术,同时实现了外包存储和外包解密,有效地降低了私钥存储和计算开销.最后通过安全性分析和实验仿真证明:该方案达到选择明文安全并具有较高效率.

关键词 广电网;属性基广播加密;权重属性;长度固定密文;计算开销小;存储开销小;选择明文安全

中图法分类号 TP391

1 相关工作

1.1 研究背景

随着物联网和云计算技术的高速发展[1],广播电视网(广电网)开始向云端转移,以新智慧、新体验为主题,进入智能化信息服务云平台战略转型阶段."云管端"协同下,广电提供商借助"云"将互联网信息接入应用平台,从而为用户提供数字电视、远程教育、政府信息发布、社区智能服务和游戏娱乐等多样化信息服务[2].例如数字电视节目服务中,抛弃传统的大面积整体推送,将用户按照订阅喜好和消费习惯分类划分,不同用户可享受专属电视节目单.云端融合后,广电网不再封闭,不法分子趁机活跃,经常私自篡改广播信息、利用网络获取智能服务等.如第26届中国国际广播电视信息网络展览会中提到的"2017年网络视频盗版侵权导致潜在广告展示和版权付费的统计损失超过200亿元".广电网作为社会信息主要传播渠道,需要密码技术保障广播内容的传输安全[3].

传统的广电网主要依靠对称密码技术,需通信双方协商对称密钥,不符合实际应用.公钥加密技术由于大大节省了密钥空间成为密码界的主流技术,公钥广播加密作为其中一种,可实现高效地一对多信息共享,并保证只有被选中的用户才可成功解密,保证了信息安全并减小了通信开销,被广泛应用于广电网.但是,随着用户的增多,广播加密由于无法灵活控制用户陷入了发展瓶颈.为提高广播效率,属性基广播加密技术被提出,将用户按照属性划分,设计灵活的密文访问结构从而高效控制用户接入,加速了广播加密技术在广电网的发展.

广电网转型后具有很多特性,广电服务商需要制作符合不同用户的个性化服务密文,随着用户数量增多,这种个性化服务大大增加了广播流量.而且用户的动态性较强,用户可能没有及时缴费被撤销服务权限,续费后又被恢复权限.此外广电网中服务一般都带有权重色彩,会根据不同的缴费状况设置不同等级服务,因此会出现不同权重值的同种属性.最后终端用户存储资源和计算资源有限,无法存储过长的私钥、进行复杂的解密运算.因此,广电网需要寻找更合适的广播加密技术.

1.2 国内外研究现状

1991年,Berkovits[4]首次提出广播加密技术(broadcast encryption, BE)的概念.1993年,Fiat等人[5]首次给出了广播加密技术的形式化定义.随着应用环境的改变,密码学界开始研究不同性能的BE技术.2001年Naor等人[6]提出了一种BE方案,引入公钥从而节省了密钥空间提高了效率.方案使用门限秘密共享机制,具有叛逆者追踪功能,但不抗共谋攻击.2005年Du等人[7]在身份基加密技术基础上提出一种身份基广播加密方案.方案利用用户身份生成公钥,接收用户必须满足身份要求才能解密,但是密文长度随接收用户数目线性增长.同年,Boneh等人[8]提出一个基于双线性映射的BE方案

(BGW 方案),BGW 方案中用户私钥为一个群元素并且抗共谋攻击,实现了学者们一直苦苦寻求的目标.从此开启了基于双线性映射的 BE 技术的研究.

2005 年,Sahai 等人[9]提出了属性基加密思想(attribute-based encryption, ABE),引入了属性的概念.2006 年 Goyal 等人[10]根据用户私钥、访问结构和系统属性之间的关系,将 ABE 技术分为基于密钥策略和基于密文策略 2 类:基于密钥策略的属性基加密技术(key policy ABE, KP-ABE)中用户私钥关联访问结构;基于密文策略的属性基加密技术(ciphertext policy ABE, CP-ABE)中密文关联访问结构.相比于 KP-ABE,CP-ABE 中信息发送方加密时可以根据需要自由选定访问结构,更适合现在应用环境,因此本文重点研究 CP-ABE. 2010 年 Emura 等人[11]构造了第 1 个固定密文长度 ABE 方案,方案中每个属性拥有正、负 2 种取值.2011 年 Chen 等人[12]提出一种固定密文长度 ABE 方案,方案在每个属性取正、负属性值的基础上加入了通配符机制,增加了方案灵活性并且计算简单.后来,基于文献[12]方案的思想,固定密文长度的 ABE 方案[13]被提出.为提高效率,ABE 外包技术被提出,通过将复杂的解密运算委托给云服务器来减轻用户计算负担.2009 年 Ibraimi 等人[14]提出了一种基于中间人的属性基加密方案(Ibraimi 方案),解决了用户的存储和解密负担过重的问题.由于大部分 ABE 方案都没有考虑权重的概念,事实上考虑权重概念很有意义.2013 年 Liu 等人[15]基于树形结构,构造了权重 ABE 方案,但方案加解密需要消耗大量的计算资源.2017 年 Wang 等人[16]根据属性的重要性不同,为属性分配不同的权重.

2008 年 Lubicz 等人[17]将属性基加密技术首次应用于广播加密技术中,创造性地提出一种属性基广播加密技术(attribute based broadcast encryption, ABBE).相比传统的 BE 技术,该方案加解密过程更加快捷,并且可实现用户灵活的访问控制.2010 年 Zhou 等人[18]提出了一个高性能的 ABBE 方案,但方案的解密计算开销过大,访问结构的实现上也不够灵活.上述方案存在一个共同问题,即不能实现无需私钥更新的细粒度的用户级撤销.因此可以说 ABBE 和 ABE 的主要区别就是 ABBE 可以允许细粒度的用户级别撤销,发送方可以直接控制单独的用户,而且无用户撤销时可以直接利用属性控制全部用户,实现与 ABE 同样的功能[23].2009 年 Attrapadung 等人[19]借助 BGW 方案提出 2 种 ABBE 方案.2 种方案均可以不更新用户私钥完成细粒度的用户级撤销.但方案的密文和用户私钥长度都与访问结构中属性个数线性相关,带来较大的通信和存储开销.2010 年 Karlov 等人[20]提出一种访问策略灵活的 ABBE 方案,方案同样基于 BGW 方案,采用布尔函数中合取范式和析取范式访问结构,支持任意访问策略,但方案密文长度仍会随访问结构而变化,并且为了实现用户级撤销,方案增加了代表身份的特殊属性,增加了访问结构的管理难度.2016 年 Zhou 等人[21]将文献[18]方案改进后提出一种可隐私保护的 ABBE 方案.方案实现密文长度固定并可隐藏访问结构,达到隐私保护目的.但方案解密计算开销随系统属性数目线性变化.属性数目较大时,方案解密效率变得极低.同年胡思路等人[22]提出一种高效的 ABBE 方案,方案密文长度固定,但用户私钥长度随用户属性数目的增加迅速增大,不适用于物联网环境.2015 年 Yang 等人[23]提出一种密文长度固定的 ABBE 方案,但用户私钥长度随访问结构中通配符数目变化,并且需要频繁更新.

1.3 本文主要工作

针对现有 ABBE 方案中广播密文长度过大、用户私钥数量过多、加解密计算复杂以及没有考虑权重概念等缺陷,构造了一个高效的权重属性基广播加密方案.方案基于经典的 BGW 方案,在撤销用户时无需更新用户私钥组件,提高了撤销效率;采用权重门限访问结构并引入通配符机制,实现了广播密文长度的固定,发送方并且可以自由选取访问结构中属性个数和动态调整权重门限值,另外方案的权重思想也具有现实意义,按照属性的重要程度划分权重取值,符合具有分等级服务的广电物联网环境;然后方案引入 Ibraimi 等人[14]的基于中间人的思想,将用户大部分私钥存储和解密计算工作委托给中间人代理完成,用户仅需本地存储一个群元素长度的私钥,解密时只需一次双线性对计算,高效地降低了用户私钥存储负担和解密时的计算负担.

