软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(6):1498−1510 [doi: 10.13328/j.cnki.jos.004993]

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

一种实现一般电路的密钥策略的属性加密方案*

胡 鹏, 高海英

(信息工程大学,河南 郑州 450001)

通信作者: 胡鹏, E-mail: hupeng007@126.com

摘 要: 属性加密方案中引入访问结构,实现了用户对密文细粒度的访问控制.任意访问结构都可以通过一般电路来实现,因此,设计实现一般电路访问结构的属性加密方案是该领域的研究热点和难点.Garg 等人基于多线性映射首次提出了实现一般电路访问结构的属性加密方案,但该方案支持的电路是受限的,电路节点只能逐层输出,系统中实现的访问结构的电路深度都是固定值 *l*.为了解决电路受限的问题,提出了一种实现一般电路的密钥策略的属性加密方案.在私钥生成算法中,通过对电路进行等价转换,引入转换密钥,实现了任意深度大于 1、小于等于 *l* 的电路访问结构;将电路中非叶子节点的密钥与该节点的两个输入节点的深度相关,实现了节点的跨层输入.基于 *k*-多线性判定性 Diffie-Hellman(*K*-MDDH)假设证明了该方案具有选择安全性.

关键词: 属性加密;多线性映射;一般电路;跨层输入;选择安全

中图法分类号: TP309

中文引用格式: 胡鹏,高海英.一种实现一般电路的密钥策略的属性加密方案.软件学报,2016,27(6):1498−1510. http://www.jos.org.cn/1000-9825/4993.htm

英文引用格式: Hu P, Gao HY. Key-Policy attribute-based encryption scheme for general circuits. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1498−1510 (in Chinese). http://www.jos.org.cn/1000-9825/4993.htm

Key-Policy Attribute-Based Encryption Scheme for General Circuits

HU Peng, GAO Hai-Ying

(Information Engineering University, Zhengzhou 450001, China)

Abstract: Through introducing the access structure into attribute-based encryption, users can achieve the fine-grained access control to the ciphertext. Any access structure can be realized by general circuit. Therefore, designing attribute-based encryption for general circuit is difficult in this field. Garg etc. presented the first general circuit access structure based on multilinear maps. However the usability of the access structures is rather limited as gate can only output layer by layer and the depth of the circuit are fixed in *l*. In order to solve this limitation, this paper proposes a key-policy attribute-based encryption scheme for general circuits based on the Garg's scheme. In key generation step, the new scheme implements any circuit that depth is greater than 1 and less than or equal to *l* by equivalent conversion of the circuit and addition of the conversion key. It also achieves cross layer output by adding its child node depth into every non-leaf node's key component. Selective security of the proposed scheme in the standard model is proved under the decisional multilinear Diffie-Hellman assumption.

Key words: attribute-based encryption; multilinear map; general circuit; cross layer output; selective security

近年来,云计算在互联网中的地位日益显著,能够给用户提供以往自身难以实现的存储空间和计算能力.但在方便和快捷的同时,云端数据的安全性也成为云计算中亟待解决的问题.为保证云端数据的机密性,通常以加

* 基金项目: 国家自然科学基金(61272488); 信息保障技术重点实验室资助项目(KJ-15-006)

Foundation item: National Natural Science Foundation of China (61272488); Science and Technology on Information Assurance Laboratory (KJ-15-006)

收稿时间: 2015-08-10; 修改时间: 2015-10-09; 采用时间: 2015-12-05; jos 在线出版时间: 2016-01-21

CNKI 网络优先出版: 2016-01-22 10:14:47, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1014.003.html

密的形式存储,然而传统的加密方式并不利于多个用户之间进行数据共享.属性加密作为一种新型加密技术,同时具有加密和访问控制的功能,可用于实现云端共享数据的细粒度访问控制.

2005 年,Sahai 和 Waters[1]在欧洲密码年会上首次提出了属性加密(attribute-based encryption,简称 ABE)的概念.在 ABE 方案中,每个用户用一组属性进行标识,与属性对应的还有访问结构这一概念,当用户的属性满足指定的访问结构时才能正常解密.2006 年,Goyal 等人[2]提出了基于属性的密钥策略加密(key-policy ABE,简称 KP-ABE)方案,将属性集合嵌入到密文中,访问结构嵌入到私钥中,只有两者相互满足时,才可正常解密.2007 年,Bethencourt 等人[3]提出了基于属性的密文策略加密(ciphertext-policy ABE,简称 CP-ABE)方案,将属性集合嵌入到私钥中,访问结构嵌入到密文中,同样,只有两者相互满足时,才能正常解密.

随着属性加密方案的不断发展,其访问结构的表达能力也越来越广泛.最初的访问结构为树状结构(access tree)[2],内部由多输入单输出的(k,n)门限节点组成.由于支持树状结构的 CP-ABE 方案的设计以及方案的安全性证明过程极为复杂,随后出现了由线性秘密分享方案(linear secret sharing schemes,简称 LSSS)[15]构成的单调访问结构,方案设计以及证明过程得到了简化.更进一步地,出现了非单调访问结构[8],使得属性加密更加完善.

2013 年,Garg 等人[4]在 Goyal 方案的基础上,利用多线性映射[5]首次提出了一般电路(general circuits)访问结构,由于任意访问结构都可由一般电路来实现,因此一般电路访问结构的表达能力最强.文献[4]中指出,如果直接把 Goyal 方案扩展为支持一般电路访问结构的 ABE 方案,则方案难以抵抗回溯攻击.为了解决该问题,文献[4]修改了 Goyal 方案自上向下为每条线路计算分享值的方式,直接为每条线路分配相互独立的随机值(多输出线路的随机值为同一个),然后为每个节点设置门密钥,门密钥为输入线路的随机值与输出线路的随机值建立一定的联系,这种门密钥生成方式解决了 Goyal 方案中由 OR 门输入相等引发的回溯攻击的问题,但是,用户的密钥量将随着节点个数线性增长,且由于多线性映射的引入,需要进行多次对运算,计算复杂度较大.随后,Kangro[6]对 Garg 方案进行了改进,通过合并参数,一定程度降低了用户的私钥规模.2014 年,Ferucio 等人[12]基于双线性映射构造的实现一般电路的 KP-ABE 方案,但该方案只适用于一些简单电路结构,一旦某条线路多次出现多输出的情况,私钥量将呈线性增长.2015 年,Xu 等人[14]首次构造了实现一般电路的 CP-ABE 方案,该方案对于电路的处理方式与 Garg 方案一致.在本文的第 3 节,我们给出了同以上 4 个方案的对比情况.需要指出的是,Garg 方案、Kangro 方案和 Xu 方案中支持的电路访问结构具有一定的限制条件:电路深度为固定值 l;电路中任意一个深度为 j 的非叶子节点,只接收来自深度为 j–1 的节点的输出,该限制条件降低了方案的适用性.

为了解决上述问题,本文在 Garg 方案的基础上提出了一种新的实现一般电路的 KP-ABE 方案,通过修改门密钥的参数形式,解决了 Garg 方案只能逐层向上输出的限制,实现了每个节点可以向任何大于自身深度的节点跨层输出;通过对电路进行等价转换,引入转换密钥,实现了任意深度大于 1,小于等于 l 的电路访问结构,扩大了方案的适用范围.基于 k-多线性判定性 Diffie-Hellman(K-MDDH)假设证明了该方案具有选择安全性,并且分析了该方案与现有方案相比均有一定的优势.

1 预备知识

1.1 访问结构

定义 1. 访问结构(access structures)[7]:给定一个非空有限集合 U.由 U 的任意非空子集构成的集合 S,称为定义在 U 上的访问结构.S 被称为单调的,如果它满足:

$$(\forall B \in S)((\exists A \in S)(A \subseteq B) \Rightarrow B \in S),$$

U 中属于 S 的子集称为授权集合,反之,U 中不属于 S 的集合称为非授权集合.

在 ABE 方案中,我们把集合 U 中的元素称为属性,每个用户用属性集合进行标记,用户拥有的属性越多,相对应的解密能力越强.

