快速解密且私钥定长的密文策略属性基加密方案

李 龙[①] 古天龙[②] 常 亮*[③] 徐周波[③] 钱俊彦[③]

[①](桂林电子科技大学机电工程学院 桂林 541004)

[②](广西信息科学实验中心(桂林电子科技大学) 桂林 541004)

[③](广西可信软件重点实验室(桂林电子科技大学) 桂林 541004)

摘 要：在保证密文策略属性基加密(CP-ABE)算法安全性的前提下，尽可能地提升其工作效率一直是密码学领域的研究热点。该文从作为 CP-ABE 效率核心的访问结构着手，首次提出基于简化有序二叉决策图(ROBDD)的访问结构，给出了相应的策略表示方法、用户可满足性判定；基于简化有序二叉决策图(ROBDD)访问结构设计了在算法时间复杂度、存储空间占用量等方面都具有较好表现的 CP-ABE 方案；在安全性方面，该方案能够抵抗用户间的合谋攻击和选择明文攻击。对比分析表明，ROBDD 访问结构具有更强的表达能力和更高的表达效率；新的 CP-ABE 方案包含时间复杂度为常数阶的密钥生成算法、解密算法，能够为用户生成定长私钥并实现快速解密。

关键词：密文策略属性基加密；二叉决策图；访问结构；快速解密

中图分类号： TP309 **文献标识码**： A **文章编号**： 1009-5896(2018)07-1661-08

DOI: 10.11999/JEIT171086

Expressive Ciphertext-policy Attribute-based Encryption Scheme with Fast Decryption and Constant-size Secret Keys

LI Long[①] GU Tianlong[②] CHANG Liang[③] XU Zhoubo[③] QIAN Junyan[③]

[①](*School of Electromechanical Engineering*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

[②](*Guangxi Experiment Center of Information Science*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

[③](*Guangxi Key Laboratory of Trusted Software*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: Under the premise of ensuring the security of Ciphertext-Policy Attribute Based Encryption (CP-ABE), to enhance efficiency as much as possible is always a research hotspot in the field of cryptography. Starting from the access structure, which is the efficiency basis of CP-ABE, a new kind of access structure is proposed based on Reduced Ordered Binary Decision Diagrams (ROBDD) for the first time, and the corresponding strategy representation method and satisfaction determination are given. Furthermore, based on the above access structure, a new CP-ABE with good performance in lots of aspects, such as time complexity of algorithms and storage occupancy of secret keys, is designed; In terms of security, the scheme can resist collusion attack and chosen plaintext attack. Comparative analysis shows that, ROBDD access structure has stronger expression ability and higher expression efficiency; In the new CP-ABE scheme, the time complexity of key generation algorithm and decryption algorithm is $O(1)$, which can generate constant-size secret keys and achieve fast decryption.

Key words: Ciphertext-Policy Attribute-Based Encryption (CP-ABE); Binary decision diagram; Access structure; Fast decryption

收稿日期：2017-11-20；改回日期：2018-04-13；网络出版：2018-05-11

*通信作者：常亮 changl@guet.edu.cn

基金项目：国家自然科学基金(U1501252, 61572146, 61562015, U1711263, 61561016)，广西重点研发计划(AC16380014, AA17202048)，广西自然科学基金(2016GXNSFDA380006, 2017GXNSFAA198283)，桂林电子科技大学创新团队项目

Foundation Items: The National Natural Science Foundation of China (U1501252, 61572146, 61562015, U1711263, 61561016), The Key Research and Development Program of Guangxi (AC16380014, AA17202048), The Natural Science Foundation of Guangxi (2016GXNSFDA380006, 2017GXNSFAA198283), The Program for Innovative Research Team of Guilin University of Electronic Technology

1 引言

在当前被广泛研究并付诸实践的共享存储、云计算等网络场景中，用户量及数据量较为巨大、数据提供者与使用者间关系复杂，因此将传统公钥加密策略应用于此类场景时将导致系统工作效率低，系统维护开销大，甚至出现系统无法正常工作的情况，给信息的安全传输及高效的访问控制带来了较大挑战，因此属性基加密(Attribute Based Encryption, ABE)应运而生。

ABE 由 Sahai 等人[1]基于身份基加密(Identity Based Encryption, IBE)提出，随后被扩展为密文策略属性基加密(Ciphertext Policy ABE, CP-ABE)[2]和密钥策略属性基加密(Key Policy ABE, KP-ABE)[3]。其中，CP-ABE 的核心思想是，加密方制定隐私策略并借助于访问结构(即公钥)完成信息加密，解密方只有在拥有满足该访问结构的属性集合(即私钥)时才能解密成功，因此能够同时实现数据加密和访问控制。此类方案较好地解决了将传统公钥加密应用于新型网络场景中时所遇到的系统开销大，数据使用者信息无法预先获取，公私钥一一对应等问题，具有更强的适用性[4]。