2 预备知识

2.1 “云管端”基础架构

“云管端”协同布局[2]促进“广电网+物联网”战略转型.“云”是计算机服务器组成的云环境,提供数据的存储与分享,但不保证数据的安全性;“管”是远距离数据传输管理协议;“端”是物联网终端设备,计算能力有限;如图 1 所示:

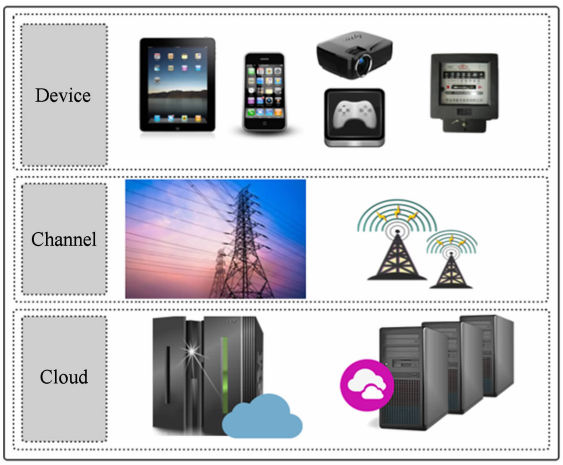

Fig. 1 The infrastructure of "Cloud, Channel, Device"

图 1 "云管端"基础架构

2.2 双线性映射

定义 1. 假设 G 和 G_T 均为大素数阶 P 的乘法循环群. 若存在映射 $e:G\times G\rightarrow G_T$ 满足 3 个性质,我们则称 e 为双线性映射:

1) 双线性性. $\forall u,v\in G$ 以及 $\forall a,b\in\mathbb{Z}_P$, $e(u^a,v^b)=e(u,v)^{ab}$ 永远成立.

2) 非退化性. $\exists g\in G$ 使得 $e(g,g)\neq 1$,其中 1 为群 G_T 的单位元.

3) 可计算性. 对 $\forall u,v\in G$,都能有效计算出 $e(u,v)$的值.

若上述双线性映射 $e:G\times G\rightarrow G_T$ 存在,则称群 G 为双线性群.

若 $e(u^a,v^b)=e(u,v)^{ab}=e(u^b,v^a)$,则称双线性映射 e 为对称的,否则称 e 为非对称的.

2.3 访问结构

定义 2. 集合 $S=\{P_1,P_2,\cdots,P_n\}$拥有 n 个参与实体,访问结构 W 是集合 $P=2^{\{P_1,P_2,\cdots,P_n\}}$ 中的一个非空子集. 假设 W 是单调的,对于 $\forall B,C$ 如果 $B\subseteq W$ 且 $B\subseteq C$,那么 $C\subseteq W$ 都成立. W 中包含的集合则可称为授权集合,非授权集合则为不属于 W 中的集合. 在属性基加密技术中,属性集合就为实体集合.

(n,t)门限访问结构较为简单,但是在实现密文长度固定方面有很好的应用. 可以描述为:将一份秘密 s 分为 n 个部分,选定门限 t,使得只有不少于 t 个部分相互协作才能恢复出秘密 s,而少于 t 个部分协作则无法得到秘密.

定义 3. 权重门限访问结构(weighted threshold access structure with wildcard, W-(n,t)). 系统属性集合 $U=\{A_1,A_2,\cdots,A_n\}$,其中 $|U|=n$,用户属性集合为 $S_u\subseteq U$,权重函数 $weight:A\rightarrow\mathbb{Z}_P$. 选定一个门限值 t 的权重门限访问结构 W-(n,t)对信息进行加密,其加密属性集合 $\Omega\subseteq U$ 中每个属性 $A_i\in\Omega$ 的权重值为 $weight(A_i)$. 若解密用户属性集合 S_u 中必须包含不少于 t 个加密属性,即 $|S_u\cap\Omega|\geqslant t$,并且 S_u 中每个属性 $A_i\in S_u\cap\Omega$ 的权重值不小于其对应的 $weight(A_i)$,用户才能正确解密. 则称可正确解密的用户属性集合满足权重门限访问结构,记为 $S_u\models W$-(n,t);否则称用户属性集合不满足权重门限访问结构,记为 $S_u\not\models W$-(n,t),拥有该集合的用户无法完成解密.

2.4 困难假设

判定性 m-BDHE 问题(decisional m-bilinear Diffie-Hellman exponent, m-BDHE). 给定一个阶为素数 P 的群 G,元素 $g\in G$ 为群 G 中的一个生成元. 随机选定 2 个元素 $\alpha,s\in\mathbb{Z}_p$和一个随机元素 $T\in G_T$. 判定性 m-BDHE 问题描述为给定参数 y:

$$\boldsymbol{y}=(g,g^s,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^m},g^{\alpha^{m+2}},\cdots,g^{\alpha^{2m}}).$$

判断 T 为 $e(g,g)^{\alpha^{m+1}s}$还是为群 G_T 中的一个随机元素 $\Re$. 攻破上述假设的优势为

$$|Pr[\mathcal{B}(\boldsymbol{y},T=e(g,g)^{\alpha^{m+1}})=0]-Pr[\mathcal{B}(\boldsymbol{y},T=\Re)=0]|.$$

定义 4. 如果不存在 PPT 算法可以以不可忽略的优势解决判定性 m-BDHE 问题,则称 m-BDHE 问题是困难的.

3 方案定义

3.1 方案形式化定义

基于中间人的属性基广播加密方案(mediated ABBE, M-ABBE)形式化定义如下:

1) 系统初始化

Setup$(1^{\lambda})\rightarrow(PK,msk)$:输入系统安全参数 1^{λ},输出系统公共参数 PK 和系统主密钥 msk.

2) 私钥提取

KeyGen$(GID,L_{GID},PK,msk)\rightarrow\{SK_{GID,1},SK_{GID,2}\}$:输入用户的身份信息 GID、用户属性集合 L_{GID}、系统公共参数 PK 和系统主密钥 msk,输出 2 部分私钥为 $SK_{GID,1}$和 $SK_{GID,2}$.

3) 广播加密

Encrypt$(\ell,\mathcal{M},PK,W)\rightarrow CT$:输入目标接收用户集合 $\ell\in S$、明文 $\mathcal{M}$、系统公共参数 PK 和访问结构 W,最后算法输出密文 CT.

4) 代理解密

Transform$(CT,GID,SK_{GID,1},PK)\rightarrow CT_{\mathrm{OUT}}/$

⊥:输入密文 CT、用户的身份信息 GID、用户的第 1 部分私钥 $SK_{GID,1}$ 和系统公共参数 PK. 中间人首先检验用户权限. 若用户属于目标接收集合 $GID\in\ell$ 并且用户属性集合 L_{GID} 满足访问结构 W,中间人则可以成功完成代理解密的工作,算法输出外包解密密文 CT_{OUT}. 否则,算法终止并输出错误⊥.

5) 用户解密

Decrypt(CT_{OUT},$SK_{GID,2}$)→$\mathcal{M}$:用户输入外包解密密文 CT_{OUT}、第 2 部分私钥 $SK_{GID,2}$. 若 CT_{OUT} 正确则算法输出明文 $\mathcal{M}$,否则用户无法完成最终解密.

3.2 安全模型

M-ABBE 中存在 2 种情况的攻击敌手:1)敌手 $\mathcal{A}$ 没有第 1 部分私钥 $SK_{i,1}$,但可以获取外包解密密文 CT_{OUT};2)敌手 $\mathcal{A}$ 没有第 2 部分私钥 $SK_{i,2}$,但可以得到最终解密后的明文 $\mathcal{M}$. 由于 $u_{\varphi 1}$ 和 $u_{\varphi 2}$ 两个元素是随机选取的,所以情况 2 类型的敌手没有办法在不知道 $SK_{i,2}$ 的情况下成功进行最终解密. 本文主要针对其中的情况 1 类型的敌手进行分析.