1.2 电 路

电路由节点和线路组成,其中,节点分为叶子节点和非叶子节点.输入端(input)的节点即为叶子节点,每个叶

子节点对应一个属性.非叶子节点由与门(AND gate)、或门(OR gate)和非门(NOT gate)3 种类型组成.而位于输出端(output)的非叶子节点,称为根节点.电路中的线路即为连接下层节点与上层节点之间的连线,其中,AND 门和 OR 门有两路输入,NOT 门为一路输入.若电路中任意节点的输出只能作为一个上层节点的输入,称为布尔电路(Boolean circuits);若电路中任意节点的输出可以作为多个上层节点的输入,称为一般电路(general circuits)[4];只包含 AND 门和 OR 门的电路称为单调电路(monotone circuits)[8].

文献[4]中提到,利用摩根定理,可以将电路中所有的 NOT 门,降低到非叶子节点所在的最底层,得到相同深度的非叶子节点只有 AND 门和 OR 门的单调电路.故本文提到的一般电路都是指单调一般电路.

电路的 n 个输入对应一个 n 维向量 $x\in\{0,1\}^n$ 每个输入对应一个属性,若用户拥有第 i 个属性,则 x 的第 i 个分量 x_i=1,反之,x_i=0.根节点的输出为 0 或 1.电路对应一个映射 $f:\{0,1\}^n\to\{0,1\}$若用户属性集合满足访问结构,则 $f(x)$=1,即根节点的输出为 1.令 $f_w(x)$表示以 w 为根节点的子电路的输出值.

为电路中的每个节点 w 赋予一个深度值,用 $depth(w)$来表示.规定叶子节点的深度为 1,每经过一条线路,深度值加 1(自下向上累加),非叶子节点的深度为从任意叶子节点到该节点所有深度的最大值.整个电路的深度等于根节点的深度.

本文约定一个电路结构由 6 元组表示,即$(l',n,q,A_1,A_2,GateType)\to f$.其中,$l'$为电路的深度,$n$ 为叶子(即输入)节点的个数,q 为非叶子(即门)节点的个数.将输入和门节点分别用正整数标记为 $inputs=\{1,\ldots,n\}$,$Gates=\{n+1,\ldots,n+q\}$,其中,根节点的标记为 $n+q$.门节点 w 的左右输入节点分别用 $A_1(w)$,$A_2(w)$表示,$GateType(w)$表示 w 的门类型,即 $GateType:Gates\to\{AND,OR\}$.

下面举例说明以上概念和约定,图 1 是一个一般电路的例子.

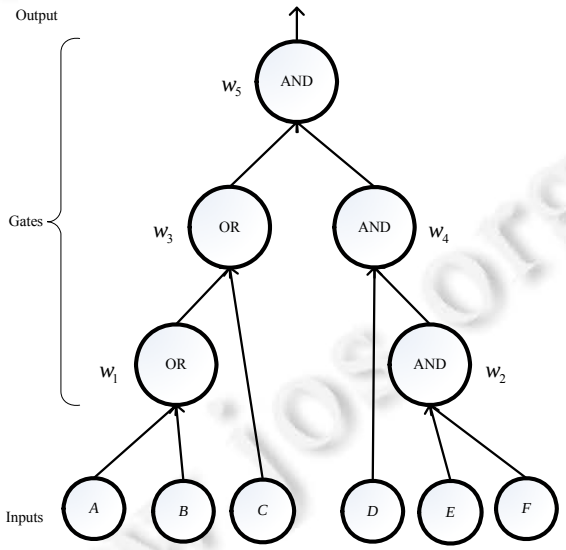


Fig.1 General circuit

图 1 一般电路

如图 1 所示,l'=4,n=6,q=5,$GateType(w_1)$=OR,$depth(w_1)$=2,$A_1(w_5)=w_3$,$A_2(w_5)=w_4$.假设用户拥有 B,C,D 属性,则用户属性集对应的向量 x=(0,1,1,10,0), $f_{w_1}(x)$=1, $f(x)=f(0,1,1,1,0)$=0,表示属性集$\{A,B,C\}$不满足该访问结构.

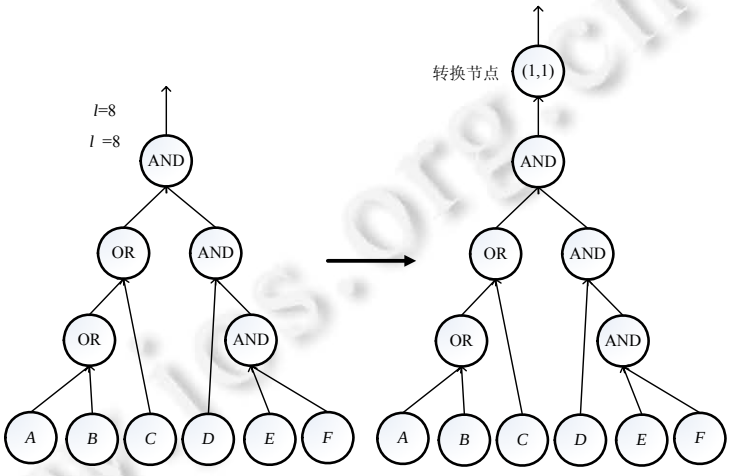
1.3 电路转换

设 l 为方案支持的电路最大深度,为了使方案支持任意深度小于 l 的电路,我们首先将深度小于 l 的电路进行等价转换,然后,在私钥生成算法中,对等价转换后的电路生成密钥.设电路的深度为 $l'(1<l'\leqslant l)$.

(1) 若 $l'=l$,转换电路等于原电路;

(2) 若 $1<l'<l$,我们在原电路的根节点的上层,增加一个单输入单输出的(1,1)转换节点,得到转换后的电路,该电路等价于原电路.

假设 ABE 方案支持的电路最大深度 l=8,图 2(a)和图 2(b)分别是原电路和等价转换后的电路.从形式上来看,可以认为转换节点处于 l 层,即我们将 l'层的电路等价转换为 l 层的电路,且根节点向一个处于 l 层的转换节点跨层输出.



(a) 原电路 (b) 等价转换后的电路

Fig.2

图 2

1.4 实现电路结构的KP-ABE方案的形式化定义

实现电路结构的 KP-ABE 方案由 3 个概率多项式时间(PPT)算法和一个确定性多项式时间算法构成[4].

Setup $(1^{\lambda},n,l)\rightarrow(PP,MSK)$: 该概率初始化算法的输入为安全参数$\lambda$,系统属性个数 n 和电路的最大深度 l.输出公共参数 PP 和主密钥 MSK.

Encrypt $(PP,x\in\{0,1\}^n,M)\rightarrow CT$: 该概率加密算法的输入为公共参数 PP,密文中属性对应的向量 $x\in\{0,1\}^n$ 和明文 M.输出密文 CT.

KeyGen $(MSK,f)\rightarrow SK$: 该概率密钥生成算法的输入为主密钥 MSK,电路 f .输出用户私钥 SK.

Decrypt $(SK,CT)\rightarrow M/\perp$: 该确定性解密算法的输入为电路 f 对应的私钥 SK 和包含属性集合 x 的密文 CT.如果 $f(x)$=1,则解密成功并输出明文 M;否则,解密失败并输出 $\perp$.

1.5 实现电路结构的KP-ABE方案的安全模型

选择安全模型可表示为攻击者和挑战者之间进行的一个游戏,如果最终攻击者给出了正确的猜测,则攻击者赢得了游戏,反之,挑战者赢得了游戏.

Init:攻击者声明在后续阶段想要挑战的属性集合对应的输入向量 x^*.

Setup:挑战者运行方案的初始化算法,将生成的公共参数 PP 发送给攻击者,保留主密钥 MSK.

Phase 1:攻击者可以自行选择电路结构 f 进行任意多项式次数的私钥查询,但要求选择的电路结构 f 不能满足挑战的输入向量 x^*,即要求 $f(x^*)=0$.挑战者运行 **KeyGen**(MSK,f),将生成的私钥发送给攻击者.

Challenge:攻击者提交两个等长的明文 M_0 和 M_1.随后挑战者随机抛币得到 $b\in\{0,1\}$,计算 **Encrypt**(PP, x^*,M_b)$\rightarrow CT^*$,并将 CT^*作为挑战密文返回给攻击者.

Phase 2:与 Phase 1 相同.

Guess:攻击者给出关于 b 的猜测 b'.