在 CP-ABE 中，访问结构作为核心基础部件，对 CP-ABE 的功能实现、性能表现等方面均具有较大影响。Waters[5]基于 LSSS 结构及多种困难性假设构造了多个 CP-ABE 方案，此类方案在密文及私钥尺寸等方面有所改进，但任一属性在访问策略中允许出现至多一次，降低了访问策略的表达能力，虽然文章提出了针对性的解决方法，但方案性能表现会相应降低；Cheung 等人[6]提出了 CPA 安全的 CP-ABE 方案，并分别借助于层级结构、Canetti-Halevi-Katz 技术在效率和安全性方面进行了研究，但方案中的访问结构采用 AND 门，仅支持属性间的 AND 操作，表达能力弱；Balu 等人[7]借助于 LISS 技术将访问策略表述为分布矩阵构造了选择性安全的 CP-ABE 方案，该方案支持属性在访问结构中的多次出现，但被加密的信息须是区间 $\left[-2^l, 2^l\right]$ 内的整数；Rao 等人[8]针对密钥更新问题，提出了能够实现属性级更新的动态 CP-ABE 策略，但其访问结构为限门结构，本质上仅支持属性间的 AND 和 OR 两种操作；针对单授权中心带来的系统可靠性低问题，赵志远等人[9]提出了一种多中心 CP-ABE，方案具有定长密文、高效解密等优势，但其中所采用的访问结构仅支持 AND 操作；Zhang 等人[10]提出了一个多属性机构环境下的属性基认证密钥交换协议，一定程度上解决了跨域访问中的安全问题，但是方案中的加密算法复杂度、密钥尺寸等受限于属性数量；文献[11]提出了隐私保护且密文定长的 CP-ABE，但仅支持合取范式表示的访问策略；文献[12]融合单调张成矩阵与 CP-ABE 机制，实现了属性撤销及共谋抵抗机制；文献[13]针对 CP-ABE 中的密钥管理问题，基于属性分层提出了一种能够实现权限委派的方案；文献[14]着眼于用户撤销问题，通过引入用户群组的概念并借助与外包计算，提出了一种灵活细粒度的 CP-ABE 方案；Wang 等人[15]将策略中的二值属性扩展为多值属性，增强了策略表达能力，并基于此提出了高效安全的方案；Smari 等人[16]提出了一种更加通用的访问结构，并将其应用于高性能分布式协同环境中。可见，对 CP-ABE 的研究主要集中于功能增强和性能提升两个方面，而且 CP-ABE 方案中往往存在着访问结构表达能力与方案性能(加密效率、密文尺寸、密钥尺寸、解密效率等)间的矛盾，限制了方案的适用性和可扩展性。

简化有序二叉决策图(Reduced Ordered Binary Decision Diagrams, ROBDD)不但能够实现对任意布尔函数的极简表示[17]，还能高效完成布尔变量及函数间的任意布尔操作[18]，是一种作为访问结构完成策略表示的理想选择。因此，本文基于 ROBDD 提供了一种灵活高效的 CP-ABE 设计。首先，提出了基于 ROBDD 的访问结构，对与之相关的策略表示方法、用户可满足性判定进行了形式化表述；该访问结构具备更强表达能力及扩展性，能够在不增加系统开销的情况下同时支持属性正负取值，能够支持属性的多次出现，能够完成与或非等属性间的所有布尔操作。进一步地，基于 ROBDD 设计完成了一种 CP-ABE 策略，该策略在算法时间复杂度、存储空间占用量等方面表现良好，尤其是私钥占用空间极小且定长、能够实现快速解密。此外，该策略能够抵抗解密用户间的合谋攻击，并且是 CPA 安全的。

2 背景知识

2.1 访问结构

本质上而言，访问策略是一条根据输入属性集合 S 无异议地得出 1 或 0 的规则 R，只有当 R 返回 1 时，称 S 满足 R，记为 $S \vDash R$；否则称 S 不满足 R，记为 $S \nvDash R$。

访问结构是访问策略的直观表达，具体表现形式有陷门[2,3,7–9]、与门[6,15,18]等，不同表现形式具备不同的数学表达，如陷门将访问策略描述为集合间的元素匹配。

2.2 CP-ABE 框架

CP-ABE 框架包含 4 个算法：

Setup 算法：由授权中心执行以生成系统公钥 PK 及主密钥 MK 。

Encrypt 算法：由数据拥有者执行以加密数据。

Keygen 算法：由授权中心根据用户属性集生成私钥 SK 。

Decrypt 算法：由数据使用者执行以解密数据。

2.3 针对 CP-ABE 的 CPA 安全游戏

定义 1　CP-ABE 策略的 CPA 安全性：若不存在概率多项式时间敌手能够以不可忽略的优势赢得如下 CPA 游戏，则称该 CP-ABE 策略是 CPA 安全的。

Initial：敌手选择访问结构 AS 并提交给挑战者；

Setup：挑战者运行 CP-ABE 中的 **Setup** 算法，将 PK 传递给敌手；

Phase 1：敌手提交属性集 S 进行私钥询问，其中 $S \nvDash \mathrm{AS}$ 。该过程是可重复的；

Challenge：敌手提交等长明文 M_0 ， M_1 给挑战者，挑战者随机选择 $\mu \in \{0,1\}$ 并借助于 AS 加密明文 M_μ ，得到密文 CT 并发送给敌手；

Phase 2：同 **Phase 1**；

Guess：敌手猜测 μ 的值为 μ' 。

敌手 A 在上述 CPA 安全游戏中的优势定义为：$\mathrm{Adv}_{\text{CP-ABE}}^{\text{CPA}}(A) = \left|\Pr[\mu = \mu'] - 1/2\right|$ 。