M-ABBE 方案的选择明文攻击安全(chosen plaintext attack, CPA)是通过敌手 $\mathcal{A}$ 和挑战者 C 之间的一个互动游戏来定义,这里另外定义一个模拟算法 $\mathcal{B}$ 帮助完成敌手 $\mathcal{A}$ 和挑战者 C 之间的互动. 假定游戏中 $\mathcal{A}$ 可以自适应询问私钥,为记录被询问的密钥,在游戏开始之前首先为模拟算法 $\mathcal{B}$ 建 2 个空白的列表:$List1=(F_i, SK_{i,1})$, $List2=(F_i, SK_{i,2})$. 游戏定义如下:

初始化. 挑战者 C 接受挑战,敌手 $\mathcal{A}$ 确定系统属性数目 n 并选择一个目标接收用户集合 ℓ^* 和一个访问结构 W^*. 然后敌手 $\mathcal{A}$ 将(ℓ^*,W^*)全部提交给模拟算法 $\mathcal{B}$,然后 $\mathcal{B}$ 将其传送给挑战者 C.

建立. 挑战者 C 选一个安全参数 1^λ,然后运行系统初始化算法生成系统公共参数 PK 和系统主密钥 msk,并将系统公共参数 PK 传送给模拟算法 $\mathcal{B}$,然后模拟算法 $\mathcal{B}$ 将系统公共参数 PK 返回给敌手 $\mathcal{A}$.

阶段 1. 敌手 $\mathcal{A}$ 进行以下私钥询问,然后敌手 $\mathcal{A}$ 选择一个不满足之前所提交的解密条件(ℓ^*,W^*)的用户 i 进行用户私钥询问.

当敌手 $\mathcal{A}$ 询问用户 i 的第 1 部分私钥 $SK_{i,1}$ 时,模拟算法 $\mathcal{B}$ 先检查列表 $List1$. 当列表中无该项记录,模拟算法 $\mathcal{B}$ 将会询问挑战者 C 关于用户 i 的私钥组件. 挑战者 C 接受询问运行私钥提取算法计算相应的私钥组件后交给模拟算法 $\mathcal{B}$. 模拟算法 $\mathcal{B}$ 得到挑战者 C 返还的私钥组件后得出 $SK_{i,1}$ 返回给敌手 $\mathcal{A}$. 并且模拟算法 $\mathcal{B}$ 同时得到 $SK_{i,2}$,然后 $\mathcal{B}$ 将记录(F_i,$SK_{i,1}$)记录到 $List1$ 列表中,并且将记录(F_i,$SK_{i,2}$)记录到 $List2$ 列表中;否则,模拟算法 $\mathcal{B}$ 可以直接从列表中索引到记录(F_i,$SK_{i,1}$),并将结果发送给敌手 $\mathcal{A}$.

挑战. 敌手 $\mathcal{A}$ 随机选取 2 条长度相同的明文消息 $\mathcal{M}_0$,$\mathcal{M}_1$ 并提交给模拟算法 $\mathcal{B}$,然后模拟算法 $\mathcal{B}$ 将其发送给挑战者 C. 最后由挑战者 C 随机选择$b\in\{0,1\}$,运行加密算法加密消息 $\mathcal{M}_b$ 并得到相应的密文 CT^* 并交给模拟算法 $\mathcal{B}$ 返回给敌手 $\mathcal{A}$.

阶段 2. 重复阶段 1.

猜想. 最终敌手 $\mathcal{A}$ 猜测 $b^*\in\{0,1\}$,如果猜测正确,模拟算法 $\mathcal{B}$ 输出 0,则称敌手 $\mathcal{A}$ 在该游戏中获胜. 走完上述流程后,定义敌手 $\mathcal{A}$ 的获胜优势为

$$Adv_A=Pr[b^*=b]-1/2.$$

定义 5. 如果对于任意 PPT 的敌手 $\mathcal{A}$ 赢得上述游戏的优势可以忽略,则称 M-ABBE 方案是 CPA 安全的.

4 方案描述

4.1 系统框架

如图 2 所示,本方案共 5 个实体,分别为权威机构(trusted authority, TA)、广播中心(broadcast center, BC)、云存储服务器(cloud storage, CS)、中间人(mediator, Mr)、接收用户(data receiver, DR). 它们的具体职责为:

1) TA. 负责管理系统属性集合,生成系统公共参数,为用户生成并分发私钥,TA 完全可信.

2) BC. 控制数据的分享. BC 可自由选择消息的目标接收用户集合,并制定灵活的访问结构,加密消息后将密文上传,供用户访问.

3) CS. 负责存储 BC 上传的密文信息. CS 不可信,并试图窥探密文所包含的隐私数据.

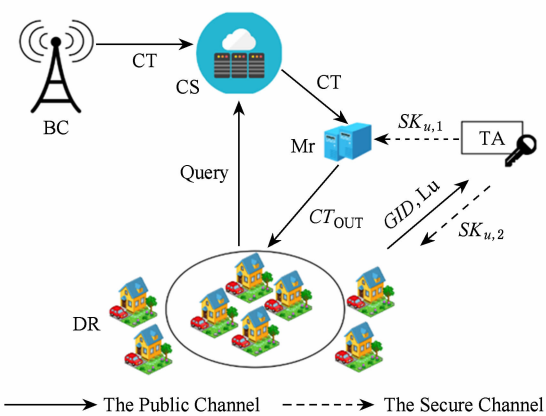

Fig. 2 The system structure

图 2 系统框架图

4) Mr. 是一个不可信任的云服务器. 负责存储用户的部分私钥,并在解密阶段代理解密,承担用户大部分计算量. 当 CS 将密文发送 Mr 后,Mr 首先查看用户身份是否合法,然后利用用户的部分私钥进行代理解密,生成外包解密密文并发送给用户.

5) DR. 负责最终解密工作. 当且仅当 DR 属于目标接收用户集合并且其属性列表满足密文访问结构才能成功完成解密工作. DR 存储空间匮乏.

4.2 方案概述

属性权重分割集 $U=\{A_1,A_2,\cdots,A_n\}$ 为系统属性集合,其中每个属性拥有一系列属性权重取值 $(A_i,weight(A_i))$,其中 A_i 在系统中所允许的最大权重取值为 $\omega_i=weight(A_i)_{\max}$,注意权重值 $weight(A_i)$ 只取整数. 将 U 中的每个属性 A_i,以权重最小份额 1 进行分割,分割后属性 A_i 对应于 $(A_i,1),(A_i,2),\cdots,(A_i,\omega_i)$,其构成的集合称为属性权重的分割集 $U^{\omega}=\{(A_1,1),(A_1,2),\cdots,(A_1,\omega_1),\cdots,(A_n,1),(A_n,2),\cdots,(A_n,\omega_n)\}$. 例如属性"教师"可以具体划分为"讲师、副教授、教授"因此可以按照权重等级定义为该属性为"(教师,1)(教师,2)(教师,3)". 除了

$$\begin{cases}\{A_1^*,A_2^*,\cdots,A_n^*\}\\(A_1,1),(A_1,2),\cdots,(A_1,\omega_1)\\(A_2,1),(A_2,2),\cdots,(A_2,\omega_2)\\\vdots\\(A_n,1),(A_n,2),\cdots,(A_n,\omega_n)\end{cases}\rightarrow\begin{cases}1,2,\cdots,n\\(n+1),(2n+1),\cdots,(\omega_1 n+1)\\(n+2),(2n+2),\cdots,(\omega_2 n+2).\\\vdots\\(n+n),(2n+n),\cdots,(\omega_n n+n)\end{cases}$$

公开 $PK=(g,g_1,\cdots,g_m,g_{m+2},\cdots,g_{2m},\{T_k\}_{k=1,2,\cdots,N},\nu,R)$ 并保留主密钥 $msk=(\alpha,\xi,r,\{\beta_k\}_{k=1,2,\cdots,N})$.