攻击者赢得上述游戏的优势定义为 $\Pr[b'=b]-\frac{1}{2}$.

定义 3[4]. 如果对于所有多项式时间的攻击者,赢得上述游戏的优势都是可忽略的,则称该 KP-ABE 方案是选择安全的.

1.6 双线性映射和多线性映射

定义 4. 双线性映射(bilinear maps)[10].设 G_1,G_2 为两个阶为素数 p 的乘法循环群,且 g 为 G_1 的生成元.对于映射 e:$G_1\times G_1\to G_2$,我们称其为双线性映射,如果其满足如下 3 个性质.

(1) 双线性性: $\forall a,b\in Z_p,h\in G_1\Rightarrow e\left(g^a,h^b\right)=e(g,h)^{ab}$.

(2) 非退化性: $e(g,g)\neq 1$.

(3) 可计算性:对于 $\forall g,h\in G_1$,均可在多项式时间内计算出 $e(g,h)$.

定义 5. 多线性映射(multilinear maps)[4].假设存在群生成算法 ς,其输入为安全参数 λ 和正整数 k,$\varsigma\left(1^\lambda,k\right)$ 输出阶都为素数 $p>2^\lambda$ 的群序列 $\vec{G}=(G_1,...,G_k)$,其中,G_i 的生成元为 g_i.假设存在一系列的双线性映射 $\left\{e_{i,j}:G_i\times G_j\to G_{i+j}\mid i,j\geqslant 1;i+j\leqslant k\right\}$(所有的 $e_{i,j}$ 和 G_i 统称为群描述),我们称这一系列映射为多线性映射,如果满足如下性质:

$$\forall a,b\in Z_p\Rightarrow e_{i,j}\left(g_i^a,g_j^b\right)=g_{i+j}^{ab}.$$

为简化描述,我们一般将每个映射 $e_{i,j}$ 的角标省略,将上式简写成如下形式:

$$e\left(g_i^a,g_j^b\right)=g_{i+j}^{ab}.$$

下面介绍基于多线性映射构造的困难假设,方案[4,6,13,14]和本方案的安全性都是基于该假设构造的.

定义 6[4]. k-多线性判定性 Diffie-Hellman(k-MDDH)假设:对于一系列阶为素数 p 的乘法循环群和相应的生成元 $g=g_1,g_2,...,g_k$,给定 $g,g^s,g^{c_1},...,g^{c_k}$,其中,$s,c_1,...,c_k\in Z_p$ 为随机选取,则区分 $T=g_k^{s\prod_{j\in[1,k]}c_j}$ 和 G_k 中的一个随机数的优势是可忽略的.

2 实现一般电路结构的 KP-ABE 方案

本方案在文献[4]方案的基础上,通过修改参数的形式,解决了原方案无法跨层输入的问题;通过增加一个转换节点,增强了电路的选择范围,下面我们来详细介绍方案.

Setup $(1^\lambda,n,l)$. 系统初始化阶段输入为安全参数 λ,电路最大深度 l 和系统属性个数 n.

首先利用群生成算法 $\varsigma(1^\lambda,k=l+1)$ 生成素数 p 阶群组 $\vec{G}(G_1,...,G_k)$,生成元分别为 $g_1,...,g_k$.令 $g=g_1$.然后,随机选取 $\alpha\in Z_p,h_1,...,h_n\in G_1$.

公共参数(PP)为群描述和 $g_{k-1}^\alpha,h_1,...,h_n$;系统主密钥($MSK$)为 α.

Encrypt $\left(PP,x\in\{0,1\}^n,M\in G_k\right)$.加密阶段输入为公共参数 PP,输入向量 $x\in\{0,1\}^n$ 和编码为 G_k 上的明文消息 M.

算法随机选择 $s\in Z_p$.令 $C_M=M\cdot\left(g_k^\alpha\right)^s$.设 S 为向量 x 中分量满足 x_i=1 的角标 i 构成的集合.则密文为

$$CT=\left(C_M,g^s,\forall i\in S,C_i=h_i^s\right).$$

KeyGen $(MSK,(l',n,q,A_1,A_2,GateType)\to f)$.密钥生成阶段输入为主密钥 MSK 和作为访问控制结构的电路 f,其中,$l'(1<l'\leqslant l)$ 为电路的深度;电路共有 n 路输入和 q 个门,第 $n+q$ 个门为根节点,$A_1,A_2,Gatetype$ 为相应的映射.

我们为每个节点 w 选取随机值 r_w,即随机选取 $r_1,...,r_{n+q}\in Z_p$.然后分别为电路中的 Inputs、OR 门和 AND 门生成相应的密钥.

Inputs: 如果 $w\in[1,n]$,算法随机选取 $z_w\in Z_p$,由相应的 r_w,生成 w 对应的密钥为

$$K_{w,1}=g^{r_w}h_w^{z_w},K_{w,2}=g^{-z_w}.$$

OR Gate: 如果 *GateType*(w)=OR,不妨设 $j,d_1,d_2(1\leqslant d_1,d_2\leqslant j-1)$ 分别为 $w,A_1(w),A_2(w)$ 的深度,随机选取 $a_w^{(1)},a_w^{(2)}\in Z_p$,由相应的 $r_{A_1(w)},r_{A_2(w)},r_w$, 生成 w 对应的密钥为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}},K_{w,2}=g_{j-d_2}^{a_w^{(2)}},\ K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}},K_{w,4}=g_j^{r_w-a_w^{(2)}r_{A_2(w)}}.$$

AND Gate: 如果 *GateType*(w)=AND,同样不妨设 $j,d_1,d_2(1\leqslant d_1,d_2\leqslant j-1)$ 分别为 $w,A_1(w),A_2(w)$ 的深度,随机选取 $a_w^{(1)},\ a_w^{(2)}\in Z_p$,由相应的 $r_{A_1(w)},r_{A_2(w)},r_w$, 生成 w 对应的密钥为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}},K_{w,2}=g_{j-d_2}^{a_w^{(2)}},\ K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}-a_w^{(2)}r_{A_2(w)}}.$$

KeyGen 算法不仅为每个输入和门生成密钥,还需要生成一些其他的辅助密钥.

(1) 当电路深度 $l'=l$ 时,利用主密钥α和 r_{n+q},生成头部密钥.

$$K_H=(g_{k-1})^{\alpha-r_{n+q}}.$$

(2) 当电路深度 $l'<l$ 时,随机选取 $a_e,r_e\in Z_p$, 由 r_{n+q} 生成转换密钥.

$$K_{e,1}=g_{e-l'}^{a_e},\ K_{e,2}=g_l^{r_e-a_er_{n+q}}.$$

再利用主密钥α和 r_e,生成头部密钥.

$$K_H=(g_{k-1})^{\alpha-r_e}.$$

Decrypt(*SK*,*CT*). 由于 $C_M=M\cdot(g_k^{\alpha})^s$, 因此,若要正确解密出消息 M,需要计算 $g_k^{\alpha s}$. 下面我们仍分两种情况讨论.

(1) 当 $l'=l$ 时,由于 $e(K_H,g^s)=e\left(g_{k-1}^{\alpha-r_{n+q}},g^s\right)=g_k^{\alpha s}g_k^{-r_{n+q}s}$ 且 $k=l+1$,故等价求 $g_k^{sr_{n+q}}=g_{l+1}^{sr_{n+q}}$;

(2) 当 $l'<l$ 时,由于 $e\left(K_H,g^s\right)=e\left(g_{k-1}^{\alpha-r_e},g^s\right)=g_k^{\alpha s}g_k^{-r_es}$ 且 $k=l+1$,故等价求 $g_k^{sr_e}=g_{l+1}^{sr_e}$.

下面分析:当密文中的向量 x 密钥中的 f 满足 $f(x)=1$ 时,可自下而上在相应条件下迭代计算出 $g_{l+1}^{sr_{n+q}}$ 或 $g_{l+1}^{sr_e}$. 我们分 3 种情况进行计算,对于电路中任意深度为 $j(1\leqslant j\leqslant l)$的节点 w,如果 $f_w(x)=1$,则通过该节点的密钥,可以计算出 $E_w=(g_{j+1})^{sr_w}$. 需要特别指出的是:若 $l'=l$,则得到根节点对应的输出 $E_{n+q}=(g_{l+1})^{sr_{n+q}}$; 若 $l'<l$,得到 $E_{n+q}=(g_{l'+1})^{sr_{n+q}}$, 然后通过转换密钥,即可得到 $(g_{l+1})^{sr_e}$.

