基于 OBDD 访问结构的无配对 CP-ABE 方案

丁晟，曹进，李晖
（西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：为了提高基于属性加密技术的计算效率，对属性基加密构造中重要的一环——访问策略进行了优化，基于有序二元决策图（OBDD）提出了一种新型的无配对 CP-ABE 方案。一方面，所提方案基于椭圆曲线密码技术，将传统 CP-ABE 方案构造中复杂的双线性配对运算替换为较为轻量级的标量乘法，降低了方案整体的计算开销。另一方面，所提方案采用基于 OBDD 的访问结构，该类型访问结构不仅能表示任何关于属性的布尔表达式，还能同时支持访问策略中属性的正负值，密钥的长度不随属性的个数而正比变化，密文长度也仅与访问策略中有效路径的个数有关。安全性和性能分析结果表明，所提方案在判定性 Diffie-Hellman (DDH) 假设下满足选择性选择明文安全，且方案的计算效率能满足物联网的实际应用需求。

关键词：密文策略基于属性加密；有序二元决策图；椭圆曲线密码；无配对
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019234

Efficient pairing-free CP-ABE based on ordered binary decision diagram

DING Sheng, CAO Jin, LI Hui
School of Cyber Engineering, Xidian University, Xi’an 710071, China

Abstract: To improve the computational efficiency of ABE, its access structure was optimized and a pairing-free CP-ABE scheme based on ordered binary decision diagram (OBDD) was proposed. Based on the elliptic curve cryptography, the complex bilinear pairing operation in traditional CP-ABE was replaced with the relatively lightweight scalar multiplication, thus the overall computation overhead was reduced. And OBDD was used as the access structure of CP-ABE, which can not only represent any Boolean expression about attributes, but also support both positive and negative attributes. The length of the key was independent of the number of attributes and the length of the ciphertext was only related to the number of valid paths in the access policy. The security and performance analysis show that the scheme can resist chosen plaintext attack under the decisional Diffie-Hellman (DDH) assumption, and the computation efficiency can meet the practical application requirements of Internet of things.

Key words: CP-ABE, ordered binary decision diagram, elliptic curve cryptography, pairing-free

1 引言

物联网作为传统互联网的延伸，旨在将现存的互联网与人们生活中的各种智能设备紧密结合，彻底打破数据孤岛，让数据流动起来。通过将数十亿的智能设备互联，物联网给予了智能电网、智慧城市、智能家居、智慧医疗等新模式更多的可能。然而，随着物联网设备之间的关系越来越紧密，如何

收稿日期：2019−07−08；**修回日期**：2019−09−18
基金项目：国家重点研发计划基金资助项目（No.2017YFB0802700）；国家自然科学基金资助项目（No.61772404, No.U1836203）
Foundation Items: The National Key Research and Development Program of China (No.2017YFB0802700), The National Natural Science Foundation of China (No.61772404, No.U1836203)

保证数据在物联网中安全高效的共享成为一个相当棘手的问题。当物联网智能设备之间共享数据时，潜在的安全问题如数据泄露、数据完整性被破坏或未授权访问等都将严重影响数据在共享过程中的安全。

随着物联网设备数量的急剧增长，数据量规模也日趋庞大，单纯依靠设备自身存储和处理数据极易使其淹没在海量的数据之下。云计算作为互联网技术另一重要革新，其丰富的存储和计算资源可帮助物联网设备代理存储和处理数据。物联网设备可将本地存储的数据上传至云端，并可随时从云端下载数据，以节省本地存储资源。对于那些难以处理的数据，由于物联网设备自身计算资源有限，可以将数据提交给云端，利用云计算丰富的计算资源对数据进行必要的处理后，直接使用云计算返回的结果来进行下一步决策。

由于数据存储在云端，脱离了数据所有者的直接管控，其安全性将受到极大挑战。针对这一问题，普遍的解决方案是将数据加密，以密文形式存储在云端。基于属性的加密能同时实施数据加密和访问控制，有效保证了数据在共享过程中的安全。然而，直接将基于属性的加密应用到物联网设备上还存在一些问题，如其一直被诟病的效率问题。传统的基于属性加密的方案构造中都涉及双线性配对这一运算，经实验测试，一次双线性配对的计算开销大约是同一椭圆曲线下一次标量乘法运算的2~3倍[1]。因此，尽可能减少算法中双线性配对的计算次数，或者巧妙运用其他运算实现同样的算法功能，可在一定程度上提高基于属性加密的算法效率。