2) 私钥提取阶段

KeyGen$(i,S_i,U^*,PK,msk)\rightarrow\{SK_{i,1},SK_{i,2}\}$: 输入用户的身份 i、用户权重属性集合 S_i、系统公共参数 PK 和系统主密钥 msk. TA 随机选取 $n+1$ 个元素 $\delta,\delta_1,\cdots,\delta_n\in\mathbb{Z}_p$,使得 $\delta=\sum_{k=1}^{n}\delta_k$. 接着,TA 随机选择 $x\in\mathbb{Z}_p$ 和 2 个元素 $u_{\psi 1}$ 和 $u_{\psi 2}$,使得 $u_{\psi 1}-u_{\psi 2}=1$. 然后根据 U^* 和 S_i,TA 计算 $SK_{i,1}$ 和 $SK_{i,2}$ 两部分私钥,其中 TA 计算 $SK_{i,1}$ 私钥组件为

$$\begin{cases}D_1=(g^{\alpha^i}\xi g^{(\delta-r)x})^{u_{\psi 1}}\\D_2=g^{u_{\psi 1}x}\\D_{3,j}=g^{\alpha^j u_{\psi 1}}\\f_k=(g^{\delta_k}T_k)^{u_{\psi 1}x}\\\omega_{i,k}=\begin{cases}\omega_k=(g^{\delta_{k'}}T_k)^{u_{\psi 1}x}\\\omega_q'=(T_q/T_k)^{u_{\psi 1}x},\ \forall q\in[1,k)\end{cases}\end{cases}$$

其中,f_k 代表 U^* 对应的私钥组件,ω_k 代表 S_i 对属性权重取值之外,每个属性还具有一个通配符取值 A_i^*,代表该属性无关紧要. 其构成的集合称为系统通配符集合 $U^*=\{A_1^*,A_2^*,\cdots,A_n^*\}$. 用户权重属性集合 S_i,其中每个属性都有一个权重值 $(A_i,weight(A_i))\in S_i$.

1) 系统初始化

Setup$(1^{\lambda})\rightarrow(PK,msk)$: 输入安全参数 1^{λ}. TA 首先确定用户的最大数目 m 和系统属性数量 n,并选择 2 个阶为素数 P 的乘法循环群 G 和 G_T,$g\in G$ 为群 G 的一个生成元,并选择双线性映射 $e:G\times G\rightarrow G_T$. 然后 TA 随机选取一个元素 $\alpha\in\mathbb{Z}_P$,对于用户 $i=1,2,\cdots,m$(为方便,这里用索引 i 代表用户),计算 $g_i=g^{\alpha^i}\in G$ 代表用户 i 的身份公共参数,并计算 $\{g_i=g^{\alpha^i}\}_{i=m+2,m+3,\cdots,2m}\in G$ 作为系统默认公共参数. 接着 TA 随机选取 2 个元素 $\xi,r\in\mathbb{Z}_P$,并计算 $v=g^{\xi}$,$R=g^r\in G$. 根据属性权重的分割集 U^{ω} 和通配符集合 U^*,TA 随机选择 N 个元素 $\{\beta_k\}_{k=1,2,\cdots,N}\in\mathbb{Z}_P$,其中 $N=|U^{\omega}|+|U^*|$,并计算 $\{T_k=g^{\beta_k}\}_{k=1,2,\cdots,N}\in G$. 注意:这里 $N\leqslant m$,并将系统属性集合中每个属性值对应一个索引 k,对应方式为

$$\begin{cases}\{A_1^*,A_2^*,\cdots,A_n^*\}\\(A_1,1),(A_1,2),\cdots,(A_1,\omega_1)\\(A_2,1),(A_2,2),\cdots,(A_2,\omega_2)\\\vdots\\(A_n,1),(A_n,2),\cdots,(A_n,\omega_n)\end{cases}\rightarrow\begin{cases}1,2,\cdots,n\\(n+1),(2n+1),\cdots,(\omega_1 n+1)\\(n+2),(2n+2),\cdots,(\omega_2 n+2).\\\vdots\\(n+n),(2n+n),\cdots,(\omega_n n+n)\end{cases}$$

应的私钥组件,其中 $k'=k-weight(A_k)\times n$,$weight(A_k)$ 代表 i 的 A_k 属性的权重值. 用户第 1 部分私钥为 $SK_{i,1}=(D_1,D_2,\{D_{3,j}\}_{j=1,2,\cdots,2m\backslash\{m+1\}},\{f_k\}_{k\in U^*},\{\omega_{i,k}\}_{k\in S_i})$.

TA 将 $SK_{i,1}$ 秘密发送给中间人进行存储. 接着 TA 计算 $D'=g^{\alpha^{m+1}u_{\psi 2}}$,并将 $SK_{i,2}=(D')$ 秘密发送给用户进行存储.

3) 数据加密阶段

Encrypt$(\ell,\mathcal{M},PK,W)\rightarrow CT$: 输入目标接收用户集合 ℓ(由 BC 提前确定好)、明文 $\mathcal{M}$、系统公共参数 PK,BC 先选择自己所不关心的通配符属性 A^*,去除之后选择一个权重门限访问结构 W-$(n-|A^*|,t)$(为表达简单这里简称 W). 接着 BC 选择一个随机秘密值 s,然后计算出会话密钥 $K=e(g_m,g_1)^s$. 然后计算广播密文头部 Hdr:

$$Hdr=\begin{cases}C_1=g^s,\\C_2=\left(\nu\prod_{j\in\ell}g_{m+1-j}\right)^s,\\C_3=\left(R\prod_{k\in W}T_k\right)^s.\end{cases}$$

BC 用 K 对称加密 $\mathcal{M}$ 得到 $CTM=\mathcal{M}(g_m,g_1)^s$,最后 BC 输出密文 $CT=(CTM,Hdr)$.

4) 代理解密

$Transform(CT,i,SK_{i,1},PK)\rightarrow CT_{\mathrm{OUT}}/\perp$:输入 CT、用户身份 i、第 1 部分私钥 $SK_{i,1}$ 和系统公共参数 PK. 中间人首先检验用户权限. 若 i 是合法用户 $i\in\ell$,并且 S_i 满足权重门限访问结构 $S_i\models W$,Mr 则可以完成代理解密工作. 否则,算法终止并输出错误. 注意这里 $S_i\models W$ 分为 2 种情况:

① i 属性集合的权重取值和访问结构中属性权重取值相同,也就是 $(A_k,weight(A_k))\in S_i$ 且 $weight(A_k)_{S_i}=weight(A_k)_{W\text{-}(n,t)}$;

② i 权重属性集合中属性权重取值大于访问结构中属性权重取值,即某个属性权重取值较大,i 权限较高 $weight(A_k)_{S_i}>weight(A_k)_{W\text{-}(n,t)}$. Mr 代理解密计算过程如下:

Mr 计算 $P=\prod_{j\in\ell,j\neq i}D_{3,m+1-j+i}$,然后选择满足 W 的属性和通配符,

情况 1. Mr 计算:

$$Q=\Big(\prod_{k\models W}f_k\prod_{\omega_{i,k}\in S_i,\omega_{i,k}\models W}\omega_k\Big).$$

情况 2. Mr 计算:

$$Q=\Big(\prod_{k\models W}f_k\prod_{\omega_{i,k}\in S_i,\omega_{i,k}\models W}\omega_k\omega'_q\Big).$$

然后计算:

$$\begin{cases}K_1=e(D_1P,C_1)e(D_2,C_3),\\ K_2=e(D_{3,i},C_2)e(Q,C_1).\end{cases}$$

最后计算 $CT_{\mathrm{OUT}}=CTM(K_1/K_2)$,得出 CT_{OUT} 后发送给 i.

5) 用户解密

$\mathrm{Decrypt}(CT_{\mathrm{OUT}},SK_{i,2})\rightarrow\mathcal{M}$:DR(用户 i)收到 CT_{OUT}后,输入第 2 部分私钥 $SK_{i,2}$,DR 最终完成解密工作恢复出明文:

$$\mathcal{M}=CT_{\mathrm{OUT}}e(C_1,SK_{i,2}).$$

5 方案分析

5.1 选择明文安全性

定理 1. 假定判断性 m-BDHE 假设是困难的,则没有 PPT 的敌手能以选择明文方式攻破 M-ABBE 方案.