2.4 双线性映射及双线性群

定义 2　双线性映射：存在素数阶为 p 的群 G_0 ， G_1 ，群 G_0 的生成元为 g ，若具有以下性质，则称 $e: G_0 \times G_0 \to G_1$ 为双线性映射：

(1)双线性性：对于任意 $u, v \in G_0$ 及 $a, b \in Z_p$ ，满足 $e\left(u^a, v^b\right) = e(u,v)^{ab}$ ；

(2)非退化性： $e(g,g) \neq 1$ 。

定义 3　双线性群：若 G_0 内运算及 $e: G_0 \times G_0 \to G_1$ 均具备可计算性，则称 G_0 为双线性群。

2.5 DBDH 假设

存在双线性映射 $e: G_0 \times G_0 \to G_1$ ，随机选取 $a, b, c, z \in Z_p$ ，给定 $g, g^a, g^b, g^c \in G_0$ ，将敌手 A 在解决 DBDH(Decisional Bilinear Diffie-Hellman)问题时的优势定义为

$$\mathrm{Adv}_{\mathrm{DBDH}}^{G_0}(A) = \left|\Pr\left[A\left(g, g^a, g^b, g^c, e(g,g)^{abc}\right)=1\right] - \Pr\left[A(g, g^a, g^b, g^c, e(g,g)^z) = 1\right]\right|$$

对于任意多项式时间敌手 A ，若 $\mathrm{Adv}_{\mathrm{DBDH}}^{G_0}(A)$ 是可忽略的，则称 DBDH 假设成立。

2.6 简化有序二叉决策图

简化有序二叉决策图(ROBDD)是规定变量序并简化之后的二叉决策图(Binary Decision Diagram, BDD)，与此相关的研究可追溯至 Akers[17], Drechsler[18]。

定义 4　BDD：对于从 $\{0,1\}^n$ 到 $\{0,1\}$ 的布尔函数 $f(x_1, x_2, \cdots, x_n)$ ，BDD 是用于表示布尔函数族 $\#f(x_1, x_2, \cdots, x_n)$ 的一个有向无环图，它满足：

(1)包含根结点 root 、终结点和内部结点 3 类结点；

(2)终结点 $\boxed{0}$ 和 $\boxed{1}$ ，分别表示布尔常量 0 和 1 ；

(3)每个非终结点 u 具有 4 属性(f^u,var,low, high)，其中， f^u 表示结点 u 所对应的布尔函数， $f^u \in \#_\pi f(x_1, x_2, \cdots, x_n)$ (若 u 是根结点，则 $f^u = f(x_1, x_2, \cdots, x_n)$)； var 表示 u 的标记变量；low 表示 u 的 0 分枝子结点； high 表示 u 的 1 分枝子结点；

(4)每个非终结点 u 具有与 u.low 和 u.high 的连接弧，分别称为 0 -边和 1 -边，分别用虚线、实线表示；

(5)在 BDD 的任一有向路径上，每个变量至多出现一次。

定义 5　OBDD：在 BDD 中，若任一有向路径上的变量 $x_1, x_2, \cdots, x_n$ 均以变量序 π 所规定的次序依次出现，则称该 BDD 为 OBDD(Ordered Binary Decision Diagram)。

定义 6　ROBDD：若 OBDD 内部结点满足：

(1)对于结点 u ， u.low $\neq$ u.high ；

(2)对于结点 u 和 v ，满足 (u.low $\neq$ v.low) $\vee$ (u.high $\neq$ v.high) $\vee$ ((u.low $\neq$ v.low) $\wedge$ (u.high $\neq$ v.high))；则称该 OBDD 为 ROBDD。

3　基于 ROBDD 的 CP-ABE 策略

本节主要对基于 ROBDD 设计完成的访问结构、CP-ABE 策略及其安全证明进行阐述。

3.1 ROBDD 访问结构

ROBDD 访问结构能够支持正值属性及负值属性，可实现属性间的与、或、非等任意布尔操作，能够完成对访问策略的灵活高效表达。根据访问策略生成 ROBDD 访问结构的过程主要包含以下步骤。

3.1.1 访问策略的布尔函数表示　首先将访问策略中的各个属性使用变量 $x_i (1 \le i \le n)$ 表示，其中 n 为属性总量，继而将使用自然语言描述的访问策略转换为布尔函数表示 $f(x_1, x_2, \cdots, x_n)$ 。其中需要指出的是限门运算的布尔函数表达：

限门运算简记为 $T(t,n)$，表示拥有 n 个属性中任意 t 个元素时便能完成限门运算 $T(t,n)$。关于 $T(t,n)$ 的布尔函数表达，首先任意选取 t 个互不相同的属性构成组合，根据组合数公式可知此类组合共有 $C(n,t)$ 个，记为 $\mathrm{Com}_1,\mathrm{Com}_2,\cdots,\mathrm{Com}_{C(n,t)}$；对 $C(n,t)$ 个组合中分别包含全部元素进行合取操作，将结果记为 $\mathrm{Con}_1,\mathrm{Con}_2,\cdots,\mathrm{Con}_{C(n,t)}$；将 $C(n,t)$ 个结果进行析取操作，得出 $T(t,n)$ 的布尔函数表达，记为 $f(t,n)=\vee_{i=1}^{C(n,t)}\mathrm{Con}_i$。