访问结构的设计也是基于属性加密中相当重要的一环。访问结构具有多种表现形式，例如线性秘密分享方案（LSSS, linear secret sharing scheme）[2]、与门[3]、门限[4]等。访问结构的优化可以提升密文策略属性基加密（CP-ABE, ciphertext-policy attribute-based encryption）系统的运行效率，可以提高访问策略的可表达能力，还能通过减少策略中冗余的属性来缩小密文长度。

本文基于有序二元决策图（OBDD, ordered binary decision diagram）访问结构，为物联网系统提出了一种新的无配对基于属性的加密方案，主要贡献如下。

1) 为物联网系统提出了一种新的无配对基于属性的加密方案。该方案对传统CP-ABE进行了相关改进，利用椭圆曲线上较为轻量级的标量乘法代替复杂的双线性配对运算，有效降低了方案的计算开销。

2) 基于OBDD技术优化了访问策略的数据结构，不仅支持任意关于属性的布尔表达式，还同时支持访问策略中属性的正负值。

2 相关研究

在过去的十年中，双线性配对的出现解决了许多之前在密码学领域无法解决的问题[5-7]。基于双线性配对，ABE被提出用于实现数据加密和访问控制的结合。Bethencourt等[4]提出了CP-ABE的具体构造，在他们的方案设计中，加密算法基于数据拥有者建立的访问树来加密消息。每个用户拥有一组代表其身份的属性以及每个属性对应的属性密钥。解密算法利用拉格朗日插值法来解密密文。Waters[2]基于LSSS访问结构提出了一个较为灵活的CP-ABE构造，并基于该构造提出了新的方案，改善了原有方案的不足。

2007年，Cheung等[3]提出了一种支持与门访问结构的CP-ABE方案，该方案同时支持正负2种属性。Zhou等[8]提出了一种密文长度恒定的CP-ABE方案，密文长度不随系统中属性数量的变化而变化。该方案性能良好，但不支持非单调或析取范式的访问结构。Wang等[9]解决了CP-ABE方案中的密钥托管问题，同时提高了属性的可表达性。Guo等[10]提出了一种密钥长度恒定的CP-ABE方案，该方案中解密密钥的数量独立于属性的数量。Li等[11]基于OBDD访问结构提出了一种新型的CP-ABE方案，该方案充分利用了OBDD访问结构丰富的表达性和计算上的高效性，但方案仍涉及双线性对的运算。尽管CP-ABE方案能有效保证云中数据的安全，并实施细粒度的访问控制，但方案中涉及大量双线性配对运算和模幂运算，计算开销过大这一问题严重限制了将其应用于物联网中的资源受限型的设备。

众所周知，基于配对的密码学协议的计算效率取决于配对运算的计算速度。针对这一问题，学者们进行了大量的研究[12-16]。为了优化椭圆曲线密码（ECC, elliptic curve cryptography）协议，Freeman等[17]分类列举了一些对于配对运算友好的椭圆曲线，并介绍了它们的具体构造以及相关的一些优化技术。Scott[18]分析了如何选择配对类型及椭圆曲线以提高ABE方案的计算效率。Rivain[19]详细讨

论了如何在 ECC 方案中更快地计算标量乘法。

一种降低用户计算开销的方法是将复杂的运算外包给其他具有更强计算能力的实体。Chevallier-Mames 等[20]在单不可信服务器模型下提出了一种将复杂的双线性配对计算外包的方案，但与 Chen 等[21]所提方案相比，计算开销仍较高。Chen 等在双不可信服务器−单恶意实体模型下提出了一种新的计算外包算法，该算法计算效率更高，但其安全模型在实际应用中是不现实的。

一种较为直接的方法是将部分解密工作外包给云端。2011 年，Green 等[22]提出了一种解密外包的 ABE 方案，属性私钥由两部分组成：El Gamal 密钥和转换密钥。代理方可以利用转换密钥对密文进行部分解密，部分解密的结果为简单的 El Gamal 密文，用户只需再利用 El Gamal 密钥进行简单运算即可完成解密。Li 等[23]对这种方式进行了改进，使其同时支持对密钥分发和解密的外包。然而，这种计算外包方式只是将计算开销转移到了代理方或云服务器，对于整个系统来说，计算开销并没有得到有效降低。

为了从根本上优化 ABE 算法，本文利用其他更高效的算术运算代替复杂的双线性对运算。Odelu 等[24]基于椭圆曲线密码学提出了一种密钥长度恒定的 CP-ABE 方案，但该方案只支持与门访问结构，限制了方案的灵活性。随后，他们基于 RSA 提出了一种新的密钥长度和密文长度均恒定的 CP-ABE 方案[25]。虽然该方案加密和解密的时间复杂度均为 $O(1)$，但仍只支持与门访问结构。