Inputs: 如果 $w\in[1,n]$且 $f_w(x)=1$,则利用该节点的密钥,进行如下计算:

$$\begin{aligned}E_w&=e\left(K_{w,1},g^s\right)e\left(K_{w,2},C_w\right)=e\left(g^{r_w}h_w^{z_w},g^s\right)e\left(g^{-z_w},h_w^s\right)\\&=e\left(g^{r_w},g^s\right)e\left(h_w^{z_w},g^s\right)e\left(g^{-z_w},h_w^s\right)=g_2^{sr_w}.\end{aligned}$$

OR Gate: 如果 *GateType*(w)=OR,不妨设 w 的深度为 j=*depth*(w),且密钥中的 d_1,d_2 与 *depth*($A_1(w)$), *depth*($A_2(w)$)保持一致.即 d_1=*depth*($A_1(w)$),d_2=*depth*($A_2(w)$).如果 $f_w(x)=1$ 且 $f_{A_1(w)}(x)=1$, 则通过 w 点的密钥进行如下计算:

$$E_w=e\left(E_{A_1(w)},K_{w,1}\right)e\left(K_{w,3},g^s\right)=e\left(g_{d_1+1}^{sr_{A_1(w)}},g_{j-d_1}^{a_w^{(1)}}\right)e\left(g_j^{r_w-a_w^{(1)}r_{A_1(w)}},g^s\right)=g_{j+1}^{sa_w^{(1)}r_{A_1(w)}}\cdot g_{j+1}^{sr_w-sa_w^{(1)}r_{A_1(1)}}=g_{j+1}^{sr_w}.$$

如果 $f_w(x)=1$ 且 $f_{A_2(w)}(x)=1$, 则进行如下计算:

$$\begin{aligned}E_w&=e\left(E_{A_2(w)},K_{w,2}\right)e\left(K_{w,4},g^s\right)\\&=e\left(g_{d_2+1}^{sr_{A_2(w)}},g_{j-d_2}^{a_w^{(2)}}\right)e\left(g_j^{r_w-a_w^{(2)}r_{A_2(w)}},g^s\right)\\&=g_{j+1}^{sa_w^{(2)}r_{A_2(w)}}\cdot g_{j+1}^{sr_w-sa_w^{(2)}r_{A_2(w)}}=g_{j+1}^{sr_w}.\end{aligned}$$

AND Gate: 如果 *GateType*(w)=AND,同样设其深度 *depth*(w)=j,且密钥中的 d_1,d_2 与 *depth*($A_1(w)$), *depth*($A_2(w)$)保持一致.如果 $f_w(x)=1$,即 $f_{A_1(w)}(x)=f_{A_2(w)}(x)=1$, 则通过 w 点的密钥进行如下计算:

$$E_w = e\left(E_{A_1(w)}, K_{w,1}\right)e\left(E_{A_2(w)}, K_{w,2}\right)e\left(K_{w,3}, g^s\right)$$
$$= e\left(g_{d_1+1}^{sr_{A_1(w)}}, g_{j-d_1}^{a_w^{(1)}}\right)e\left(g_{d_1+1}^{sr_{A_2(w)}}, g_{j-d_2}^{a_w^{(2)}}\right)e\left(g_j^{r_w - a_w^{(1)} r_{A_1(w)} - a_w^{(2)} r_{A_2(w)}}, g^s\right)$$
$$= g_{j+1}^{sa_w^{(1)} r_{A_1(w)}} \cdot g_{j+1}^{sa_w^{(2)} r_{A_2(w)}} \cdot g_{j+1}^{sr_w - sa_w^{(1)} r_{A_1(w)} - sa_w^{(2)} r_{A_2(w)}} = g_{j+1}^{sr_w}.$$

根据以上 3 种情况自下而上计算,若 $f(x)=1$,即可得到根节点对应的 $E_{n+q} = (g_{l'+1})^{sr_{n+q}}$. 由前面的分析可知,当电路深度 $l'=l$ 时,可直接正常解密;而当电路深度 $l'<l$ 时,再通过转换密钥进行如下计算:

$$E_l = e\left(g_{l'+1}^{sr_{n+q}}, K_{e,1}\right)e\left(K_{e,2}, g^s\right) = e\left(g_{l'+1}^{sr_{n+q}}, g_{l-l'}^{a_e}\right)e\left(g_l^{r_e - a_e r_{n+q}}, g^s\right) = g_{l+1}^{sa_e r_{n+q}} \cdot g_{l+1}^{sr_e - sa_e r_{n+q}} = g_{l+1}^{sr_e}.$$

以上两种情况均可进一步计算出明文消息 M.

2.1 安全性证明

下面给出 KP-ABE 方案在选择安全下的安全性证明,安全性基于 k-多线性判定性 Diffie-Hellman(K-MDDH)假设.

定理 1. 对任意深度为 $l'(1<l'\leqslant l)$的电路结构,在 K-MDDH 假设成立的条件下,本节提出的 KP-ABE 方案具有选择安全性.

证明:模拟者的目的是解决 K-MDDH 问题,模拟者已知群组 $\vec{G} = (G_1,\ldots,G_k)$ 和 $g, g^s, g^{c_1},\ldots,g^{c_k}, T$, 其中,$T$ 为 $g_k^{sc_1\cdots c_k}$ 或 G_k 上的随机数 g_k^z, T 为两者的概率皆为 1/2,模拟者需要对 T 进行判定.方案攻击者的目的是赢得与模拟者之间的游戏(见第 2.4 节).模拟者将利用攻击者在游戏中传递的信息解决 K-MDDH 问题.过程如下:

Init: 攻击者声明想要挑战的输入向量 $x^*\in\{0,1\}^n$.

Setup: 模拟者随机选择 $y_1,\ldots,y_n \in Z_p$, 对于 $w\in[1,n]$,令

$$h_w = \begin{cases} g^{y_w}, & x_w^* = 1 \\ g^{y_w + c_1}, & x_w^* = 0 \end{cases},$$

模拟者随机选取 $\xi \in Z_p$, 令 $g_k^{\alpha} = g_k^{c_1\cdots c_k + \xi}$, 该值可以利用 $g^{c_1},\ldots,g^{c_k}$, 使用对运算迭代得到.

注意到由于随机数 y_w 和 ξ 的参与,使得从攻击者的角度来说,h_w 和 g_k^{α} 与真实的方案无法区分.

Phase1: 攻击者在本阶段申请电路 $(l', n, q, A_1, A_2, GateType) \to f$ 对应的私钥,要求 $f(x^*)=0$.下面模拟者利用 $g, g^{c_1},\ldots,g^{c_k}$, 分 3 种情况模拟节点 w 的密钥.需要指出的是,对于电路内部 $f_w(x^*)=1$ 的节点 w,其输出模拟为 $g_{j+1}^{sr_w}$, 其中,r_w 为 Z_p 上的随机值;而对于 $f_w(x^*)=0$ 的节点 w,其输出模拟为 $g_{j+1}^{sr_w}$, r_w 为 $c_1\ldots c_{j+1}$ 与一个随机值的和的形式.

Inputs:

(I) 当$(x^*)_w=1$ 时,随机选取 $r_w, z_w \in Z_p$, 模拟 w 点的密钥为

$$K_{w,1} = g^{r_w} h_w^{z_w}, K_{w,2} = g^{-z_w}.$$

(II) 当$(x^*)_w=0$ 时,随机选取 $\eta_w, \varphi_w \in Z_p$, 令 $r_w = c_1 c_2 + \eta_w, z_w = -c_2 + \varphi_w$, 模拟 w 点的密钥为

$$K_{w,1} = g^{r_w} h_w^{z_w} = g^{c_1 c_2 + \eta_w} (g^{y_w + c_1})^{(-c_2 + \varphi_w)}$$
$$= g^{-c_2 y_w + \eta_w + (y_w + c_1)\varphi_w} = (g^{c_1})^{-y_w} (g^{c_1})^{\varphi_w} g^{\eta_w + y_w \varphi_w},$$
$$K_{w,2} = g^{-z_w} = g^{c_2 - \varphi_w} = (g^{c_2}) g^{-\varphi_w}.$$

容易看出,模拟者利用已知信息,可在多项式时间模拟出 $K_{w,1}$ 和 $K_{w,2}$.由于随机数 η_w 和 φ_w 的参与,使得攻击者无法区分模拟的 $K_{w,1}$ 和 $K_{w,2}$ 和真实的 $K_{w,1}$ 和 $K_{w,2}$.