3.1.2 布尔函数的 ROBDD 表示 根据布尔函数构造其 ROBDD 表示的算法如表 1 所示。

由上而下、从左至右对所有结点编号，最终得到 $\mathrm{ROBDD}=\left\{\mathrm{Node}_{\mathrm{id}}^{i}|\mathrm{id}\in\mathrm{ID},i\in I\right\}$，其中 ID 为非终结点编号之集合，$I$ 为变量之集合。$\mathrm{Node}_{\mathrm{id}}^{i}$ 可使用 4 元组 $<\mathrm{id},i,\mathrm{high},\mathrm{low}>$ 表示，id 为结点编号，i 为属性编号，high 为 1 -边结点编号，low 为 0 -边结点编号。终结点 $\boxed{0}$，$\boxed{1}$ 的编号为 0 和 1。

表 1 ROBDD的构造算法

输入：布尔函数 f 及变量最大编号 $n-1$。
输出：布尔函数 f 在变量序 $\pi:x_0<x_1<\cdots<x_{n-1}$ 下的 ROBDD表示。

```
(1)  # define max  n-1
(2)  node* Construct-step(char  *f , int  i );
(3)  node* Construct(char  *f ) {
(4)    int  i = 0 ;
(5)    node  *u ;
(6)    Empty the computed table;
(7)    return (u=Construct-step( f,i ));
(8)  }
(9)  node* Construct-step(char  *f , int  i ) {
(10)   static int  id = 1 ;
(11)   node  *u, * v0, * v1 ;
(12)   if ( i > max ) {
(13)     if ( *f == "0" )  u → id = 0 ;
(14)     else      u → id = 1 ;
(15)     return  u ;
(16)   }
(17)   else {
(18)     v0=Construct-step(f_{x_i=0}, i+1) ;
(19)     v1=Construct-step(f_{x_i=1}, i+1) ;
(20)     if ( v0 = v1 )   return v0;
(21)     else if computed-table entry  (v0, v1, u) exists
         return  u ;
(22)       u → index = i ;
(23)       u → id = + + id ;
(24)       u → low = v0 ;
(25)       u → high = v1 ;
(26)       Store  (v0, v1, u)  in computed table;
(27)       return  u ;
(28)     }
(29) }
```

定义 7 有效路径：在 ROBDD 结构中，根结点 root 与终结点 $\boxed{1}$ 间的任意路径均称为有效路径。

定义 8 对 ROBDD 结构的满足性：若属性集 S 中能够与 ROBDD 结构中的任意有效路径相匹配，则称属性集 S 满足访问结构 ROBDD，记为 $S\vDash\mathrm{ROBDD}$。

例 1 根据访问策略构造 ROBDD 结构。给定访问策略：拥有属性 x_0 或属性 (x_1,x_2,x_3) 中的任意两个属性的用户能够完成解密。

(1)根据访问策略得出布尔函数 $f_1(x_0,x_1,x_2,x_3)=x_0+x_1x_2+x_1x_3+x_2x_3$；

(2)在变量序 $\pi:x_0<x_1<x_2<x_3$ 下根据算法 1 构造 ROBDD 表示；随后对结点进行编号得到图1所示的 ROBDD 访问结构，其数学表达式为 $\mathrm{ROBDD}=\left\{\mathrm{Node}_2^0,\mathrm{Node}_3^1,\mathrm{Node}_4^2,\mathrm{Node}_5^2,\mathrm{Node}_6^3\right\}$。

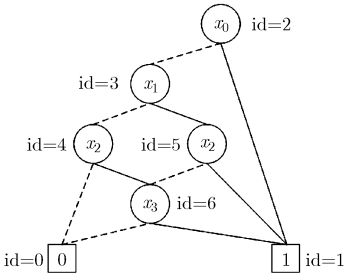


图 1 布尔函数 $f_1(x_0,x_1,x_2,x_3)$ 的 ROBDD 表示

3.2 基于 ROBDD 的 CP-ABE 结构

本文提出的 CP-ABE 方案支持正值属性 i 和负值属性 $\neg i$，为了叙述方便，参考文献[6]使用统一标识 $\underline{i}$ 表示属性的两种取值。假设系统属性集 N 中含 n 个元素，编号为 $\{0,1,\cdots,n-1\}$。

本文提出的基于 ROBDD 访问结构的 CP-ABE 方案包含以下算法：

Setup 算法：由授权中心执行：选择阶为 p 的双线性群 G_0，生成元为 g，定义双线性映射 $e:G_0\times G_0\to G_1$；随机选择 Z_p 中的元素 $y,t_0,t_1,\cdots,t_{n-1},t_0^{'},t_1^{'},\cdots,t_{n-1}^{'}$。令 $Y=e(g,g)^y$，$T_i=g^{t_i}(i\in N)$，$T_i^{'}=g^{t_i^{'}}(i\in N)$，生成系统公钥 $\mathrm{PK}=<e,g,Y,\left\{\left(T_i,T_i^{'}\right)\middle|i\in N\right\}>$ 及主密钥 $\mathrm{MK}=<y,\left\{\left(t_i,t_i^{'}\right)\middle|i\in N\right\}>$。