3　基础知识

3.1　有序二元决策图

二元决策图（BDD）是一个有根、有向的非循环图，可用于高效的表示布尔函数。所有的布尔函数都可以转换为变量之间基本逻辑运算，例如 AND、OR、NOT 等的组合。

BDD 由 2 种节点构成：决策节点和终端节点。每个决策节点会被标记为某一布尔变量 X，同时决策节点拥有 2 个子节点。当布尔变量 X 获得赋值为 1 时，它的子节点被称为高节点；当 X 获得赋值为 0 时，它的子节点被称为低节点。如果二元决策图中所有路径上的不同变量从根节点开始都以同样的次序出现，那么这种二元决策图被称为有序二元决策图（OBDD）。

举例来说，图 1 是用 OBDD 表示布尔函数 $f(x_0,x_1,x_2,x_3)=x_0+x_1x_2+x_1x_3+x_2x_3$。决策节点用圆圈表示，终端节点用方块表示。实线表示通向高节点的边，虚线表示通向低节点的边。布尔函数 $f(x_0,x_1,x_2,x_3)=x_0+x_1x_2+x_1x_3+x_2x_3$ 的值是通过从根节点开始沿着决策图中的某一路径向下，依次为每个决策节点中的变量赋值来得到的。函数 $f(x_0=1,x_1=1,x_2=0,x_3=0)$ 的值可以从 x_0 开始，沿实线向下移动到 x_1，再沿着实线移动到 x_2，最后连续沿着 2 条虚线移动到终端节点 1。

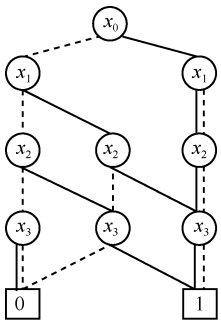


图 1　布尔函数 $f(x_0,x_1,x_2,x_3)=x_0+x_1x_2+x_1x_3+x_2x_3$ 的 OBDD 表示

3.1.1　生成 OBDD 访问结构

本节详细介绍如何将一个布尔表达式转换成对应的 OBDD 访问结构。

假设系统中定义了 n 种属性 i，编号依次为 $i_0,i_1,\cdots,i_{n-1}$。访问策略包含系统中定义的所有属性。属性 i 的属性值为正，代表该访问策略要求满足策略的属性集里需含有属性 i；属性 i 的属性值为负，代表满足策略的属性集里不需要含有属性 i。基于布尔表达式的访问策略可表示为 $f(i_0,i_1,\cdots,i_{n-1})$。

将 OBDD 中的所有节点进行编号，获得最终访问结构的表达式为

$$\mathrm{OBDD}=\left\{\mathrm{Node}_{\mathrm{id}}^{i}\mid \mathrm{id}\in \mathrm{ID}, i\in U\right\}$$

其中，ID 是决策节点序号的集合；U 是访问结构里出现的属性的集合；$\mathrm{Node}_{\mathrm{id}}^{i}$ 是一个元组 $(\mathrm{id},i,\mathrm{high},\mathrm{low})$，id 是当前节点的序号，$i$ 是当前节点内属性的序号，high 代表 1 分支节点，low 代表 0 分支节点，如图 2 所示。

3.1.2　判断是否满足访问结构

假设 U 是一个属性集，判断该属性集是否满足访问结构 OBDD 可按如下方式进行。

从根节点开始，对于具有属性 i 的决策节点，如果该属性 i 属于集合 U，则代表该属性的属性值

为 1，判断过程将沿 1 分支节点向下；否则，判断将沿 0 分支节点向下。以上过程将重复执行直到抵达终端节点。如果终端节点为 1，则表示属性集 U 满足该访问策略 OBDD；如果终端节点为 0，则表示属性集 U 不满足该访问策略 OBDD。

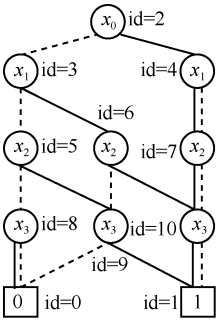


图 2 生成 OBDD 访问结构

3.2 CP-ABE 框架

一个 CP-ABE 系统通常由 5 种算法组成，分别为系统初始化、授权机构设置、密钥生成、加密和解密，定义如下。

系统初始化 $(k)\rightarrow \mathrm{PP}$

系统设置算法将安全参数 k 作为输入，然后输出系统所需的全部公共参数 PP。

授权机构设置 $(\mathrm{PP})\rightarrow \mathrm{PK},\mathrm{SK}$

基于第一步生成的公共参数 PP，属性授权机构为自己和系统中的每一个属性生成公钥 PK 和私钥 SK。

密钥生成 $(\mathrm{PP},i,\mathrm{GID},\mathrm{SK})\rightarrow \mathrm{SK}_{i,\mathrm{GID}}$