证明. 假设一个 PPT 的敌手 $\mathcal{A}$ 赢得 M-ABBE 方案模型游戏的优势 $\varepsilon=Adv_A$ 是不可忽略的,那么挑战者 C 就可以定义一个 PPT 的模拟算法 $\mathcal{B}$,能够以不可忽略优势 $\varepsilon/2$ 解决 m-BDHE 问题. 模拟过程如下:

初始化. 挑战者 C 接受一个判断性 m-BDHE 困难问题挑战 $(g,\boldsymbol{y}_{g,\alpha,m}=(g_1,g_2,\cdots,g_m,g_{m+2},\cdots,g_{2m}),T)$,其中 $g_i=g^{\alpha^i}\in G$,并且 $\alpha\in\mathbb{Z}_P$ 是未知的. 挑战者 C 运行一个模拟算法 $\mathcal{B}$,敌手 $\mathcal{A}$ 选择系统属性数目 n,$\mathcal{B}$ 设置系统属性集合为 $U=\{A_1,A_2,\cdots,A_n\}$,并进行权重分割得到属性权重分割集 U^ω,另外,除了属性权重取值之外,每个属性还具有一个通配符取值 A_i^*,代表该属性无关紧要. 其构成的集合称为系统通配符集合 $U^*=\{A_1^*,A_2^*,\cdots,A_n^*\}$. 当用户 i 加入系统时,根据用户 i 所具有的属性为其分配权重属性集合 $S_i\subseteq U^\omega$. 然后 A 选定目标接收者集合 ℓ^* 和通配符机制的权重门限访问结构 W^*,并将 (ℓ^*,W^*) 提交给挑战者 C.

建立. C 首先选择一个安全参数 1^λ,运行系统初始化算法生成系统公共参数 PK 以及主密钥 msk,并将 PK 传送给 $\mathcal{B}$ 交给敌手 $\mathcal{A}$. 具体为 C 选择随机数 $d,r_0,\delta_1,\delta_2,\cdots,\delta_n\in\mathbb{Z}_P$ 并计算:

$$v=g^d\Big(\prod_{j\in\ell^*}g_{m+1-j}^{-1}\Big)=g^{d-\sum_{j\in\ell^*}\alpha^{m+i-j}}=g^{\xi},$$

$$R=g^{r_0}\prod_{k\in W^*}g^{\alpha^{m+1-k}}=g^{r_0+\sum_{k\in W^*}\alpha^{m+1-k}}=g^r.$$

接着 C 根据 U^ω 和 U^*,随机选择 $N=|U^\omega|+|U^*|$ 个元素 $u_1,u_2,\cdots,u_N\in\mathbb{Z}_p$,计算 $\{T_k=g^{u_k-\alpha^{m+1-k}}\}_{k=1,2,\cdots,N}$,最后 C 得出系统公共参数 PK 并传送给模拟算法 $\mathcal{B}$,其中 $PK=(g,g_1,\cdots,g_m,g_{m+2},\cdots,g_{2m},\{T_k\}_{k=1,2,\cdots,N},\nu,R)$.

阶段 1. $\mathcal{A}$ 选择一个不满足解密条件的用户 i 进行私钥询问(注意:此用户 i 有 2 种,i 不是目标用户 $i\notin\ell^*$ 或者 S_i 不满足访问结构 $S_i\not\models W^*$). $\mathcal{A}$ 能够进行有限次数的以下询问,当询问 i 的第 1 部分私钥 $SK_{i,1}$ 时,$\mathcal{B}$ 检查列表 $List1$,若列表中无该项记录,$\mathcal{B}$ 将会询问挑战者 C 关于 i 的私钥组件. 挑战者 C 接受询问运行私钥提取算法计算相应的私钥组件后交给模拟算法 $\mathcal{B}$. 模拟算法 $\mathcal{B}$ 得到挑战者 C 返还的私钥组件后得出 $SK_{i,1}$ 返回给 $\mathcal{A}$. 然后 $\mathcal{B}$ 将 $(F_i,SK_{i,1})$ 记录到 $List1$ 中. 否则,模拟算法 $\mathcal{B}$ 可以直接从列表中索引到记录并发送给 $\mathcal{A}$. 以上游戏交互具体为,$\mathcal{B}$ 首先选择选取元素 δ,x,并使得 $\delta=\sum_{i=1}^{n}\delta_i$,然后随机选择 2 个元素 $u_{\varphi1}$ 和 $u_{\varphi2}$ 使得 $u_{\varphi1}-u_{\varphi2}=1$. 针对以上 2 种用户 i 情况,$\mathcal{B}$ 将会询问 C 并进行相应计算:

情况 1. 用户 i 不属于目标用户集合 $i\notin\ell^*$,C 计算 i 私钥部分:

$$D_1=g_i^{du_{\psi 1}}\prod_{j\in\ell^*}(g_{m+1-j+i})^{-1}(g^{\delta x u_{\psi 1}})\times\left(g^{r_0}\prod_{k\in W^*}g^{a^{m+1-k}}\right)^{-xu_{\psi 1}}=(g^{a^i\xi+(\delta-r)x})^{u_{\psi 1}}.$$

然后计算:

$$D_2=g^{xu_{\psi 1}},$$

$$D_{3,j}=g^{a^j u_{\psi 1}}.$$

对于 i 属性部分,根据 U^*,计算其系统通配符所对应私钥组件为

$$f_k=(g^{\delta_{k'}}g^{u_k-a^{m+1-k}})^{u_{\psi 1}x}=(g^{\delta_{k'}}T_k)^{u_{\psi 1}x}.$$

然后根据 S_i,计算:

$$\omega_{i,k}=\begin{cases}\omega_k=(g^{\delta_{k'}}g^{u_k-a^{m+1-k}})^{u_{\psi 1}x}=(g^{\delta_{k'}}T_k)^{u_{\psi 1}x},\\ \omega_q'=(g^{u_q-a^{m+1-q}}/g^{u_k-a^{m+1-k}})^{u_{\psi 1}x}=\\ \quad(T_q/T_k)^{u_{\psi 1}x},\ \forall q\in[1,k),\end{cases}$$

C 将 $SK_{i,1}=(D_1,D_2,\{D_{3,j}\}_{j=1,2,\cdots,2m\backslash\{m+1\}},\{f_i\}_{i\in U^*},\{\omega_{i,k}\}_{k\in S_i})$ 发送给模拟算法 $\mathcal{B}$ 转交给敌手 $\mathcal{A}$.

注意:用户 i 不属于目标用户集合,所以挑战者 C 可以产生 i 正确私钥.

情况 2. 用户 i 属于目标用户集合 $i\in\ell^*$,但 $S_i\not\models W^*$. 则 S_i 中必然存在至少一个属性 A_k 与访问结构 W^* 中属性权重值不相同. C 找出该位置上属性 A_{k^*}. 首先,对于用户 i 身份私钥部分,C 随机选择 2 个元素 $\delta',x'\in\mathbb{Z}_P$,并通过设置 $g^{\delta'}=g^{\delta}$,$g^{x'-\alpha^{k^*}}=g^x$,使得 $\delta=\delta'$,$x=x'-\alpha^{k^*}$,然后计算 i 的私钥部分:

$$D_1=(g^{a^i\xi}g^{(\delta-r)x})^{u_{\psi 1}}=g_i^{u_{\psi 1}d}\prod_{j\in\ell^*,j\neq ID}(g_{m+1-j+i})^{-1}g^{\delta'(x'-\alpha^{k^*})}g^{-r_0(x'-\alpha^{k^*})}\times\left(\prod_{k\in W^*}g^{\alpha^{m+1-k}}\right)^{-u_{\psi 1}x'}\left(\prod_{k\in W^*,k\neq k^*}g^{\alpha^{m+1-k+k^*}}\right)^{u_{\psi 1}},$$

$$D_2=g^{u_{\psi 1}x}=g^{u_{\psi 1}(x'-\alpha^{k^*})},$$

$$D_{3,j}=g^{\alpha^j u_{\psi 1}}.$$

根据 U^*,i 系统通配符所对应私钥组件为

$$f_k=(g^{\delta_{k'}}T_k)^{u_{\psi 1}x}=(g^{\delta_{k'}}g^{u_k-a^{m+1-k}})^{u_{\psi 1}(x'-\alpha^{k^*})}.$$