OR Gate: 不妨设 w 的深度 $depth(w)=j$,且密钥中的角标 $d_1, d_2 (1\leqslant d_1, d_2 \leqslant j-1)$ 与 $depth(A_1(w)), depth(A_2(w))$ 保持一致.

(I) 如果 $f_w(x^*)=1$,随机选取 $a_w^{(1)}, a_w^{(2)}, r_w \in Z_p$, 分以下 3 种情况模拟 w 的门密钥.

(1) $f_{A_1(w)}(x^*) = 0, f_{A_2(w)}(x^*) = 1$, 输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式:

$$r_{A_1(w)} = c_1 \ldots c_{d_1+1} + \eta_{A_1(w)}, r_{A_2(w)},$$

则对应的密钥模拟为

$$K_{w,1} = g_{j-d_1}^{a_w^{(1)}}, K_{w,2} = g_{j-d_2}^{a_w^{(2)}},$$

$$K_{w,3} = g_j^{r_w - a_w^{(1)} r_{A_1(w)}} = g_j^{r_w - a_w^{(1)}\left(c_1 \ldots c_{d_1+1} + \eta_{A_1(w)}\right)} = \left(g_j^{c_1 \ldots c_{d_1+1}}\right)^{-a_w^{(1)}} g_j^{r_w - a_w^{(1)} \eta_{A_1(w)}},$$

$$K_{w,4} = g_j^{r_w - a_w^{(2)} r_{A_2(w)}},$$

其中, $g_j^{c_1 \ldots c_{d_1+1}}$ 可以先后利用 $g^{c_1}, \ldots, g^{c_{d_1+1}}$ 做 $d_1 \left(1 \leqslant d_1 \leqslant j-1\right)$ 次对运算得到 $g_{d_1+1}^{c_1 \ldots c_{d_1+1}}$, 再与 g_{j-d_1-1} 做 1 次对运算得到.

(2) $f_{A_1(w)}(x^*) = 1, f_{A_2(w)}(x^*) = 0$, 输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式.

$$r_{A_1(w)}, r_{A_2(w)} = c_1 \ldots c_{d_2+1} + \eta_{A_2(w)},$$

则对应的密钥模拟为

$$K_{w,1} = g_{j-d_1}^{a_w^{(1)}}, K_{w,2} = g_{j-d_2}^{a_w^{(2)}},$$

$$K_{w,3} = g_j^{r_w - a_w^{(1)} r_{A_1(w)}},$$

$$K_{w,4} = g_j^{r_w - a_w^{(2)} r_{A_2(w)}} = g_j^{r_w - a_w^{(2)}\left(c_1 \ldots c_{d_2+1} + \eta_{A_2(w)}\right)} = \left(g_j^{c_1 \ldots c_{d_2+1}}\right)^{-a_w^{(2)}} g_j^{r_w - a_w^{(2)} \eta_{A_2(w)}},$$

其中, $g_j^{c_1 \ldots c_{d_2+1}}$ 可以先后利用 $g^{c_1}, \ldots, g^{c_{d_2+1}}$ 做 $d_2 \left(1 \leqslant d_2 \leqslant j-1\right)$ 次对运算得到 $g_{d_2+1}^{c_1 \ldots c_{d_2+1}}$, 再与 g_{j-d_2-1} 做 1 次对运算得到 $g_j^{c_1 \ldots c_{d_2+1}}$.

(3) $f_{A_1(w)}(x^*) = 1, f_{A_2(w)}(x^*) = 1$, 输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式.

$$r_{A_1(w)}, r_{A_2(w)}$$

则对应的密钥模拟为

$$K_{w,1} = g_{j-d_1}^{a_w^{(1)}}, K_{w,2} = g_{j-d_2}^{a_w^{(2)}}, \; K_{w,3} = g_j^{r_w - a_w^{(1)} r_{A_1(w)}}, K_{w,4} = g_j^{r_w - a_w^{(2)} r_{A_2(w)}}.$$

(II) 如果 $f_w(x^*)=0$,即 $f_{A_1(w)}(x^*) = f_{A_2(w)}(x^*) = 0$. 随机选取 $\varphi_w^{(1)}, \varphi_w^{(2)}, \eta_w \in Z_p$, 输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式为

$$r_{A_1(w)} = c_1 \ldots c_{d_1+1} + \eta_{A_1(w)}, \; r_{A_2(w)} = c_1 \ldots c_{d_2+1} + \eta_{A_2(w)}.$$

令 $a_w^{(1)} = c_{d_1+2} \ldots c_{j+1} + \varphi_w^{(1)}$, $a_w^{(2)} = c_{d_2+2} \ldots c_{j+1} + \varphi_w^{(2)}$, $r_w = c_1 \ldots c_{j+1} + \eta_w$, 模拟 w 点的密钥为

$$K_{w,1} = g_{j-d_1}^{a_w^{(1)}} = g_{j-d_1}^{c_{d_1+2} \ldots c_{j+1} + \varphi_w^{(1)}} = g_{j-d_1}^{c_{d_1+2} \ldots c_{j+1}} g_{j-d_1}^{\varphi_w^{(1)}},$$

$$K_{w,2} = g_{j-d_2}^{a_w^{(2)}} = g_{j-d_2}^{c_{d_2+2} \ldots c_{j+1} + \varphi_w^{(2)}} = g_{j-d_2}^{c_{d_2+2} \ldots c_{j+1}} g_{j-d_2}^{\varphi_w^{(2)}},$$

$$K_{w,3} = g_j^{r_w - a_w^{(1)} r_{A_1(w)}} = \left(g_j^{c_{d_1+2} \ldots c_{j+1}}\right)^{\eta_{A_1(w)}} \left(g_j^{c_1 \ldots c_{d_1+1}}\right)^{\varphi_w^{(1)}} g_j^{\eta_w - \varphi_w^{(1)} \eta_{A_1(w)}},$$

$$K_{w,4} = g_j^{r_w - a_w^{(w)} r_{A_2(w)}} = \left(g_j^{c_{d_2+2} \ldots c_{j+1}}\right)^{\eta_{A_2(w)}} \left(g_j^{c_1 \ldots c_{d_2+1}}\right)^{\varphi_w^{(2)}} g_j^{\eta_w - \varphi_w^{(2)} \eta_{A_2(w)}},$$

其中, $g_j^{c_1 \ldots c_{d_1+1}}$ 和 $g_j^{c_1 \ldots c_{d_2+1}}$ 可以利用(I)中的方式得到. $g_{j-d_1}^{c_{d_1+2} \ldots c_{j+1}}$ 先后利用 $g^{c_{d_1+2}}, \ldots, g^{c_{j+1}}$ 做 $j - d_1 - 1$ 次对运算得到. $g_{j-d_2}^{c_{d_2+2} \ldots c_{j+1}}$ 同理.而 $g_j^{c_{d_1+2} \ldots c_{j+1}}$ 在 $g_{j-d_1}^{c_{d_1+2} \ldots c_{j+1}}$ 的基础上与 g_{d_1} 做一次对运算得到. $g_j^{c_{d_2+2} \ldots c_{j+1}}$ 同理.

注意到(I)(II)中,从模拟者的角度来说,$K_{w,1}, K_{w,2}, K_{w,3}$ 和 $K_{w,4}$ 均是可模拟的.由于随机数 $\varphi_w^{(1)}, \varphi_w^{(2)}$ 的参与,使得从攻击者的角度来说,$K_{w,1}, K_{w,2}, K_{w,3}$ 和 $K_{w,4}$ 和真实的密钥无法区分.

AND Gate: 不妨设 w 的深度 $depth(w)=j$,且密钥中的角标 $d_1, d_2 \left(1 \leqslant d_1, d_2 \leqslant j-1\right)$ 与 $depth(A_1(w))$, $depth(A_2(w))$保持一致.