密钥生成算法将公共参数、属性 i、身份 GID 以及属性授权机构的 SK 作为输入，输出属性私钥 $\mathrm{SK}_{i,\mathrm{GID}}$，并将其发送给对应的用户。

加密 $(\mathrm{PP},M,(\mathbb{A},\rho),\{\mathrm{PK}_i\})\rightarrow \mathrm{CT}$

给定一消息 M，访问矩阵 (A,ρ) 和访问策略中所有属性的公钥，加密算法输出密文 CT。

解密 $(\mathrm{PP},\mathrm{CT},\{\mathrm{SK}_{i,\mathrm{GID}}\})\rightarrow M$

如果某个用户拥有的一组属性满足密文的访问策略，解密算法可以成功恢复消息 M，否则解密失败。

3.3 安全模型

本节给出无配对运算的 CP-ABE 方案的安全模型。该模型由以下描述的挑战者和敌手之间的游戏定义。

初始化

敌手首先选择一个挑战访问结构 $\mathbb{A}$，然后将其发送给挑战者。

设置

挑战者运行设置算法，为系统生成必要的全局参数，为每个属性生成公私钥对。然后挑战者将系统全局参数和属性公钥发送给敌手。

阶段 1

攻击者可以自适应地查询任何属性私钥，唯一的限制是相查询的属性集不能满足挑战访问结构 $\mathbb{A}$。

挑战阶段

敌手选择 2 条等长的消息 M_0和M_1，并将它们发送给挑战者。然后挑战者掷一枚随机硬币 $\beta\in\{0,1\}$，并在访问结构 $\mathbb{A}$ 下对消息 M_β 加密，然后发送给敌手。

阶段 2

敌手可以继续查询属性私钥，唯一的限制条件与阶段 1 相同。

猜测

敌手对 β 输出猜测结果 β'。敌手在这场游戏中的优势被定义为 $\Pr[\beta'=\beta]-\frac{1}{2}$。

定义 1 如果任何多项式时间敌手赢得这个安全游戏的优势是可以被忽略的，则所提方案被认为是选择性 CPA 安全的。

3.4 DDH 假设

椭圆曲线上的判定性 Diffie-Hellman（DDH, decisional Diffie-Hellman）假设的定义描述如下。

挑战者选择一个素数阶 r 的循环群 P。令 G 是循环群 P 的一个生成元，a 和 b 是从 $\mathbb{Z}_r$ 中随机选择的。如果挑战者给攻击者一个元组 (G,aG,bG)，那么攻击者在多项式时间内区分元素 $abG\in P$ 和随机元素 $R\in P$ 是困难的。算法 β 解决 P 中 DDH 假设的优势定义为 ε，当

$$|\Pr[\beta(G,aG,bG,Z=abG)=0]-\Pr[\beta(G,aG,bG,Z=R)=0]|\geqslant\varepsilon$$

定义 2 如果多项式时间算法解决 DDH 困难问题的优势是可忽略的，那么 DDH 假设是成立的。

4 方案构造

本节将给出为物联网中高效安全数据共享所设计的基于 OBDD 访问结构的无配对 CP-ABE 的具体构造。由于双线性配对一直被认为是基于属性加密方案设计中计算开销最大的运算，因此本文选择用椭圆曲线上相对轻量级的标量乘法来代替复杂的双线性配对运算，以提高方案在加密和解密阶段

的计算效率。此外，采用基于 OBDD 的访问结构来提高访问策略的表达能力，该类型访问结构既同时支持属性的正负值，也支持任何布尔运算。所提方案由以下 5 种算法组成。

1) 系统初始化

令 GF(p)为一阶为 p 的有限域。E 是定义在 GF(p)上的一条椭圆曲线。G 是椭圆曲线 E 上一阶为 r 的元素。G 生成了一个 E 的循环子群，其中椭圆曲线离散对数问题是困难的。

2) 授权机构设置

系统中定义的属性集合N包含 n 个元素，编号为{0,1,2,⋯,n−1}。对于N中的每个属性 i，属性授权机构为该属性的正值随机选择 $k_i \in \mathbb{Z}_r$，并为该属性的负值随机选择 $k_i' \in \mathbb{Z}_r$。属性 i 的正值和负值对应的属性公钥分别为 k_iG 和 $k_i'G$。