然后根据 S_i,计算:

$$\omega_{i,k}=\begin{cases}\omega_k=(g^{\delta_{k'}}g^{u_k-a^{m+1-k}})^{u_{\psi 1}(x'-\alpha^{k^*})}=\\ \quad(g^{\delta_{k'}}T_k)^{u_{\psi 1}(x'-\alpha^{k^*})},\\ \omega_q'=(g^{u_q-a^{m+1-q}}/g^{u_k-a^{m+1-k}})^{u_{\psi 1}(x'-\alpha^{k^*})}=\\ \quad(T_q/T_k)^{u_{\psi 1}(x'-\alpha^{k^*})},\ \forall q\in[1,k),\end{cases}$$

C 将 $SK_{i,1}=(D_1,D_2,\{D_{3,j}\}_{j=1,2,\cdots,2m\backslash\{m+1\}},\{f_i\}_{i\in U^*},\{\omega_{i,k}\}_{k\in S_i})$ 发送给 $\mathcal{B}$ 转交给敌手 $\mathcal{A}$.

注意:当 $S_i\not\models W^*$ 时,C 可以找出那个不符合的属性 A_{k^*},利用 A_{k^*} 的属性值产生的因子 $g^{a^{m+1}}$,可以和 D_1 中的 $g^{-a^{m+1}}$ 相互抵消,因此挑战者 C 不必知道 $g^{a^{m+1}}$ 也可产生正确的私钥.

挑战. $\mathcal{A}$ 随机选择 2 条长度相同的明文消息 $\mathcal{M}_0$,$\mathcal{M}_1$ 交给 C. 由 C 随机地选择 $b\in\{0,1\}$ 中的一个,运行加密算法计算 $CTM^*=\mathcal{M}\times T'$,并随机选择元素 $t\in\mathbb{Z}_P$,并计算:

$$C_0^*=g^t,$$

$$C_2^*=b^{r_0+\sum_{k\in W^*}u_k}=(g^{r_0+\sum_{k\in W^*}u_k})^t,$$

$$C_1^*=\left(g^d\prod_{j\in\ell^*}(g_{m+1-j})^{-1}\prod_{j\in\ell^*}(g_{m+1-j})\right)^t=\left(v\prod_{j\in\ell^*}(g_{m+1-j})\right)^t,$$

并将 $CT^*=\{CTM^*,C_0^*,C_1^*,C_2^*\}$ 发送给 $\mathcal{B}$ 转交给 $\mathcal{A}$.

阶段 2. 重复阶段 1.

猜想. 最终敌手 $\mathcal{A}$ 猜测 $b^*\in b$,如果猜测正确,模拟算法 $\mathcal{B}$ 输出 0,则称 $\mathcal{A}$ 在该游戏中获胜.

分析:如果 $T=e(g,g_{m+1})$,$\mathcal{A}$ 在游戏中的获胜概率为 $1/2+\varepsilon$;如果 T 是群 G_T 中随机元素,$\mathcal{A}$ 在游戏中的获胜概率为 1/2. 所以 $\mathcal{B}$ 做出准确模拟的优势为 $1/2Pr[\mathcal{B}(\mathbf{y},T=e(g,g_{m+1}))=0]+1/2Pr[\mathcal{B}(\mathbf{y},T=\Re)=0]-1/2=\varepsilon/2$,即模拟算法 $\mathcal{B}$ 能够以一个不可忽略的优势解决 m-BDHE 问题,但这一问题已被证明是困难的,因此假设不成立,证明 M-ABBE 方案是 CPA 安全的.

5.2 抗共谋攻击安全性

在属性基广播加密方案中,抗共谋攻击是一个很大的挑战,用户为了在恢复明文 $\mathcal{M}$ 时,必须先获得对称会话密钥 $e(g,g_{m+1})^s$. 不诚实的用户和敌手都有可能试图恢复该对称会话密钥. 由于属性基广播加密方案利用的是目标接收用户集合 ℓ 和属性访问结构的双重密文访问控制,用户的属性信息和身份信息在系统中都很关键. 本方案中共谋攻击分为 2 种:属性-身份共谋攻击和属性-属性的共谋攻击.

在情况 1 中,假设有攻击者 a 和 b,a 属于目标接收用户集合 $a\in\ell$,但是 $S_a\not\models W$;b 不属于目标接收用户集合 $b\notin\ell$,但 $S_b\models W$. 此时,如果 a 和 b 进行共谋,就存在明文 $\mathcal{M}$ 泄露的危险. 本方案中使用了随机因子抵抗情况 1 的共谋攻击. 具体来说在方案的私钥提取算法中,用户身份私钥 D_1 绑定用户身份和随机因子 $\xi,u_{\psi 1}$,同时用户属性私钥 f_k 和 $\omega_{GID,k}$

绑定随机因子 x,对于 a 和 b 来说 $u_{\psi 1}$ 不同,而且 δ,r,x 是随机的,因此无法联合私钥,所以本方案抗属性-身份共谋攻击.

在情况 2 中,假设 a 和 b 都属于目标接收用户集合 $a,b\in\ell$,但 $S_a\models W$,$S_b\models W$. 为了得到明文,现在 a 和 b 进行共谋,尝试将属性部分私钥并在一起. 但是本方案中用户属性私钥和不同的随机因子 δ_k,r,x 绑定. 因此,即使攻击者 a 和 b 尝试进行属性-属性共谋,也无法进行正确的 $\delta=\sum_{k=1}^{n}\delta_k$ 计算,因此会话密钥不会被恢复. 本文方案也可抗属性-属性共谋攻击.

5.3 性能分析

方案性能评估分为 2 方面:理论分析和实验仿真. 理论分析方面,将本方案对比 Attrapadung 等人在文献[19]中的第 1 个方案 Attrap1、Attrapadung 等人在文献[19]中的第 2 个方案 Attrap2、Karlov 等人在文献[20]中的方案、Zhou 等人在文献[18]中的方案以及胡思路等人在文献[22]中的方案,分析方案的功能、通信开销、存储开销和计算开销,将结果列表给出;实验仿真方面,将本方案对比文献[19]的第 1 个方案 Attrap1、文献[19]的第 2 个方案 Attrap2 和文献[22]的方案,通过相同环境中实验仿真,分析方案的私钥长度、加密和解密时间,将结果作图说明.

在进行方案性能评估时,$|G|$ 和 $|G_T|$ 分别代表群 G 和群 G_T 中一个元素的长度;N 代表系统属性值总数;n 代表访问结构中的属性个数;S_u 代表用户拥有的属性个数;r 代表被撤销的人数;ex 和 p 分别代表模指数和双线性对运算. 需要注意的是文献[19]第 1 个方案 Attrap1 中 n 代表访问结构中矩阵的行数;文献[20]方案中 $N=2n$;文献[18]方案中 $N=3n$.

5.3.1 理论分析

比较方案的功能、通信开销和存储开销时,由于通信开销与方案密文长度有关,存储开销与方案用户私钥长度有关,因此对比分析时主要对比了方案的密文长度和私钥长度. 由于广电网中通信资源有限,因此方案的密文长度越短越好,又由于接收用户存储资源匮乏,因此方案的用户私钥长度也越短越好.

