抗密钥委托滥用的可追踪属性基加密方案

闫玺玺，何旭，刘涛，叶青，于金霞，汤永利
（河南理工大学计算机科学与技术学院，河南 焦作 454003）

摘 要：针对可追踪属性基加密方案利用追踪功能解决密钥委托滥用问题的不完备性，提出了一种抗密钥委托滥用的可追踪属性基加密方案。将秘密参数分享给用户私钥中关联属性的全部组件，使解密过程必须由全部组件共同参与完成，仅由用户私钥的一部分不能进行解密操作，从而实现真正的抗密钥委托滥用。利用一种短签名技术保护用户私钥中的追踪参数，防止追踪参数被伪造，从而获得对用户的追踪能力。同时支持抗密钥委托滥用和可追踪增强了所提方案的安全性。与相关方案的对比分析表明，所提方案在参数尺寸和计算代价上具有更好的性能优势。

关键词：属性基加密；抗密钥委托滥用；白盒；可追踪性
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020016

Traceable attribute-based encryption scheme with key-delegation abuse resistance

YAN Xixi, HE Xu, LIU Tao, YE Qing, YU Jinxia, TANG Yongli
School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China

Abstract: Aiming at the problem that the traceability of a traceable attribute-based encryption (ABE) scheme was not sufficient to address the key abuse completely, a traceable ABE scheme against key-delegation abuse was proposed. A secret parameter was be shared to all user private key components corresponding to attributes, and the decryption was completed by using all these components together, such that only parts of them could not realize the decryption and the real key-delegation abuse resistance ability was be obtained consequently. A short signature technique was employed to prevent the tracing parameter embedded in a user private key from being forged, so as to achieve the traceability of the user who leaked his user private key. Supporting both key-delegation abuse resistance and user tracing enhances the security of the proposed scheme. And compared with related schemes, the proposed scheme has better advantage in terms of the parameters size and the computation cost.

Key words: attribute-based encryption, key-delegation abuse resistance, white-box, traceability

1 引言

云计算的推广和应用方便了人们生活。无论用户的地理位置如何变化，都可以远程访问云端，获取资源和计算服务。云服务提供商可能在云端部署多个计算节点以响应不同的请求，例如分别处理和

收稿日期：2019−10−28；**修回日期**：2019−12−18
基金项目：国家自然科学基金资助项目（No.61802117）；“十三五”国家密码发展基金资助项目（No.MMJJ20170122）；河南省科技攻关基金资助项目（No.192102210280）；河南省高校科技创新团队基金资助项目（No.20IRTSTHN013）；河南理工大学创新型科研团队基金资助项目（No. T2018-1）
Foundation Items: The National Natural Science Foundation of China (No.61802117), The “13th Five-Year” National Crypto Development Foundation (No.MMJJ20170122), Projects of Henan Provincial Department of Science and Technology (No.192102210280), The Innovative Scientists and Technicians Team of Henan Provincial High Education (No.20IRTSTHN013), The Innovative Research Team of Henan Polytechnic University (No.T2018-1)

发布交通路况信息、天气预报信息和物价信息等不同资源信息的多个服务器。云端计算节点如图 1 所示。云服务提供商不希望用户没有限制地访问其经营的计算节点，如果用户要获得某个节点上的服务，就需要付费购买相应的访问权限。实际中，如何控制终端用户对计算节点的访问权限是一个重要的研究课题。属性基加密（ABE, attribute-based encryption）[1]特别是密文策略属性基加密（CP-ABE, ciphertext-policy attribute based encryption）[2]，允许数据拥有者为加密数据制定灵活的访问策略并且不需要预先获知接收方的具体身份，可以实现细粒度访问控制和支持一对多通信模式。因此，ABE 被视为实现终端用户对计算节点访问控制的一个理想途径。