3) 密钥生成

假设用户拥有一属性集 U。对于系统中定义的每一个属性 i，如果 $i \in U$，那么对于该用户来说该属性取正值，对应的属性私钥为 k_i；否则，该属性取负值，对应的属性私钥为 k_i'。若为拥有属性集 U 的用户生成密钥，属性授权机构可计算 $\sum_{i\in U} \underline{k_i}$，其中，$\sum_{i\in U} \underline{k_i}$ 表示 k_i 或 k_i'。

4) 加密

首先，将明文消息映射到椭圆曲线 E 上的一点 M。数据拥有者设置的访问结构为

$$\mathrm{OBDD} = \{\mathrm{Node}_{\mathrm{id}}^{i} \mid \mathrm{id} \in \mathrm{ID}, i \in U\}$$

令有效路径 (root $\to$1) 的数量为 V，其中每条有效路径为 $\{P_j, j \in [0, v-1]\}$。数据所有者随机选择 $s \in \mathbb{Z}_r$，并计算

$$C_{P_j} = M + s\left(\sum_{i\in P_j} \underline{k_i} G\right), C = sG$$

整个密文为 $\{\mathrm{OBDD}, C, C_{P_j}, j \in [0, V-1]\}$。

5) 解密

若要解密密文 CT，数据使用者拥有的属性集必须满足数据拥有者制定的访问策略。具体的解密步骤可以通过以下递归算法实现。

步骤 1　寻找编号为 2 的节点，即根节点，并将其定义为当前节点。

步骤 2　提取当前节点中包含的信息 $\mathrm{Node}_{\mathrm{id}}^{i}$。对于属性 i：如果 $i \in U \wedge \underline{i} = i$，则算法转到步骤 3 继续执行；如果 $i \in U \wedge \underline{i} = \overline{i} \vee i \notin U$（$\overline{i}$ 表示 NOT i），则算法转到步骤 4 继续执行。

步骤 3　搜索当前节点的 1 分支节点。

① 如果 1 分支节点是终端节点 0，则终止递归算法并返回解密失败。

② 如果 1 分支节点是终端节点 1，则算法转到步骤 5 继续执行。

③ 如果 1 分支节点是非终端节点，则将其定义为当前节点，算法转到步骤 2 继续执行。

步骤 4　搜索当前节点的 0 分支节点。

① 如果 0 分支节点是终端节点 0，则终止递归算法并返回解密失败。

② 如果 0 分支节点是终端节点 1，则算法转到步骤 5 继续执行。

③ 如果 0 分支节点是非终端节点，则将其定义为当前节点，算法转到步骤 2 继续执行。

步骤 5　如若数据使用者拥有的属性集满足某一条有效路径 P_j，那么为了恢复出明文 M 可以计算

$$C_{P_j} - \mathrm{SK}C = M + s\left(\sum_{i\in P_j} \underline{k_i} G\right) - \sum_{i\in P_j} \underline{k_i} sG = M$$

最后，数据使用者可以将 M 映射回明文消息。

5　安全性分析

5.1　安全证明

本节将证明所提方案在 DDH 假设下是选择性 CPA 安全的。

定义 3　如果存在一个多项式时间的敌手 $\mathcal{A}$ 可以一个不可忽略的优势 $\varepsilon > 0$ 来破解提出的方案，那么存在一个多项式时间算法 $\mathcal{B}$ 可以 $\frac{\varepsilon}{2}$ 的优势来区分 DDH 元组和随机元组。

令 G 为 E 的一个阶为 r 的生成元，β 是集合{0,1}中的随机元素，R 是 E 中一随机元素。DDH 挑战者 $\mathcal{C}$ 首先随机选择 $a, b \in \mathbb{Z}_r$。如果 $\beta = 0$，则令 Z=abG；否则令 Z=R。挑战者 $\mathcal{C}$ 将元组(G,aG,bG,Z)提交给模拟器 $\mathcal{B}$。然后 $\mathcal{B}$ 在下面的游戏中代替 $\mathcal{C}$ 扮演挑战者的角色。

系统初始化

$\mathcal{A}$ 首先向 $\mathcal{B}$ 提交一个挑战访问结构 $\{\mathbb{A} = \{\mathrm{Node}_{\mathrm{id}}^{i} \mid \mathrm{id} \in \mathrm{ID}, i \in U\}$。

设置

为了给敌手 $\mathcal{A}$ 生成系统中的每个属性 i 的属性公钥，$\mathcal{B}$ 随机选择 $k_i, k_i' \in \mathbb{Z}_r$。令 k_iaG 为正属性 i 的公钥，$k_i'aG$ 为负属性 i 的公钥。因为 k_i, k_i' 是随