Encrypt(PK, M, ROBDD)算法：由数据拥有者使用 ROBDD 访问结构加密数据 $M\in G_1$。假设

ROBDD 中有效路径的总数为 $T\left(1\le T\le 2^{|I|}-1\right)$，表示为 $R=(R_0,R_1,\cdots,R_{T-1})$。加密操作如下：

随机选择 $s\in Z_p$ 并计算 $\widetilde{C}=M\cdot Y^s$，$\widehat{C}=g^s$，$C_{R_t}=\left(\prod_{i\in I_t}\underline{T_i}\right)^s=g^{\left(\sum_{i\in I_t}\underline{t_i}\cdot s\right)}$，其中 I_t 为 R_t 上所包含属性之集合。生成密文为

$$\text{CT}=<\text{ROBDD},\widetilde{C},\widehat{C},\left\{C_{R_t}|R_t\in R\right\}>$$

在上述加密算法中，主要的计算量为群 G_0 中的 $T+1$ 次指数运算和 $\sum_{0\le t\le(T-1)}(I_t-1)$ 次乘法运算、群 G_1 中的 1 次指数运算和 1 次乘法运算；密文的主要存储量包括 ROBDD、群 G_0 中的 $T+1$ 个元素及群 G_1 中的 1 个元素。

Keygen(ROBDD, S, MK)算法：由授权中心根据属性集 S 生成私钥 SK。对于 $i\notin S$，默认 $\underline{i}=\neg i$。KeyGen算法运行如下：

(1)查询ROBDD结构中根结点，将其定义为当前结点，设置 $t_{\text{SK}}=0$；

(2)读取当前结点信息，若 $i\in S\wedge\underline{i}=i$，执行 $t_{\text{SK}}+=t_i$，转到步骤(3)；若 $i\in S\wedge\underline{i}=\neg i\vee i\notin S$，执行 $t_{\text{SK}}+=t_i'$，转到步骤(4)；

(3)若high域指向终结点，转到步骤(5)；否则将该子结点定义为当前结点并转到步骤(2)；

(4)若low域指向终结点，转到步骤(5)；否则将该子结点定义为当前结点并转到步骤(2)；

(5)随机选择 $r\in Z_p$，计算 $\widehat{D}=g^{y-r}$,$D=g^{(r/t_{\text{SK}})}$，生成私钥 SK=$<\widehat{D},D>$。

该算法主要计算量为群 G_0 中的 2 次指数运算，私钥占用空间为群 G_0 中的 2 个元素。

在该算法中，需要输入 ROBDD 结构，即该算法生成的私钥与 ROBDD 相关。此举是合理效的，不但可以降低私钥生成过程中的计算量及私钥占用存储空间，并能够在一定程度上避免因全局属性发生变化带来的重加密、密钥重生成等工作。当然，也可通过使用全局属性集的方法来生成私钥，以减少私钥数量、减轻授权机构的密钥生成负担。

Decrypt(CT, SK)算法：由解密用户使用私钥 SK 完成对密文 CT 的解密。

假设密文为 CT=$<\text{ROBDD},\widetilde{C},\widehat{C},\left\{C_{R_t}\middle|R_t\in R\right\}>$，私钥为 SK=$<\widehat{D},D>$，解密过程可通过递归算法实现：

(1)查询 ROBDD 结构中的根结点，将其定义为当前结点；

(2)读取当前结点的信息，若 $i\in S\wedge\underline{i}=i$，转到步骤(3)；若 $i\in S\wedge\underline{i}=\neg i\vee i\notin S$，转到步骤(4)；

(3)根据 high 域查找 1-边子结点：

(a)若为 $\boxed{0}$，终止递归算法，返回解密失败；

(b)若为 $\boxed{1}$，转到步骤(5)；

(c)若为非终结点，将其定义为当前结点并转到步骤(2)；

(4)根据 low 域查找 0-边子结点：

(a)若为 $\boxed{0}$，终止递归算法，返回解密失败；

(b)若为 $\boxed{1}$，转到步骤(5)；

(c)若为非终结点，将其定义为当前结点并转到步骤(2)；

(5)若当前已成功匹配路径 R_t，依次计算 $e\left(\widehat{C},\widehat{D}\right)\cdot e\left(C_{R_t},D\right)=e(g,g)^{s\cdot(y-r)}\cdot e(g,g)^{s\cdot r}=e(g,g)^{s\cdot y}=Y^s$, $M=\widetilde{C}/Y^s=\widetilde{C}/e(g,g)^{s\cdot y}$，解密成功并返回 M。

由以上推导可知，当 SK $\vDash$ ROBDD 时用户成功解密密文，此时 **Decrypt** 算法的主要计算量为 2 次线性对计算、G_1 中的 2 次乘法运算。

假设 3 位用户拥有属性集分别为 $S_1=\{x_0,x_1\}$，$S_2=\{x_1,x_2\}$，$S_3=\{x_1,x_3\}$，数据使用图 1 中 ROBDD 结构进行加密，此 3 位用户能够解密成功，解密路径及相应的密钥元素如图 2 所示。