从表 1 中可以看出,在方案的功能方面,对比方案全部没有考虑属性权重思想,其实引入属性权重概念具有现实意义,尤其是在分等级服务的广电网环境中. 如系统中属性“会员”、“年龄”、“地区”、“职业”,其中“会员”属性可以根据等级划分为“黄钻、绿钻、蓝钻”,因此可以按照权重等级定义为该属性为“(会员,1)(会员,2)(会员,3)”;“年龄”属性可以根据等级划分为“老年、少年、中年、青年”,对应权重属性为“(年龄,1)(年龄,2)(年龄,3)(年龄,4)”;同样“地区”属性可以划分为“三环、二环、一环”,对应权重属性为“(地区,1)(地区,2)(地区,3)”. 当发送方选择“(会员,2)(年龄,3)(地区,1)(职业,*)”作为密文访问结构中属性时,即表示发送方不考虑用户的“职业”属性,其余用户属性权重值均不小于对应加密属性权重值的接收用户才可解密,如住在二环的蓝钻青年即可解密. 因此,本方案通过属性权重的引入增加了访问结构的灵活性,满足了多样化的隐私需求.

Table 1 Comparison of Communication and Storage Overhead

表 1 通信开销与存储开销性能对比

Scheme	Size of Cipertext	Size of User's Privacy Key	Weighted	Outsourced
Ref[19]	$\|G_T\|+(2n+1)\|G\|$	$(S_u+2)\|G\|$	×	×
Ref[19]	$\|G_T\|+(2r+n+1)\|G\|$	$(S_u+4)\|G\|$	×	×
Ref[20]	$\|G_T\|+(2n+1)\|G\|$	$(2N+n+1)\|G\|$	×	×
Ref[18]	$\|G_T\|+2\|G\|$	$(2n+1)\|G\|$	×	×
Ref[22]	$\|G_T\|+3\|G\|$	$n(2n+1)+1\|G\|$	×	×
Ours	$\|G_T\|+3\|G\|$	$\|G\|$	√	√

Note: “√” means this scheme has this funtion, “×” means this scheme does not have this function.

在通信开销方面,从表 1 可以看出,文献[19]第 1 个方案 Attrap1、文献[19]第 2 个方案 Attrap2、文献[20]的方案密文长度都随着访问结构中的属性数目线性增长,属性数目增多,通信开销将飞速增长,不适合广电网应用环境. 文献[18,22]中方案和本方案都实现了密文长度的固定. 其中,文献[18]方案在

密文长度上比本方案小了一个$|G|$群元素和一个$|G_T|$群元素长度,而且也是基于同样 BGW 技术的思想.但是文献[18]方案只利用了属性基加密技术,只能实现属性级别的撤销.若撤销某个具体用户,必须进行复杂的私钥更新操作,不适合用户动态性强的广电网环境.最后,本方案和文献[22]方案的密文长度相同.

在存储开销方面,文献[19]第 1 个方案 Attrap1、文献[19]第 2 个方案 Attrap2、文献[18,20,22]方案的用户私钥长度都与访问结构中属性个数相关.其中文献[22]方案中用户私钥长度随着访问结构中属性个数增加而飞速增长,并且达到二次增长的相关关系,文献[20]方案中用户私钥长度还与系统属性个数线性相关.由于这些私钥需要用户本地存储,因此上述方案会给用户带来沉重的存储负担,不适用于接收用户的存储资源匮乏的环境.与以上方案不同,我们的方案采纳了中间人思想,通过外包存储将繁重的私钥存储任务委托给中间人执行,用户本地只需存储一个$|G|$长度的私钥,减轻了用户存储负担.并且本方案引入属性权重思想,系统可根据属性的重要性为其分配不同的权重,更适合实际应用背景.综上,本方案更适合应用于广电网环境.

比较方案的计算开销时,由于群 G 和群 G_T 上模乘运算的开销远远小于模指数运算和双线性对运算开销,因此对比分析时,只对比了 G 和 G_T 的模指数运算和双线性对运算.由于广电网中用户计算资源匮乏,因此方案加解密计算中模指数运算和双线性对运算数目越少越好.

从表 2 可以看出,在广播加密阶段文献[19]第 1 个方案 Attrap1、文献[19]第 2 个方案 Attrap2 和文献[20]方案中模指数计算数目均与访问结构中属性个数呈线性增长关系,不符合实际应用.文献[18,22]方案和本方案的加密计算开销固定并且差别很小,其中文献[18]方案比本方案的计算开销还少 2 个群 G 上的模指数的计算开销,文献[22]方案和本方案计算开销相同.但在解密阶段时,文献[18]方案需进行 $2n$ 次双线性对运算,计算开销随着访问结构中属性个数的增加线性增长.虽然文献[22]方案在解密计算时的双线性对运算数目固定,但也比本方案计算开销大.本方案通过引入中间人实现了解密外包,将复杂的解密计算委托给中间人执行,用户自己只需进行一个双线性对计算,更适合用户计算资源匮乏的广电网环境.

Table 2 Comparison of Computation Cost

表 2 计算开销性能对比

Scheme	Encryption Cost	Decryption Cost
Ref[19]	$(2n+3)ex$	$nex+(2n+3)p$
Ref[19]	$(2n+3r+2)ex$	$(2n+2r)ex+(n+r+1)p$
Ref[20]	$(1+2n)ex$	$(2n+1)p$
Ref[18]	$2ex$	$(2n)p$
Ref[22]	$4ex$	$(2n)ex+5p$
Ours	$4ex$	p

5.3.2 实验仿真

实验环境配置如下:Intel® Core™ i5-4210U CPU @1.70 GHz,双核,4.00 GB RAM, Windows 10 操作系统.实验仿真是基于 JPBC 密码库[24],采用 Java 语言实现.仿真中基于 a.properties 参数得到 3 个椭圆曲线群 G_1,G_2,G_T 以及一个有限域,并生成一个对称双线性映射 $e:G_1\times G_2\rightarrow G_T$.实验中选取了 5,10,15,20,25,30 共 6 个属性数目的参考点,并编写时间测量函数定量提取这 6 个参考点的加解密时间.图中的时间测量结果以毫秒(ms)为单位,并且所有数据是程序运行 30 次所取的平均值.具体仿真结果如图 3~5 所示:

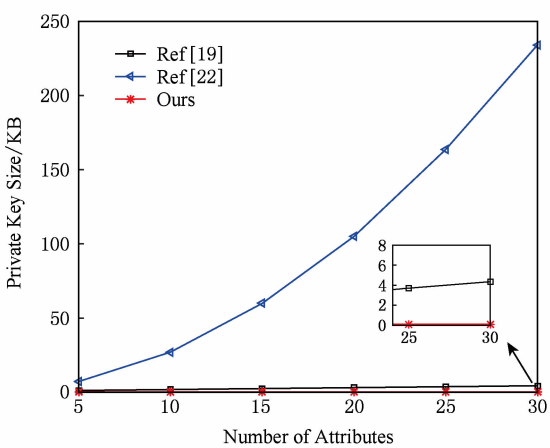

Fig. 3 Length of private key

图 3 用户私钥长度

由于文献[19]第 1 个方案 Attrap1 和文献[19]第 2 个方案 Attrap2 中密文访问结构相同,因此仿真时只选择了文献[19]第 1 个方案 Attrap1.图 3 所示,文献[19]第 1 个方案 Attrap1 中用户私钥的长度随着用户属性个数线性增加,在属性为 30 个时用户私钥长度 4.35 KB.文献[22]方案中用户私钥的长度随着用户属性个数的增加飞速增加,在属性为 30 个时用户私钥长度高达到 235 KB.而本方案不

同,用户私钥长度一直保持固定不变,只为 0.128 KB.这是由于本方案中引入了外包存储,所以用户只需要存储一个$|G|$群元素的私钥即可.