机选择的，所以公共参数实际上也是随机的。

阶段 1

$\mathcal{A}$ 自适应地将属性集U提交给 $\mathcal{B}$ 以求获得相应的属性私钥。唯一限制条件是敌手无法查询任何可用于成功解密密文的属性私钥。换句话说，属性集 U 不能是 $\mathbb{A}$ 的任何有效路径。

挑战

$\mathcal{A}$ 在随机选择 2 条等长消息 $M_0, M_1 \in E$，并将它们提交给 $\mathcal{B}$。然后 $\mathcal{B}$ 掷一枚随机硬币 $\beta \in \{0,1\}$，并根据访问结构 $\mathbb{A}$ 加密 M_β。令 $C=bG$，$C_{P_j} = M_\beta + \left(\sum_{i \in P_j} \underline{k}_i Z\right)$。$\mathcal{B}$ 将挑战密文 $\mathrm{CT} = \{C, C_{P_j}\}$ 返回给敌手 $\mathcal{A}$。

阶段 2

与阶段 1 相同。敌手 $\mathcal{A}$ 可以提交其他属性私钥查询，只要不违反与阶段 1 相同的限制条件。

猜测

$\mathcal{A}$ 输出对 β 的猜测 β'。如果 $\beta' = \beta$，$\mathcal{B}$ 输出 0 表示 $Z=abG$；否则，$\mathcal{B}$ 输出 1 表示 $Z=R$。

如果$Z = abG$，那么它是真正的密文。在这种情况下，由于 $\mathcal{A}$ 的优势在假设中定义为 ε。因此有

$$\Pr[\mathcal{B}(G, aG, bG, Z = R) = 0] = \frac{1}{2} + \varepsilon$$

如果 $Z=R$，则对敌手 $\mathcal{A}$ 而言是完全随机的。从而有

$$\Pr[\mathcal{B}(G, aG, bG, Z = R) = 0] = \frac{1}{2}$$

因此，$\mathcal{B}$ 破解 DDH 问题的优势为

$$\mathcal{B} = \frac{1}{2}(\Pr[\mathcal{B}(G, aG, bG, Z = aBG) = 0] + \Pr[\mathcal{B}(G, aG, bG, Z = R) = 0]) - \frac{1}{2} = \frac{1}{2}\left(\frac{1}{2} + \varepsilon + \frac{1}{2}\right) - \frac{1}{2} = \frac{\varepsilon}{2}$$

5.2 共谋攻击

对于 CP-ABE 来说，共谋攻击是方案设计时需要考虑的最重要的安全问题之一。由于 ABE 旨在授予属性集满足访问结构的用户访问权限，因此不具备访问资格的用户不应能够恢复出明文，即使他们彼此串通。换句话说，他们不能通过组合或计算他们自己的属性私钥来获得可用于成功解密密文的密钥。在本文的方案中，每个用户的密钥是其属性集中每个属性值对应的 $\underline{k}_i \bmod r$ 的总和。假设有 n 个属性，编号依次为 $\{0,1,2,\cdots,n-1\}$，每个属性对应的密钥为 $\underline{k}_i$（当属性值为正时，属性私钥为 $\underline{k}_i = k_i$；否则，$\underline{k}_i = k_i'$）。总共有 2^n 个可能的密钥，分别为

$$\begin{aligned}
\mathrm{SK}_0 &= k_0 + k_1 + \cdots + k_{n-2} + k_{n-1} \\
\mathrm{SK}_1 &= k_0' + k_1 + \cdots + k_{n-2} + k_{n-1} \\
\mathrm{SK}_2 &= k_0' + k_1' + \cdots + k_{n-2} + k_{n-1} \\
&\vdots \\
\mathrm{SK}_{2^n-1} &= k_0' + k_1' + \cdots + k_{n-2}' + k_{n-1} \\
\mathrm{SK}_{2^n} &= k_0' + k_1' + \cdots + k_{n-2}' + k'_{n-1}
\end{aligned}$$

实际上，这 2^n 个属性私钥形成了一个拥有 $2n$ 个变量 $k_0, k_1, \cdots, k_{n-1} k_0', k_1', \cdots, k_{n-1}'$ 的线性方程组，分别为

$$\begin{aligned}
&\mathrm{SK}_0 = k_0 + k_1 + \cdots + k_{n-2} + k_{n-1} + \\
&0k_0' + 0k_1' + \cdots + 0k_{n-2}' + 0k_{n-1}' \\
&\mathrm{SK}_1 = 0k_0 + k_1 + \cdots + k_{n-2} + k_{n-1} + \\
&k_0' + 0k_1' + \cdots + 0k_{n-2}' + 0k_{n-1}' \\
&\mathrm{SK}_2 = 0k_0 + 0k_1 + \cdots + k_{n-2} + k_{n-1} + \\
&k_0' + 0k_1' + \cdots + 0k_{n-2}' + 0k_{n-1}' \\
&\vdots \\
&\mathrm{SK}_{2^n-1} = 0k_0 + 0k_1 + \cdots + 0k_{n-2} + k_{n-1} + \\
&k_0' + k_1' + \cdots + k_{n-2}' + k_{n-1}' \\
&\mathrm{SK}_{2^n} = 0k_0 + 0k_1 + \cdots + 0k_{n-2} + 0k_{n-1} + \\
&k_0' + k_1' + \cdots + k_{n-2}' + k_{n-1}'
\end{aligned}$$