3.3 安全性证明

在安全性方面，本节通过将 CPA 安全性归约到 DBDH 假设来证明方案的安全性。

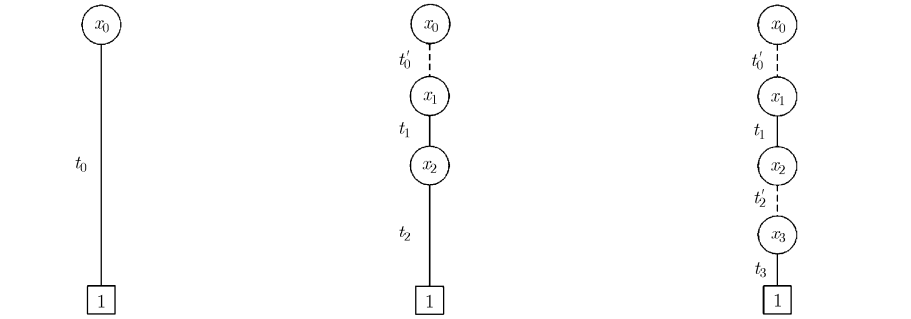
定理　若存在概率多项式时间敌手 Adv 能够以不可忽略的优势赢得 CP-ABE 游戏，则可以构造一个模拟器 Sim 以不可忽略的优势破解 DBDH 难题。

证明　假设 Adv 以优势 ε 赢得 CP-ABE 游戏，本文将构造以优势 $\varepsilon/2$ 破解 DBDH 难题的 Sim。定义阶为 p 的群 G_0 及双线性映射 $e:G_0\times G_0\to G_1$，挑战者随机选择 $a,b,c,z\in Z_p$, $v\in\{0,1\}$ 及 $g\in G_0$，并根据 v 对 Z 进行定义：若 $v=0$，令 $Z=e(g,g)^{abc}$，否则令 $Z=\ e(g,g)^z$。随后，挑战者将 $<g,A,B,C,Z>=<g,g^a,g^b,g^c,Z>$ 发送给 Sim。在接下来的过程中，Sim 担任挑战者的角色。

Initial. Adv 将 ROBDD=$\left\{\text{Node}_{\text{id}}^i\middle|\text{id}\in\text{ID},i\in I\right\}$ 传递给 Sim。

Setup: Sim 定义 $Y=e(A,B)=e(g,g)^{ab}$，选择 $\left(t_i,t_i'\right)\in Z_p\ (i\in I)$。

Phase 1: Adv 提交属性集 S 进行密钥查询，且 SK $\nvDash$ ROBDD，即 S 无法与 ROBDD 结构中的所有有效路径匹配，因此，对于任一有效路径 R_t，必定存在 $j\in I_t$ 满足 $j\in S\wedge\underline{j}=\neg j$ 或 $j\notin S\wedge\underline{j}=j$。不失一



(a) S_1={x_0,x_1}; $t_{SK}=t_0$ (b) S_2={x_1,x_2}; $t_{SK}=t_0'+t_1+t_2$ (c) S_3={x_1,x_3}; $t_{SK}=t_0'+t_1+t_2+t_3$

图 2 属性集、解密路径及密钥元素

般性，本文以 $j \notin S \wedge \underline{j}=j$ 为例完成本游戏。

对所有 $i \in I_t$ 分别设置 $\underline{t_i}$：对于 $j \notin S \wedge \underline{j}=j$，令 $\underline{t_j} = b \cdot t_j'$；当 $i \neq j$ 时分为以下情况：

(1) $i \in S \wedge \underline{i} = i$，$\underline{t_i} = t_i$；

(2) $i \in S \wedge \underline{i} = \neg i$，$\underline{t_i} = b \cdot t_i$；

(3) $i \notin S \wedge \underline{i} = \neg i$，$\underline{t_i} = t_i'$；

(4) $i \notin S \wedge \underline{i} = i$，$\underline{t_i} = b \cdot t_i'$。

继而生成私钥组件 $\widehat{D} = g^{ab-r}$，$D = g^{\left(r/\sum_{i\in I} \underline{t_i}\right)}$。

Challenge：Adv 提交等长明文 M_0 和 M_1，Sim 随机选择 $\mu \in \{0,1\}$，定义 $\widetilde{C} = M_\mu \cdot Z$ 并生成密文 $\mathrm{CT}=<\mathrm{ROBDD},\widetilde{C},C,\left\{C_{R_t}=g^{\sum_{i\in I} \underline{t_i}\cdot c} \middle| R_t \in R\right\}>$。

Phase 2：同 **Phase 1**。

Guess：Adv 猜测 μ 的取值为 μ'。若 $\mu=\mu'$，Sim 输出“DBDH”，否则输出“Random”。

若 $Z = e(g,g)^{abc}$，CT 是有效密文，此时 Adv 的获胜优势为 ε，即

$$P\left[\mathrm{Sim} \to \text{"DBDH"} \middle| Z = e(g,g)^{abc}\right] = P\left[\mu = \mu' | Z = e(g,g)^{abc}\right] = 1/2+\varepsilon$$

若 $Z = e(g,g)^z$，对 Adv 而言，密文 $M_\mu \cdot Z$ 是完全随机的，此时 $\mu \neq \mu'$ 的概率为 1/2，即

$$P\left[\mathrm{Sim} \to \text{"Random"} \middle| Z = e(g,g)^z\right] = P\left[\mu = \mu' \middle| Z = e(g,g)^z\right] = 1/2$$

综上可得，Sim 破解 DBDH 难题的优势为 $1/2 \cdot(1/2+\varepsilon)+1/2\cdot 1/2-1/2=\varepsilon/2$。 证毕