(I) 如果 $f_w(x^*)=1$,即 $f_{A_1(w)}(x^*) = f_{A_2(w)}(x^*) = 1$, 随机选取 $a_w^{(1)}, a_w^{(2)}, r_w, \in Z_p$, 模拟 w 点的密钥为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}},K_{w,2}=g_{j-d_2}^{a_w^{(2)}},\ K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}-a_w^{(2)}r_{A_2(w)}}.$$

(II) 如果 $f_w(x^*)=0$,分以下 3 种情况.

(1) $f_{A_1(w)}(x^*)=0, f_{A_2(w)}(x^*)=1$, 随机选取 $\varphi_w^{(1)},a_w^{(2)},\eta_w\in Z_p$, 输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式.

$$r_{A_1(w)}=c_1...c_{d_1+1}+\eta_{A_1(w)},r_{A_2(w)}.$$

令 $a_w^{(1)}=c_{d_1+2}...c_{j+1}+\varphi_w^{(1)},r_w=c_1...c_{j+1}+\eta_w$, 则对应的密钥模拟为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}}=g_{j-d_1}^{c_{d_1+2}\cdots c_{j+1}+\varphi_w^{(1)}}=g_{j-d_1}^{c_{d_1+2}\cdots c_{j+1}}\cdot g_{j-d_1}^{\varphi_w^{(1)}},$$

$$K_{w,2}=g_{j-d_2}^{a_w^{(2)}},$$

$$K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}-a_w^{(2)}r_{A_2(w)}}=g_j^{c_1\cdots c_{j+1}+\eta_w-\left(c_{d_1+2}\cdots c_{j+1}+\varphi_w^{(1)}\right)\left(c_1\cdots c_{d_1+1}+\eta_{A_1(w)}\right)-a_w^{(2)}r_{A_2(w)}}$$

$$=\left(g_j^{c_1\cdots c_{d_1+1}}\right)^{-\varphi_w^{(1)}}\left(g_j^{c_{d_1+2}\cdots c_{j+1}}\right)^{-\eta_{A_1(w)}}g_j^{\eta_w-\varphi_w^{(1)}\eta_{A_1(w)}-a_w^{(2)}r_{A_2(w)}},$$

其中, $g_{j-d_1}^{c_{d_1+2}\cdots c_{j+1}}$, $g_j^{c_1\cdots c_{d_1+1}}$ 和 $g_j^{c_{d_1+2}\cdots c_{j+1}}$ 可以采用前面叙述的方式得到.

(2) $f_{A_1(w)}(x^*)=1, f_{A_2(w)}(x^*)=0$, 随机选取 $a_w^{(1)},\varphi_w^{(2)},\eta_w\in Z_p$, 由输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式.

$$r_{A_1(w)},r_{A_2(w)}=c_1...c_{d_2+1}+\eta_{A_2(w)}.$$

令 $a_w^{(2)}=c_{d_2+2}...c_{j+1}+\varphi_w^{(2)},r_w=c_1...c_{j+1}+\eta_w$, 则对应的密钥模拟为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}},$$

$$K_{w,2}=g_{j-d_2}^{a_w^{(2)}}=g_{j-d_2}^{c_{d_2+2}\cdots c_{j+1}+\varphi_w^{(2)}}=g_{j-d_2}^{c_{d_2+2}\cdots c_{j+1}}\cdot g_{j-d_2}^{\varphi_w^{(2)}},$$

$$K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}-a_w^{(2)}r_{A_2(w)}}=g_j^{c_1\cdots c_{j+1}+\eta_w-a_w^{(1)}r_{A_1(w)}-\left(c_{d_2+2}\cdots c_{j+1}+\varphi_w^{(2)}\right)\left(c_1\cdots c_{d_2+1}+\eta_{A_2(w)}\right)}$$

$$=\left(g_j^{c_1\cdots c_{d_2+1}}\right)^{-\varphi_w^{(2)}}\left(g_j^{c_{d_2+2}\cdots c_{j+1}}\right)^{-\eta_{A_2(w)}}g_j^{\eta_w-a_w^{(1)}r_{A_1(w)}-\varphi_w^{(2)}\eta_{A_2(w)}},$$

其中, $g_{j-d_2}^{c_{d_2+2}\cdots c_{j+1}}$, $g_j^{c_1\cdots c_{d_2+1}}$ 和 $g_j^{c_{d_2+2}\cdots c_{j+1}}$ 可以采用前面叙述的方式得到.

(3) $f_{A_1(w)}(x^*)=0, f_{A_2(w)}(x^*)=0$, 随机选取 $\varphi_w^{(1)},\varphi_w^{(2)},\eta_w\in Z_p$, ,由输入中 $r_{A_1(w)}$ 和 $r_{A_2(w)}$ 对应的形式为

$$r_{A_1(w)}=c_1...c_{d_1+1}+\eta_{A_1(w)},\ r_{A_2(w)}=c_1...c_{d_2+1}+\eta_{A_2(w)}.$$

令 $a_w^{(1)}=2^{-1}c_{d_1+2}...c_{j+1}+\varphi_w^{(1)},a_w^{(2)}=2^{-1}c_{d_2+2}...c_{j+1}+\varphi_w^{(2)},r_w=c_1...c_{j+1}+\eta_w$, 则对应的密钥模拟为

$$K_{w,1}=g_{j-d_1}^{a_w^{(1)}}=g_{j-d_1}^{2^{-1}c_{d_1+2}\cdots c_{j+1}+\varphi_w^{(1)}}=\left(g_{j-d_1}^{c_{d_1+2}\cdots c_{j+1}}\right)^{2^{-1}}g_{j-d_1}^{\varphi_w^{(1)}},$$

$$K_{w,2}=g_{j-d_2}^{a_w^{(2)}}=g_{j-d_2}^{2^{-1}c_{d_2+2}\cdots c_{j+1}+\varphi_w^{(2)}}=\left(g_{j-d_2}^{c_{d_2+2}\cdots c_{j+1}}\right)^{2^{-1}}g_{j-d_2}^{\varphi_w^{(2)}},$$

$$K_{w,3}=g_j^{r_w-a_w^{(1)}r_{A_1(w)}-a_w^{(2)}r_{A_2(w)}}=g_j^{c_1\cdots c_{j+1}+\eta_w-\left(2^{-1}c_{d_1+2}\cdots c_{j+1}+\varphi_w^{(1)}\right)\left(c_1\cdots c_{d_1+1}+\eta_{A_1(w)}\right)-\cdots\left(2^{-1}c_{d_2+2}\cdots c_{j+1}+\varphi_w^{(2)}\right)\left(c_1\cdots c_{d_2+1}+\eta_{A_2(w)}\right)}$$

$$=\left(g_j^{c_1\cdots c_{d_1+1}}\right)^{-\varphi_w^{(1)}}\left(g_j^{c_{d_1+2}\cdots c_{j+1}}\right)^{-2^{-1}\eta_{A_1(w)}}\left(g_j^{c_1\cdots c_{d_2+1}}\right)^{-\varphi_w^{(2)}}\left(g_j^{c_{d_2+2}\cdots c_{j+1}}\right)^{-2^{-1}\eta_{A_2(w)}}g_j^{\eta_w-\varphi_w^{(1)}\eta_{A_1(w)}-\varphi_w^{(2)}\eta_{A_2(w)}},$$

其中, $g_{j-d_1}^{c_{d_1+2}\cdots c_{j+1}}$, $g_{j-d_2}^{c_{d_2+2}\cdots c_{j+1}}$, $g_j^{c_1\cdots c_{d_1+1}}$, $g_j^{c_1\cdots c_{d_2+1}}$, $g_j^{c_{d_1+2}\cdots c_{j+1}}$ 和 $g_j^{c_{d_2+2}\cdots c_{j+1}}$ 可以采用前面叙述的方式得到.

注意到(I)(II)中,从模拟者的角度来说,$K_{w,1}$、$K_{w,2}$ 和 $K_{w,3}$ 均是可模拟的.由于随机数 $\varphi_w^{(1)},\varphi_w^{(2)}$ 的参与,使得从攻击者的角度来说,$K_{w,1},K_{w,2},K_{w,3}$ 与真实密钥无法区分.

下面分两种情况模拟其他的辅助密钥.