该线性方程组的系数矩阵为

$$\begin{pmatrix}
1 & 1 & \cdots & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 1 & 1 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 1 & 1 & 1 & 1 & \cdots & 0 & 0 \\
 & & \ddots & & & & & \ddots & & \\
0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & 0 \\
0 & 0 & \cdots & 0 & 0 & 1 & 1 & \cdots & 1 & 1
\end{pmatrix}$$

很明显，系数矩阵的秩小于变量的数量。因此，这种线性方程组具有无限多个解。换句话说，对于那些不合格的数据用户，他们无法通过使用自己的密钥计算获得有关 $\underline{k}_i$ 的确切值的任何有价值的信息。因此，本文方案可以有效抵抗共谋攻击。

6 性能分析

本节将所提方案与其他方案在性能表现方面进行了对比，包括加解密计算开销、密钥生成计算开销、

密文长度和密钥长度。在分析计算开销时，着重统计了方案中涉及的一些主要的运算，如群元素的幂运算、双线性对运算、标量乘法。为了便于理解，将分析中用到的符号在表 1 进行简要说明。

表 1　　符号示例

符号	意义
C_G	群元素的幂乘或标量乘法
C_e	双线性对运算
V	OBDD 中有效路径的个数
N	系统中定义的属性个数
S	访问策略中的属性个数
K	密钥生成所用到的属性个数
σ	成功解密所需的最少属性个数
L	群元素大小

为了证明双线性配对运算比标量乘法计算开销大，表 2 中对比了在本文的实验环境中 2 种运算的计算开销。实验环境为一台搭载 Intel 的 Pentium G620 CPU，2.60 GHz 和 2 GB RAM 机器，该机器运行 Ubuntu Linux 16.04LTS 系统。方案基于 PBC 库（版本 0.5.14），选择了 512 bit 有限域上的一条超奇异曲线上 160 bit 的椭圆曲线群，来实现 80 bit 的安全性。实验结果是 30 轮实验的平均值。从表 2 可见，一次双线性配对运算的计算开销大约是一次标量乘法的 2~3 倍。

表 2　　各种运算计算开销对比

运算	计算开销/ms
C_e	3.97
C_G	1.51

从表 3 中可以清楚地看到，所提方案在多个方面均优于其他方案。密钥生成和解密的时间复杂度均为 $O(1)$，且由于所提方案的密钥生成阶段仅涉及模加运算，因此其密钥生成阶段的计算开销几乎可以忽略不计，而较文献[3]方案和文献[4]方案更为高效的文献[11]方案仍需要进行 2 次群元素的幂乘运算。解密过程仅需要一次标量乘法，虽然在时间复杂度上与文献[11]方案一样均为 $O(1)$，但文献[11]方案仍需要进行双线性配对运算。此外，所提方案中属性授权机构为用户分发的密钥长度是固定的，而非正比于属性的数量，且较文献[11]方案来说，密钥长度仅为文献[11]方案的一半。加密过程的计算开销以及密文长度均正比于 OBDD 访问结构中有效路径的个数，而非访问结构中属性的个数，这显然有效降低了方案的计算和存储开销，尤其是当 V 较小时。

7　结束语

为了保证物联网数据安全高效的共享，本文应用 CP-ABE 技术来对数据进行安全的加密，同时实施细粒度的访问控制。基于 OBDD 的访问结构提出了一种新型的无配对 CP-ABE 方案。利用椭圆曲线密码技术，将原本 CP-ABE 方案构造中复杂的双线性配对运算替换为轻量级的标量乘法，从而降低了方案的计算开销。同时方案采用 OBDD 访问结构，该类型访问结构不仅能表示任何关于属性的布尔表达式，还同时支持访问策略中属性的正负值。安全性和性能分析结果表明，所提方案在 DDH 假设下满足选择性选择明文安全，且方案的计算效率能满足物联网的实际应用需求。

参考文献：

[1] DING S, LI C, LI H. A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT[J]. IEEE Access, 2018(6): 27336-27345.