3.4 功能与效率分析

3.4.1 访问结构的表达能力及效率 本文将直观对比与分析 ROBDD 结构与限门结构[2,18]、与门结构[5]间的表达能力及效率。

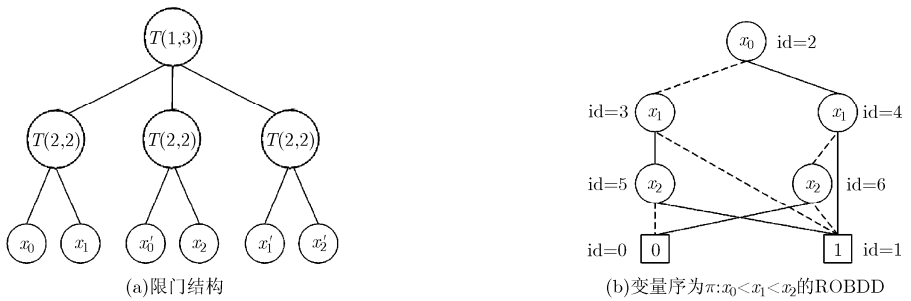
例 2 假设访问策略的布尔函数描述为

$$f_2(x_0,x_1,x_2) = x_0x_1' + x_0'x_2 + x_1'x_2'$$

由图 3 及表 2 可见，与门结构由于功能简单而无法实现对该布尔函数的表达。限门结构无法借助于单个属性表示正、负取值，导致 $f_2(x_0,x_1,x_2)$ 的限门结构表示中属性及叶子结点的数量均成倍增加；此外，限门结构中同一属性不同取值间的固有关系被切断，意味着无法支持逻辑非操作。本文中提出的 ROBDD 结构能够借助单个属性表示正负两种取值、支持属性的重复出现、支持所有布尔操作，因此能够表述任意形式的访问策略，具有更强的表达能力、更高的运行效率。

3.4.2 CP-ABE 策略的效率 在 CP-ABE 策略的性能衡量方面，主要参考各个子算法的时间复杂度、密文及私钥长度等指标。其中，算法时间复杂度的计算主要参考群中指数运算、双线性对运算的次数[2]。

在表 3 中，各个符号的意义如下：E_{G_0} 和 E_{G_1} 分别表示群 G_0 和 G_1 中的指数运算，P_e 表示双线性对运算，N 为全局属性之集合，Φ 为访问结构中所含



(a)限门结构 (b)变量序为π:$x_0<x_1<x_2$的ROBDD

图 3 $f_2(x_0, x_1, x_2)$的访问结构

表2 访问结构对比分析

CP-ABE 方案	访问结构	布尔操作				变量数	节点数
		AND	OR	限门	NOT		
文献[5]	与门结构	√	×	×	×	\	\
文献[2]，文献[13]	限门结构	√	√	√	×	6	10
本文方案	ROBDD	√	√	√	√	3	5

属性之集合，l 为生成用户私钥时所使用属性之集合，T 为ROBDD结构中有效路径数量，σ 为解密时所需属性的最少数量，B_{G_0} 和 B_{G_1} 分别表示 G_0 和 G_1 中元素长度。

由表 3 可见，本文中提出的 CP-ABE 策略具有更好的性能表现，具体表现在：**Keygen** 算法及 **Decrypt** 算法的时间复杂度与属性数量无关，均为 $O(1)$，因此能够快速生成密钥、快速解密；用户私钥定长，与属性数量无关；密文长度与 ROBDD 结构中有效路径数量有关，不与属性数量直接相关。以上特征能够显著降低整个系统在加密、密钥生成、解密、信息交互等方面的负担，并提升系统工作效率。

4　结束语

在保证 CP-ABE 安全性的前提下，尽可能提升其工作效率一直是密码学领域的研究热点。本文首次采用 ROBDD 作为 CP-ABE 中的访问结构，以此为基础完成了方案设计并证明了其安全性。在与同类型算法的对比中得出，本文方案在访问策略表达能力、工作效率等方面均具有明显优势。在后续工作中，将对 ROBDD 访问结构以及相应的 CP-ABE 作深入研究，充分挖掘 ROBDD 在数据存储、布尔运算等方面的优势，研究与 CP-ABE 策略相关的属性管理、用户撤销、密文更新等机制。

表 3　CP-ABE策略对比分析

CP-ABE方案	**Encrypt**算法	**Keygen**算法	**Decrypt**算法		密文尺寸	用户私钥尺寸	安全性
	E_{G_0}	E_{G_0}	E_{G_1}	P_e			
文献[5]	$N+1$	$2N+1$	$O(N)$	$O(N)$	$(N+1)B_{G_0}+B_{G_1}$	$(2N+1)B_{G_0}$	CCA
文献[2]	$2\Phi+1$	$2l+2$	$O(\sigma)$	$O(\sigma)$	$(2\Phi+1)B_{G_0}+B_{G_1}$	$(2l+1)B_{G_0}$	CPA
文献[13]	$2\Phi+1$	$l+3$	$O(\sigma)$	$O(\sigma)$	$(2\Phi+1)B_{G_0}+B_{G_1}$	$(l+2)B_{G_0}$	CPA
文献[6]	$\Phi+1$	$l+1$	$O(\sigma)$	$O(\sigma)$	$(\Phi+1)B_{G_0}+B_{G_1}$	$(l+1)B_{G_0}$	CPA
本文方案	$T+1$	2	$O(1)$	$O(1)$	$(T+1)B_{G_0}+B_{G_1}$	$2B_{G_0}$	CPA

参 考 文 献

[1] SAHAI A and WATERS B. Fuzzy identity-based encryption [C]. Proceedings of International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457–473. doi: 10.1007/11426639_27.