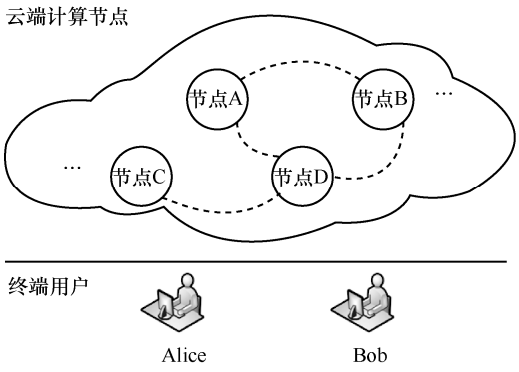


图 1　云端计算节点

然而，ABE 本身存在的一些安全问题制约了其在访问控制方面的应用。大多数关于 ABE 的文献[1-5]主要关注并且可以保证抗串谋攻击。如图 1 所示，假设用自然数表示属性，用户 Alice 拥有属性 $\{1,3,5\}$，用户 Bob 拥有属性 $\{2,4,6\}$，节点 C 上的访问策略为“$1 \wedge 4 \wedge 6$”。显然无论 Alice 还是 Bob 都不能单独访问节点 C，但是如果 Alice 和 Bob 获得他们属性集合的超集 $\{1,2,3,4,5,6\}$，那么他们就可以访问节点 C。为了避免这种情况，ABE 需要保证抗串谋，也就是要保证“用户不能派生超集”。然而，派生超集的逆过程派生子集在已有的关于 ABE 的文献中缺少充分的关注[6-7]。为了更好地说明“用户派生子集”问题对 ABE 安全性的影响，可以考虑下面一个具体的场景。

如图 1 所示，假设一个云服务提供商 P 经营 4 个云计算节点 A、B、C 和 D，其中每个节点的接入服务售价是 7 元/月。用户 Alice 支付 28 元给 P 从而购得 A、B、C 和 D 的访问权限，访问权限对应的属性集合为 $S = S_A \cup S_B \cup S_C \cup S_D$。其中，$S_A$、$S_B$、$S_C$ 和 S_D 是 S 的子集，并且可以分别用于访问节点 A、B、C 和 D。此时若允许“用户派生子集”，Alice 就可以从中谋取利益。例如 Alice 分别生成关联属性集合 S_A、S_B、S_C 和 S_D 的 4 个用户私钥，并且以 5 元/月销售每个用户私钥；Alice 又分别生成关联属性集合 $S_A \cup S_B$，$S_B \cup S_C$ 和 $S_C \cup S_D$ 的 3 个用户私钥，并且以 10 元/月销售每个用户私钥。注意，Alice 派生 S 的子集可以是 S_A、S_B、S_C 和 S_D 中的单个，也可以是其中任意 2 个的并集、任意 3 个的并集或者全部 4 个的并集，因此 S 的子集不只限于以上的例子。当 Alice 成功出售这 7 个用户私钥时，她将获得 50 元的收入。显然与 Alice 最初购买访问权限所支付的 28 元相比，她得到了非正常的经济利益。另外，由于 Alice 比 P 的售价低，更易获得潜在用户的青睐，使 Alice 会对合法的服务提供商 P 造成严重的竞争威胁。因此，ABE 不仅要保证“用户不能派生超集”，还应保证“用户不能派生子集”。文献[7]将“用户不能派生子集”正式定义为抗密钥委托滥用（key-delegation abuse resistance）。

除了抗串谋和抗密钥委托滥用外，可追踪性也是 ABE 需要实现的安全保障。由于 ABE 中用户私钥仅与用户持有的属性有关，而不同的用户可能持有相同的属性，当发生用户私钥泄露时，如何确定泄露用户私钥的恶意用户就成为 ABE 中重要的可追踪问题[8]。继续考虑上述场景，假使 Alice“不能派生子集”，但是如果其可以直接泄露关联属性集合 S 的用户私钥而不被追踪发现，那么仍然能够通过直接泄露自己的私钥给非授权用户来获得非法利益。因此，实现 ABE 的可追踪性是十分必要的。

当前研究工作缺乏对既支持抗密钥委托滥用又具有可追踪功能的 ABE 方案的关注。一方面，现有可追踪 ABE 方案不具备上述场景要求的“抗用户派生子集”的能力。他们声称的抗密钥滥用能力大多是利用追踪功能对泄露自己部分或全部解密密钥的用户起到威慑作用。实际上，用户仍然能将自己属性集合的一部分（即子集）所关联的部分解密密钥泄露给非授权的第三方，部分解密密钥只有完整解密密钥中的部分组件，但仍然可以完成正确的解密操作。因此，通过追踪功能而附带产生的抗密钥滥用能力是不完备的，只能起到

威慑和事后追责的作用，而不能在事前避免“用户派生子集”。

文献[7]扩展方案提出了一种雾计算中抗密钥委托滥用且可追踪的 CP-ABE 方案，但是该方案效率不高。具体而言，文献[7]扩展方案的追踪方法如下。将用户的身份标识编码成虚拟属性，并将虚拟属性加入真实的属性集合中。当用户泄露自己的私钥时，用户私钥所关联的虚拟属性连同真实属性会被一起泄露，从而可以通过解析虚拟属性得到其对应的用户身份标识，实现对恶意用户的可追踪。然而，该追踪方法导致文献[7]扩展方案的公共参数大小、密文大小、用户私钥大小及加密和解密计算量都与用户身份标识编码后的长度线性相关，制约了文献[7]扩展方案的执行效率。