[2] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. Springer, 2011: 53-70.

[3] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]//The 14th ACM conference on Computer and communications security. ACM, 2007: 456-465.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy. IEEE, 2007: 321-334.

[5] JOUX A. A one round protocol for tripartite Diffie-Hellman[J]. Journal

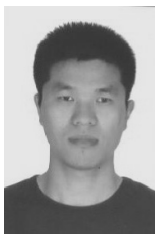
表 3　　性能对比

方案	密钥生成	加密	解密	密文长度	密钥长度
文献[3]	$(2K+1)C_G$	$(N+1)C_G$	$O(N)$	$(N+2)L$	$(2N+1)L$
文献[4]	$(2K+2)C_G$	$(2S+1)C_G$	$O(\sigma)$	$(2S+2)L$	$(2K+1)L$
文献[11]	$2C_G$	$(V+1)C_G$	$O(1)$	$(V+2)L$	$2L$
本文方案	—	$(V+1)C_G$	$O(1)$	$(V+2)L$	L

of Cryptology, 2004, 17(4): 263-276.
[6] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319.
[7] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Annual International Cryptology Conference. Springer, 2001: 213-229.
[8] ZHOU Z, HUANG D, WANG Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2013, 64(1): 126-138.
[9] WANG S, LIANG K, LIU J K, et al. Attribute-based data sharing scheme revisited in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1661-1673.
[10] GUO F, MU Y, SUSILO W, et al. CP-ABE with constant-size keys for lightweight devices[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(5): 763-771.
[11] LI L, GU T, CHANG L, et al. A ciphertext-policy attribute-based encryption based on an ordered binary decision diagram[J]. IEEE Access, 2017(5): 1137-1145.
[12] BEUCHAT J L, GONZÁLEZ-DÍAZ J E, MITSUNARI S, et al. High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves[C]//International Conference on Pairing-Based Cryptography. Springer, 2010: 21-39.
[13] BARRETO P S L M, GALBRAITH S D, Ó'HÉIGEARTAIGH C, et al. Efficient pairing computation on supersingular abelian varieties[J]. Designs, Codes and Cryptography, 2007, 42(3): 239-271.
[14] CANARD S, DEVIGNE J, SANDERS O. Delegating a pairing can be both secure and efficient[C]//International Conference on Applied Cryptography and Network Security. Springer, 2014: 549-565.
[15] GUILLEVIC A, VERGNAUD D. Algorithms for outsourcing pairing computation[C]//International Conference on Smart Card Research and Advanced Applications. Springer, 2014: 193-211.
[16] CANARD S, DESMOULINS N, DEVIGNE J, et al. On the implementation of a pairing-based cryptographic protocol in a constrained device[C]//International Conference on Pairing-Based Cryptography. Springer, 2012: 210-217.
[17] FREEMAN D, SCOTT M, TESKE E. A taxonomy of pairing-friendly elliptic curves[J]. Journal of Cryptology, 2010, 23(2): 224-280.
[18] SCOTT M. On the efficient implementation of pairing-based protocols[C]//IMA International Conference on Cryptography and Coding. Springer, 2011: 296-308.
[19] RIVAIN M. Fast and regular algorithms for scalar multiplication over elliptic curves[J]. IACR Cryptology ePrint Archive, 2011(1): 338.
[20] CHEVALLIER-MAMES B, CORON J S, MCCULLAGH N, et al. Secure delegation of elliptic-curve pairing[C]//International Conference on Smart Card Research and Advanced Applications. Springer, 2010: 24-35.
[21] CHEN X, SUSILO W, LI J, et al. Efficient algorithms for secure outsourcing of bilinear pairings[J]. Theoretical Computer Science, 2015, 562: 112-121.
[22] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of abe ciphertexts[C]//The 20th USENIX Conference on Security. USENIX Association, 2011.
[23] LI J, CHEN X, LI J, et al. Fine-grained access control system based on outsourced attribute-based encryption[C]//European Symposium on Research in Computer Security. Springer, 2013: 592-609.
[24] ODELU V, DAS A K. Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography[J]. Security and Communication Networks, 2016, 9(17): 4048-4059.
[25] ODELU V, DAS A K, KHAN M K, et al. Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts[J]. IEEE Access, 2017(5): 3273-3283.

[作者简介]

丁晟（1990− ），男，陕西西安人，西安电子科技大学博士生，主要研究方向为数据安全、访问控制、区块链等。



曹进（1986− ），男，陕西西安人，博士，西安电子科技大学副教授、博士生导师，主要研究方向为无线网络安全。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码信息安全、信息论与编码理论。