(1) 当电路深度 $l'=l$ 时,按以下方式模拟“头部密钥”.

由前面的分析可以知道,由第 j 层 $f_w(x^*)=0$ 的节点可得 $r_w=c_1...c_{j+1}+\eta_w$, 则第 $l'=l$ 层所在的根节点对应的 $r_{n+q}=c_1...c_k+\eta_{n+q}$, 且 $\alpha=c_1...c_k+\xi$, 故“头部密钥”模拟为

$$K_H=g_{k-1}^{\alpha-r_{n+q}}=g_{k-1}^{\xi-\eta_{n+q}}.$$

(2) 当电路深度 $l'<l$ 时,则按以下方式模拟转换密钥.

电路的根节点在第 l'层,可知 $r_{n+q}=c_1...c_{l'+1}+\eta_{n+q}$, 随机选取 $\varphi_e,\eta_e\in Z_p$,令 $a_e=c_{l'+2}...c_{l+1}+\varphi_e, r_e=c_1...c_{l+1}+\eta_e$, 则对应的转换密钥模拟为

$$K_{e,1}=g_{l-l'}^{a_e}=g_{l-l'}^{c_{l'+2}...c_{l+1}+\varphi_e}=g_{l-l'}^{c_{l'+2}...c_{l+1}}\cdot g_{l-l'}^{\varphi_e},$$

$$K_{e,2}=g_l^{r_e-a_e r_{n+q}}=g_l^{c_1...c_{l+1}+\eta_e-(c_{l'+2}...c_{l+1}+\varphi_e)(c_1...c_{l'+1}+\eta_{n+q})}$$

$$=\left(g_l^{c_1...c_{l'+1}}\right)^{-\varphi_e}\left(g_l^{c_{l'+2}...c_{l+1}}\right)^{-\eta_{n+q}}g_l^{\eta_e-\varphi_e\eta_{n+q}}.$$

由于 $l'<l$, $g_l^{c_1...c_{l'+1}}$ 可以先后利用 $g^{c_1},...,g^{c_{l'+1}}$ 做 l'次对运算得到 $g_{l'+1}^{c_1...c_{l'+1}}$, 若下角标未达到 l,则再与 $g_{l-l'-1}$ 做 1 次对运算得到 $g_l^{c_1...c_{l'+1}}$. $g_l^{c_{l'+2}...c_{l+1}}$ 同理.

按以下方式模拟头部密钥.

由 $r_e=c_1...c_k+\eta_e, \alpha=c_1...c_k+\xi$, 则此时头部密钥模拟为

$$K_H=g_{k-1}^{\alpha-r_e}=g_{k-1}^{\xi-\eta_e}.$$

注意到,从模拟者的角度来说,$K_{e,1},K_{e,2}$ 和 K_H 均可在多项式时间计算得到.由于随机数的参与,使得从攻击者的角度来说,$K_{e,1},K_{e,2},K_H$ 和真实的方案无法区分.

最后,模拟者将上述模拟的所有节点密钥以及辅助密钥发送给攻击者.

Challenge: 令 S^*为满足 $x_i^*=1\,(i\in[1,n])$ 的角标 i 所构成的集合.本阶段模拟者接收到攻击者提交的两个明文 m_0,m_1,然后模拟者随机选取 $b\in\{0,1\}$,生成挑战密文:

$$CT=(m_b\cdot T\cdot g_k^{s\xi}, g^s, \forall j\in S^*\ \ C_j=(g^s)^{y_j}).$$

Phase2: 与 Phase1 相同.

Guess: 攻击者给出对 b 的猜测 b'.如果 $b=b'$,则模拟者判定 $T=g_k^{s\prod_{j\in[1,k]}c_j}$, 否则判定 T 为 G_k上的随机数(设为 $g_k^z, z\in Z_p$).

最后我们来计算模拟者判定成功的优势,假设攻击者以ε的优势赢得了游戏,则有:

Pr[模拟者判定正确]

$=\Pr[\text{模拟者判定}T=g_k^{sc_1...c_k}\mid T=g_k^{sc_1...c_k}]\cdot\Pr[T=g_k^{sc_1...c_k}]+\Pr[\text{模拟者判定}T=g_k^z\mid T=g_k^z]\cdot\Pr[T=g_k^z]$

$=\Pr[b'=b\mid T=g_k^{sc_1...c_k}]\cdot\Pr[T=g_k^{sc_1...c_k}]+\Pr[b\neq b\mid T=g_k^z]\cdot\Pr[T=g_k^z]$

$=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\times\frac{1}{2}$

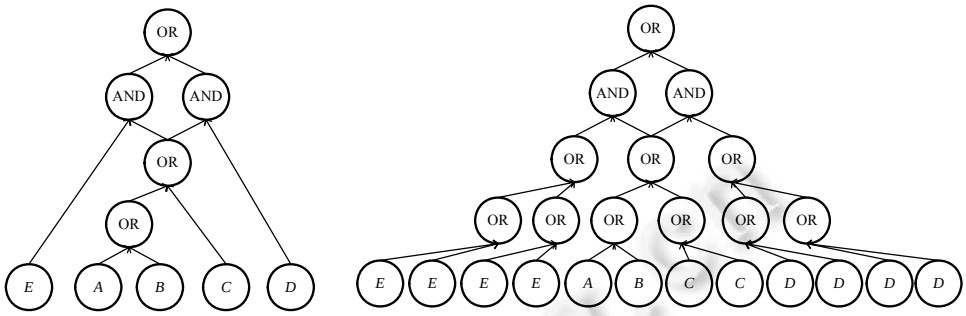
$=\frac{1}{2}+\frac{\varepsilon}{2}.$

由以上分析可知,若存在一个优势为ε的多项式时间攻击者赢得了上述游戏,则存在一个模拟者以$\varepsilon/2$ 的优势解决 K-MDDH 问题.故本节提出的 KP-ABE 方案在 K-MDDH 假设下是选择安全的.

3 方案对比

本文与文献[4,6,12,14]相比,优化了原有电路的结构,实现了跨层输出和层数的选择,对于单个用户来说,层数选择的优势在于,访问结构的选择更加灵活,当用户需要比较简单的访问结构时,不必受系统深度的限制,增加不必要的无效节点,从而增大不必要的存储量和计算量;跨层输出的优势在于,当用户需要关系比较复杂、规模比较大的访问结构时,可以节省中间很多用来填充中间层的节点.而对于系统整体来说,因为需要考虑到所有用户,最大深度设置的会比较大,因此当用户量十分庞大时,这样的优势积累是十分明显的.

下面举一个简单的实例加以说明,对于$((A\cup B)\cup C)\cap(E\cup D)$这样一个表达式,可以用如图 3(a)所示的电路结构直接进行表示.



(a) 直接表示 (b) 等效电路

Fig.3

图 3

而由于原方案[4]并不支持跨层输出的性质,故该电路结构并不能直接应用至方案中,需要对其进行等价转换,即采用 $X \cup X$ 这样的结构来填充跨层的线路,最终的等效结构如图 3(b)所示.可以发现,电路的总节点数急剧增加,由原来的 10 个节点,增加到 24 个节点;总密钥量由 28(2×5+4×3+3×2),增加到 70(2×12+4×10+3×2),单从跨层优化的角度来看,在这样一个简单电路下,本方案比原方案密钥存储和解密计算效率均提升了 60%,并且对于一般的表达式来说,其电路结构均易出现跨层的情况,对于一般情况,效率的提升也比较明显.

上面仅仅考虑的跨层的情况,对于电路层数来说,当系统初始化时设置的深度与该电路的深度不一致时,还需要增加电路的深度,即在输出处增加两个深度之差个节点.前面已经提到,对于系统来说,需要考虑到所有用户,一般系统深度会设置的比较大,这里我们假设系统深度为 10,上述电路深度为 5,故原方案中需要增加 5 个节点,即增加密钥的数量为 10,这种情况下本方案存储和计算效率提升约为 35%(相对于原始电路密钥量 28),一般而言,电路中包含的属性越多,电路深度值越大.

以上考虑的是单个用户的情况,在云系统海量用户的积累下,优化效果将更加明显.下面我们分别从跨层输出和层数选择两方面,以表 1 总结以上举例对比.