综上所述，为了克服现有可追踪 ABE 方案在抗密钥委托滥用上的不足，以及改善文献[7]扩展方案效率不高的问题，本文从改进文献[7]扩展方案性能出发，在继承其抗密钥委托滥用优点的基础上，采用一种更为高效的追踪方法，提出一种新的抗密钥委托滥用的可追踪属性基加密方案。本文的主要创新点如下。

1) 为了同时支持抗密钥委托滥用和可追踪，本文方案借鉴文献[9]中“粘合”属性层和秘密分享层的思想，将抗密钥委托滥用功能和可追踪功能视为 2 个分离的层，即抗密钥委托滥用层和可追踪层，并且设计了 2 个独立的参数 α 和 β。将 α 嵌入抗密钥委托滥用层，将 β 嵌入可追踪层。最终，通过 α 和 β 之间的运算，实现抗密钥委托滥用层和可追踪层之间的“粘合”，从而使本文方案同时获得了抗密钥委托滥用和可追踪 2 个重要的功能。

2) 本文方案采用文献[8]中基于短签名[10]结构的追踪方法，与文献[7]扩展方案相比，公共参数、密文和用户私钥的尺寸更短，加密和解密的计算量更小，从而获得了更高效的性能。

3) 本文方案的可追踪性证明基于标准模型上的安全游戏，比文献[7]扩展方案基于一般双线性群模型（generic bilinear group model）的可追踪性证明更加严格，安全性更高。

2 相关工作

正如前文场景所述，抗密钥委托滥用和可追踪是 ABE 需要实现的重要安全保证。在可追踪 ABE 方面，Liu 等[8]利用一种短签名结构保护用于追踪的参数，提出了一种支持任意单调访问结构的白盒可追踪 CP-ABE 方案。Liu 等[8]指出 ABE 中存在 2 种类型的追踪：白盒追踪和黑盒追踪。白盒追踪中追踪算法根据被泄露的用户私钥进行追踪；黑盒追踪中追踪算法只能根据解密设备进行追踪，而参与构造解密设备的用户私钥和解密算法是隐藏的，因此解密设备也被称为黑盒。Ning 等[11]采用与文献[8]相似的追踪结构，提出了一种支持大属性集且追踪存储开销为常数级的白盒可追踪 CP-ABE 方案。在抗密钥滥用 ABE 方面，现有相关文献[12-18]大多利用追踪方法来解决密钥滥用问题，因此它们也属于可追踪 ABE 的研究范畴。但是，可追踪性对于想要泄露用户私钥的用户来说只能起到威慑作用，实际上，用户仍然具有派生子集的能力。为了真正实现抗用户派生子集，Jiang 等[6]设计了一个新的 CP-ABE 方案，其中解密操作要求全部属性的共同参与，如果只拥有全部属性的一部分（即子集），则不能完成正确的解密操作，从而真正达到抗用户派生子集的目的。Jiang 等[7]进一步将他们实现的抗用户派生子集 CP-ABE 方案应用到雾计算中，并且正式将这种性质定义为抗密钥委托滥用。用抗密钥滥用来表达文献[12-18]的工作是为了与 Jiang 等[6-7]所实现的抗密钥委托滥用进行区分。此外，Qiao 等[19]提出了一个雾计算中支持黑盒追踪的 CP-ABE 方案，但他们解决权限滥用（即密钥滥用）问题的方式仍然依赖于方案的可追踪性。

3 预备知识

3.1 访问结构

本文定义的访问结构 $\mathbb{A}$ 由与门（用符号“$\wedge$”表示）构成，即 $\mathbb{A}=\underset{i\in W}{\wedge} i$，其中，$W$ 表示属性全集的一个子集，i 表示一个属性。给定一个属性集合 S，S 满足 $\mathbb{A}$ 当且仅当 $W\subseteq S$。

文献[7]实现抗用户派生子集的方法依赖于与门访问结构，本文方案沿用了文献[7]的技术思路，所以本文方案仅支持与门访问结构。

3.2 判定性双线性 Diffie-Hellman 假设

假设 1 设 $\mathbb{G}$ 是阶为素数 p 的双线性群，g 是 $\mathbb{G}$ 的一个生成元，e 是 $\mathbb{G}$ 上双线性映射。判定性双线性 Diffie-Hellman（DBDH, decisional bilinear