[2] BETHENCOURT J, SAHAI A, and WATERS B. Ciphertext-policy attribute-based encryption[C]. IEEE Symposium on Security and Privacy. Oakland, USA, 2007: 321–334. doi: 10.1109/SP.2007.11.

[3] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]. ACM Conference on Computer and Communications Security. New York, 2006: 89–98. doi: 10.1145/1180405.1180418.

[4] 曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016, 53(10): 2137–2151. doi: 10.7544/issn1000-1239.2016. 20160684.
CAO Zhenfu, DONG Xiaolei, ZHOU Jun, *et al*. Research advances on big data security and privacy preserving[J]. *Journal of Computer Research and Development*, 2016, 53(10): 2137–2151. doi: 10.7544/issn1000-1239.2016.20160684.

[5] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[J]. *LNCS*, 2011, 6571: 321–334. doi: 10.1007/978-3-642-19379-8_4.

[6] CHEUNG L and NEWPORT C. Provably secure ciphertext policy ABE[C]. ACM Conference on Computer and Communications Security. New York, 2007: 456–465. doi: 10.1145/1315245.1315302.

[7] BALU A and KUPPUSAMY K. An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption[J]. *Information Sciences*, 2014, 276(4): 354–362. doi: 10.1016/j.ins.2013.12.027.

[8] RAO Y S and DUTTA R. Dynamic ciphertext-policy attribute-based encryption for expressive access policy[J].

LNCS, 2014, 8337: 275–286. doi: 10.1007/978-3-319-04483-5_28.

[9] 赵志远, 王建华, 徐开勇. 定长密文且快速解密的分布式属性基加密方案研究[J]. 电子与信息学报, 2017, 39(11): 2724–2732. doi: 10.11999/JEIT170072.
ZHAO Zhiyuan, WANG Jianhua, and XU Kaiyong. Distributed attribute-based encryption with constant-size ciphertext and fast decryption[J]. *Journal of Electronics & Information Technology*, 2017, 39(11): 2724–2732. doi: 10.11999/JEIT170072.

[10] ZHANG Kai, MA Jianfeng, LIU Jiajia, *et al*. Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption[J]. *Science China Information Sciences*, 2016, 59(9): 99105. doi: 10.1007/s11432-016-0012-9.

[11] ZHOU Z, HUANG D, and WANG Z. Efficient privacy-preserving ciphertext-policy attribute based encryption and broadcast encryption[J]. *IEEE Transactions on Computers*, 2013, 64(1): 126–138. doi: 10.1109/TC.2013.200.

[12] 李拴保, 王雪瑞, 傅建明, 等. 多云服务提供者环境下的一种用户密钥撤销方法[J]. 电子与信息学报, 2015, 37(9): 2225–2231. doi: 10.11999/JEIT150205.
LI Shuanbao, WANG Xuerui, FU Jianming, *et al*. User key revocation method for multi-cloud service providers[J]. *Journal of Electronics & Information Technology*, 2015, 37(9): 2225–2231. doi: 10.11999/JEIT150205.

[13] DENG Hua, WU Qianhong, QIN Bo, *et al*. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts[J]. *Information Sciences*, 2014, 275(11): 370–384. doi: 10.1016/j.ins.2014.01.035.

[14] LI Jiguo, YAO Wei, ZHANG Yichen, *et al*. Flexible and fine-grained attribute-based data storage in cloud computing [J]. *IEEE Transactions on Services Computing*, 2016, (99): 1–1. doi: 10.1109/TSC.2016.2520932.

[15] WANG Shulan, LIANG Kaitai, LIU Joseph K, *et al*. Attribute-based data sharing scheme revisited in cloud computing[J]. *IEEE Transactions on Information Forensics & Security*, 2017, 11(8): 1661–1673. doi: 10.1109/TIFS.2016.2549004.

[16] SMARI W W, CLEMENTE P, and LALANDE J F. An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system[J]. *Future Generation Computer Systems*, 2014, 31(1): 147–168. doi: 10.1016/j.future.2013.05.010.

[17] AKERS S B. Binary decision diagrams[J]. *IEEE Transactions on Computers*, 1978, 27(6): 509–516. doi: 10.1109/TC.1978.1675141.

[18] DRECHSLER R and SIELING D. Binary decision diagrams in theory and practice[J]. *International Journal on Software Tools for Technology Transfer*, 2001, 3(2): 112–136. doi: 10.1007/s100090100056.

李 龙： 男，1989 年生，博士生，研究方向为密码算法分析与设计.

古天龙： 男，1964 年生，教授，博士生导师，研究方向为信息安全.

常 亮： 男，1980 年生，教授，研究方向为可信软件设计及测试.

徐周波： 女，1976 年生，副教授，研究方向为病毒防治和入侵检测.

钱俊彦： 男，1973 年生，教授，研究方向为形式化验证.