Table 1 Summarize of optimization

表 1 优化小结

图 3	跨层输出(密钥量)	层数选择(实际深度/系统深度)
原方案	70	10/10
本方案	28	5/10
效率提升 (%)	60	35

下面我们将本文方案与文献[4,6,12,14]中提出的方案进行对比.设系统属性个数为 n,加密时密文中包含的属性个数为 a,系统规定的最大电路深度为 l,用户私钥相关的电路深度为 l',则各方案对比结果见表 2.

Table 2 Results of comparison

表 2 方案对比结果

方案	公共参数	密文量	电路参数规模			电路层数	是否支持跨层	映射
			Input	OR	AND			
Garg 方案[4]	n+2	a+3	2	4	3	l	否	多线性映射
Kangro 方案[6]	n+2	a+3	2	3	2	l	否	多线性映射
Xu 方案[14]	n+2	a+3	2	3	3	l	否	多线性映射
Ferucio 方案[12]	n+2	a+3				l'	是	双线性映射
本文方案	n+2	a+3	2	4	3	$l'(1<l'\leqslant l)$	是	多线性映射

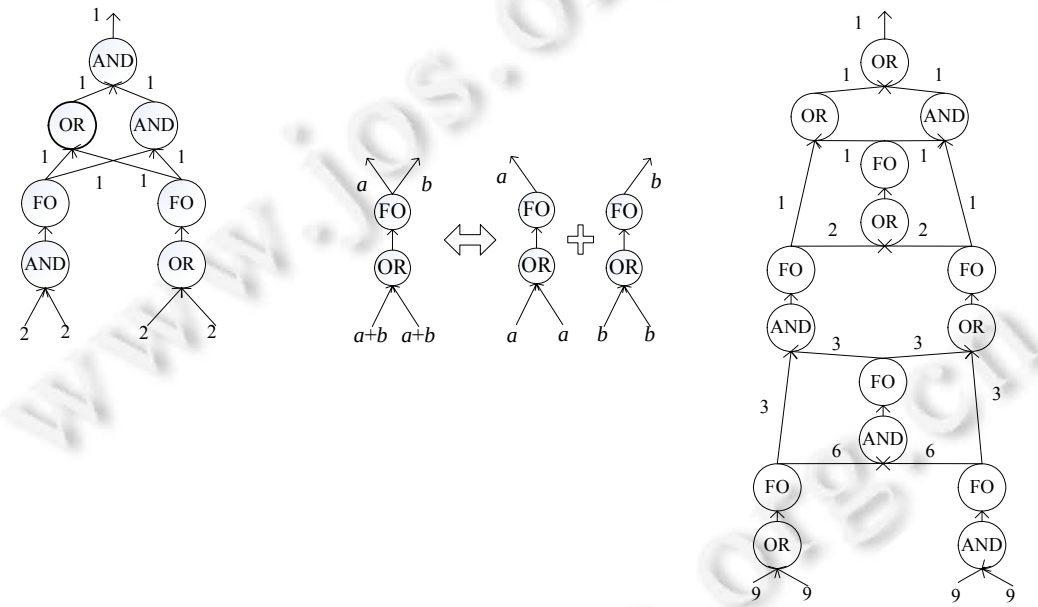
注:表 2 中公共参数、密文量和密钥量各元素所在群的元素个数,密钥量仅比较每个 Input、OR 和 AND 节点对应的密钥量,这里我们将群描述和访问结构按 1 个单位计.由于 Xu 方案附带其他功能,这里仅计算其中基础方案的各项指标.

由表 2 中我们可以发现,本方案与文献[4,6,14]中方案采用的处理方式相近,从单个门的密钥量而言,Kangro

方案最优,Xu 方案其次,本方案与 Garg 方案一致但从跨层和层数可以节省大量门节点和计算量的角度考虑,在许多电路中,可以达到甚至超越 Kangro 方案的效果;从实现的访问结构的表达能力来说,本方案最优,Garg 方案、Xu 方案、Kangro 方案一致.需要提到的是,由于参数设置的问题,Kangro 方案和 Xu 方案并不能扩展为跨层电路,但可以采用本文提出的电路等价转换的方法将其修改为支持层数小于等于 l 的电路,在此不做详细介绍.

文献[12]中的方案与其他方案的设计思想相差较大,无法在表中做出统一比较,下面我们给出不同情况下的比较结果.

文献[12]中的方案基于双线性映射,采用 Goyal 方案的思想和 FANOUT 门(简称 FO 门)的概念,且密钥仅在电路最底端和 FO 门中生成.可以认为其方案将多个节点利用 FO 门,合并为一个节点来实现单个节点的多输出功能(如图 4(a)所示),在多输出节点无串联的电路中(如图 4(b)所示,底部数字为各输入处的密钥量),效率与 Goyal 方案等价.当电路中存在多输出串联的情况时(如图 4(c)所示,底部数字为各输入处的密钥量),其密钥量将呈线性增长.



(a) 利用 FO 门合并节点 (b) 多输出并联 (c) 多输出串联

Fig.4

图 4

从图 4(c)中容易发现,一旦出现多个多输出门串联的情况,密钥量增长速度将非常快.根据文献[12]可以计算出,除 36 个输入处的密钥外,每个 FO 门还产生 2 个门密钥,密钥长度为 48.而利用本文方案根据各个门的类型不同,密钥长度为 40.与文献[12]相比,本方案对多输出串联电路具有较高的有较高的执行效率.在实际情况中,可以根据具体情况决定使用哪一种方案.

4 结束语

本文在 Garg 方案的基础上提出了一个新的实现一般电路的 KP-ABE 方案,并基于 k-多线性判定性 Diffie-Hellman(K-MDDH)假设证明了该方案具有选择安全性,与已有的基于多线性映射的 KP-ABE 方案对比,该方案实现的一般电路的表达能力更强,应用范围更广,效率更高.目前,实现一般电路的 ABE 方案代价仍然很大,如何设计高效简洁的方案,将是今后亟需解决的问题.

致谢 审稿专家和编辑老师为本文提出了宝贵的修改建议,在此表示衷心的感谢.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the EUROCRYPT 2005. Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

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

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

[4] Garg S, Gentry C, Halevi S, Sahai A, Waters B. Attribute-Based encryption for circuits from multilinear maps. In: Canetti R, Garay JA, eds. Advances in Cryptology CRYPTO 2013. LNCS 8043, Springer-Verlag, 2013. 479−499. [doi: 10.1007/978-3-642-40084-1_27]

[5] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices. In: Proc. of the EUROCRYPT 2013. LNCS 7881, Springer-Verlag, 2013. 1−17. [doi: 10.1007/978-3-642-38348-9_1]

[6] Kangro K. On attribute-based encryption for circuits from multilinear maps [Bachelor Thesis]. Faculty of Mathematics and Computer Science, Institute of Computer Science, University of Tartu, 2013. http://comserv.cs.ut.ee/forms/ati_report/downloader.php?file=C586399CB9A43098CC0FF1BE9F33FC0218BEC3AE

[7] Stinson D. Cryptography: Theory and Practice. 3rd ed., CRC Press, 2005.

[8] Osreovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. ACM Press, 2007. 195−203. [doi: 10.1145/1315245.1315270]

[9] Bellare M, Hoang VT, Rogaway P. Foundations of garbled circuits. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM Press, 2012. 784−796. [doi: 10.1145/2382196.2382279]

[10] Boneh D, Franklin MK. Identity-Based encryption from the Weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. on Advances in Cryptology. Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[11] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Technion-Israel Institute of Technology, Faculty of Computer Science, 1996.

[12] Ţiplea FL, Drăgan CC. Key-Policy attribute-based encryption for Boolean circuits from bilinear maps. In: Ors B, Preneel B, eds. Cryptography and Information Security in the Balkans. LNCS 9024, Springer-Verlag, 2015. 175−193. [doi: 10.1007/978-3-319-21356-9_12]

[13] Xu J, Wen QY, Li WM, Jin ZP. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. IEEE Trans. on Parallel and Distributed Systems, 2015, 119−129. [doi: 10.1109/TPDS.2015.2392752]

[14] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the Public Key Cryptography 2011. LNCS 6571, Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

胡鹏(1992－),男,江西南昌人,硕士生,主要研究领域为公钥密码.

高海英(1978－),女,博士,副教授,主要研究领域为密码理论.