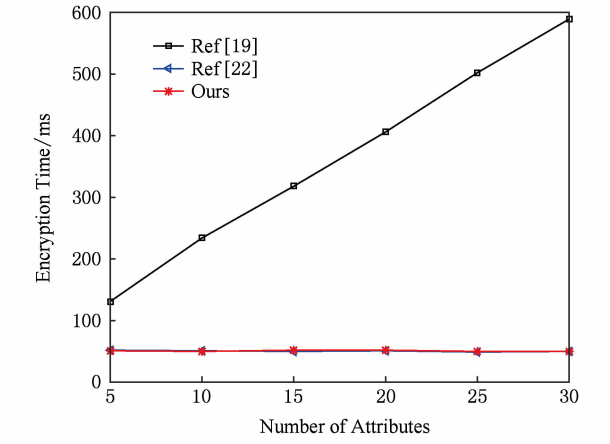

Fig. 4 Encryption time

图 4 加密运算时间

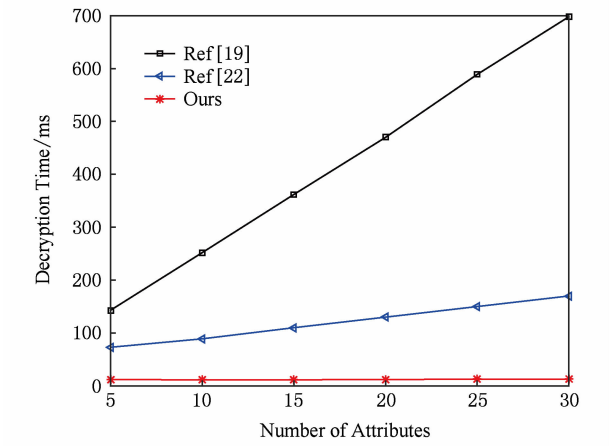

Fig. 5 Decryption time

图 5 解密运算时间

由图 4、图 5 可知,文献[19]第 1 个方案 Attrap1 的加密时间和解密时间都与方案访问结构中属性个数呈线性关系,不适用于用户计算资源有限的环境.文献[22]方案和本方案的加密时间都基本不变,加密时间几乎相同.但在解密计算时,文献[22]方案解密时间会随着属性个数逐渐增长,这是由于其方案中模指数运算数目随着属性个数呈线性增长关系.但我们的密文长度固定的属性基广播加密方案不同,用户解密时间固定不变,不随属性的变化而变化.这是由于本方案中借助了中间人进行解密外包,中间人代理解密后将外包解密密文交给用户,用户只需进行一次双线性对运算即可.所以综合加密时间与解密时间的对比分析,本方案计算性能要高于文献[22]的方案.

6 总 结

针对广电网中安全需求和应用特性,本文构造了一个高效的权重属性基广播加密方案.方案基于经典的 BGW 方案,并融合了门限属性基加密技术的优点,撤销用户时无需更新用户私钥组件,同时实现了广播密文长度的固定;引入属性权重概念更具有现实意义,并且增强了密文访问结构的灵活性;增加了通配符机制,满足了多样的隐私需求;通过引入外包存储和解密,实现较小存储开销和计算开销,符合终端用户中计算资源有限的广电网特征.经证明:本方案具有抗共谋攻击性.但是本方案仅实现了标准模型下的选择明文安全,如何将方案进行改进从而达到更高的安全性是今后的研究方向.

参 考 文 献

[1] Silva B N, Khan M, Han K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges [J]. IETE Technical Review, 2017, 35(2): 205-220

[2] Wang Yuwen. Thinking about the development of Internet of things service for next generation broadcasting network [J]. China New Telecommunications, 2017, 19(15): 74-75 (in Chinese)
(王宇雯. 关于下一代广播电视网络开展物联网业务的思考[J]. 中国新通信, 2017, 19(15): 74-75)

[3] Wang Zhiyu, Wang Yifei, Zhu Donghua. Research on multi-service cloud platform of the IoT in home based on cable TV network [J]. Radio & TV Broadcast Engineering, 2017, 44(6): 65-67 (in Chinese)
(王智宇, 王亦飞, 朱东华. 基于广播电视网络的家庭物联网多业务云平台初探[J]. 广播与电视技术, 2017, 44(6): 65-67)

[4] Berkovits S. How to broadcast a secret [C] //Proc of EUROCRYPT 1991. Berlin: Springer, 1991: 535-541

[5] Fiat A, Naor M. Broadcast encryption [C] //Proc of CRYPTO 1993. Berlin: Springer, 1993: 480-491

[6] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers [C] //Proc of CRYPTO 2001. Berlin: Springer, 2001: 41-62

[7] Du Xinjun, Wang Ying, Ge Jianhua, et al. An ID-based broadcast encryption scheme for key distribution [J]. IEEE Trans on broadcasting, 2005, 51(2): 264-266

[8] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C] //Proc of CRYPTO 2005. Berlin: Springer, 2005: 258-275

[9] Sahai A, Waters B. Fuzzy identity-based encryption [C] // Proc of EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[10] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf of Computer and Communications Security. New York: ACM, 2006: 89-98

[11] Emura K, Miyaji A, Omote K, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [J]. International Journal of Applied Cryptography, 2010, 2(1): 46-59

[12] Chen Cheng, Zhang Zhenfeng, Feng Dengguo. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost [C] //Proc of ProvSec 2011. Berlin: Springer, 2011: 84-101

[13] Zhang Yinghui, Chen Xiaofeng, Li Jin, et al. FDR-ABE: Attribute-based encryption with flexible and direct revocation [C] //Proc of the 5th IEEE Conf of Intelligent Networking and Collaborative Systems. Piscataway, NJ: IEEE, 2013: 38-45

[14] Ibraimi L, Petkovic M, Nikova S, et al. Mediated ciphertext-policy attribute-based encryption and its application [C] //Proc of WISA 2009. Berlin: Springer, 2009: 309-323

[15] Liu Ximeng, Ma Jianfeng, Xiong Jinbo, et al. Ciphertext-policy weighted attribute based encryption for fine-grained access control [C] //Proc of the 5th IEEE Conf of Intelligent Networking and Collaborative Systems. Piscataway, NJ: IEEE, 2013: 51-57

[16] Wang Shulan, Liang Kaitai, Liu J K, et al. Attribute-based data sharing scheme revisited in cloud computing [J]. IEEE Trans on Information Forensics & Security, 2017, 11(8): 1661-1673

[17] Lubicz D, Sirvent T. Attribute-based broadcast encryption scheme made efficient [C] //Proc of AFRICACRYPT 2008. Berlin: Springer, 2008: 325-342

[18] Zhou Zhibin, Huang Dijiang. Constructing efficient attribute-based broadcast encryption [C] //Proc of IEEE INFOCOM Conf of Computer Communications Workshops. Piscataway, NJ: IEEE, 2010: 1-2

[19] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption [C] //Proc of the Pairing-Based Cryptography—Pairing 2009. Berlin: Springer, 2009: 248-265

[20] Junod P, Karlov A. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies [C] //Proc of the 10th ACM Conf of Digital Rights Management. New York: ACM, 2010: 13-24

[21] Zhou Zhibin, Huang Dijiang, Wang Zhijie. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption [J]. IEEE Trans on Computers, 2014, 64(1): 126-138

[22] Hu Silu, Chen Yanli. Attribute-based broadcast encryption scheme with constant ciphertext size [J]. Application Research of Computers, 2016, 33(6): 1780-1784 (in Chinese)
(胡思路, 陈燕俐. 一种基于属性的固定密文长度广播加密方案[J]. 计算机应用研究, 2016, 33(6): 1780-1784)

[23] Phuong T V X, Yang G, Susilo W, et al. Attribute based broadcast encryption with short ciphertext and decryption key [C] //Proc of ESORICS 2015. Berlin: Springer, 2015: 252-269

[24] Morales-Sandoval M, Gonzalez-Compean J L, Diaz-Perez A, et al. A pairing-based cryptographic approach for data security in the cloud [J]. International Journal of Information Security, 2017 (2): 1-21

Li Xuejun, born in 1969. PhD, associate professor, master supervisor. Her main research interests include attribute based encryption, information security, Internet of things.

Yuan Yawen, born in 1994. Master. Her main research interests include attribute based encryption, Internet of things.

Jin Chunhua, born in 1980. PhD. Her main research interests include attribute based encryption, Internet of things.