Diffie-Hellman）假设是指挑战者随机选取 $a,b,c,z\in\mathbb{Z}_p$，$\mathbb{Z}_p$ 为模 p 的剩余类集，不存在多项式时间的攻击者能以不可忽略的优势正确区分下面 2 个元组。

$$\left(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc}\right)$$

$$\left(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{z}\right)$$

3.3 *l*-SDH 假设

假设 2　设 $\mathbb{G}$ 是阶为素数 p 的双线性群，g 是 $\mathbb{G}$ 的一个生成元。$\mathbb{G}$ 上的 l-强 Diffie-Hellman（l-SDH, l-strong Diffie-Hellman）问题定义为：给定 $(l+1)$ 元组 $\left(g,g^x,g^{x^2},\cdots,g^{x^l}\right)$ 作为输入，输出 $\left(c,g^{\frac{1}{x+c}}\right)$ 使 $c\in\mathbb{Z}_p$ 且 $g^{\frac{1}{x+c}}\in\mathbb{G}$。算法 $\mathcal{A}$ 可以优势 ϵ 攻破 $\mathbb{G}$ 上的 l-SDH 假设，如果 $\Pr[\mathcal{A}(g,g^x,g^{x^2},\cdots,g^{x^l})=(c,g^{\frac{1}{x+c}})]\geqslant\epsilon$，其中 x 是从 $\mathbb{Z}_p^*$ 中随机选取的元素。

定义 1　$\mathbb{G}$ 上的 (l,t,ϵ)-SDH 假设成立，如果不存在 t-时间的算法可以至少 ϵ 的优势解决 $\mathbb{G}$ 上的 l-SDH 问题。

4　算法与安全模型定义

4.1　算法定义

本文方案由 5 个算法组成，分别是系统初始化算法 setup、加密算法 encrypt、用户私钥生成算法 KeyGen、解密算法 decrypt 和追踪算法 trace。具体算法定义如下。

1) $\text{setup}(\kappa,\mathcal{U})\to(\text{PK},\text{MK})$。ABE 系统的建立者执行初始化算法 setup。算法以安全参数 κ 和属性全集 $\mathcal{U}$ 作为输入，输出公共参数 PK 和主密钥 MK，并初始化追踪表 $T=\varnothing$，$\varnothing$ 为空集。MK 和 T 由机构（authority）持有和维护。

2) $\text{encrypt}(\text{PK},\mathbb{A},m)\to\text{CT}$。加密方执行加密算法 encrypt。算法以公共参数 PK、属性全集 $\mathcal{U}$ 上的访问结构 $\mathbb{A}$ 和消息 m 作为输入，输出密文 CT。其中访问结构 $\mathbb{A}$ 包含在 CT 中。

3) $\text{KeyGen}(\text{PK},\text{MK},\text{id},S)\to\text{SK}$。机构执行用户私钥生成算法 KeyGen。算法以公共参数 PK、主密钥 MK、用户身份 id 和用户属性集合 S 作为输入，输出用户私钥 SK。

4) $\text{decrypt}(\text{PK},\text{CT},\text{SK})\to m$ or $\perp$。用户执行解密算法 decrypt。算法以公共参数 PK、密文 CT 和用户私钥 SK 作为输入。如果 SK 关联的用户属性满足 CT 中的访问结构，则算法输出消息 m；否则输出 $\perp$，表示解密失败。

5) $\text{trace}(\text{PK},\text{SK},T)\to\text{id}$ or $\top$。机构执行追踪算法 trace。如果不考虑隐私保护，公开追踪表 T，则可以进行公开的追踪操作。算法以公共参数 PK、用户私钥 SK 和追踪表 T 作为输入。如果 SK 是格式良好的，则算法查询追踪表 T 并输出 SK 关联的用户身份 id。如果 SK 不是格式良好的，则算法输出 $\top$，表示 SK 不需要被追踪。“SK 是格式良好的”意味着 SK 可以通过格式检查条件，保证 SK 可以被用于正常的解密过程。

4.2　方案安全模型定义

本文采用文献[7]定义的方案安全模型，该模型定义为挑战者与攻击者之间交互的安全游戏，该游戏是选择明文攻击（CPA, chosen plaintext attack）下的不可区分性（IND, indistinguishability）游戏，即 IND-CPA 游戏。具体描述如下。

1) 初始化前，攻击者将欲挑战的访问结构 $\mathbb{A}^*$ 传递给挑战者。

2) 初始化，挑战者运行初始化算法，将公共参数 PK 传递给攻击者。

3) 阶段 1，攻击者向挑战者询问 $(\text{id}_1,S_1),\cdots,(\text{id}_{q_1},S_{q_1})$ 关联的用户私钥，其中，id 为用户身份，S 为该用户的属性集合。

4) 挑战，攻击者向挑战者提交 2 个等长的消息 m_0 和 m_1。挑战者掷一枚均匀的硬币 $\eta\in\{0,1\}$，并在 $\mathbb{A}^*$ 下加密 m_η 生成挑战密文 CT^*。挑战者将 CT^* 传递给攻击者。

5) 阶段 2，攻击者向挑战者询问 $(\text{id}_{q_1+1},S_{q_1+1}),\cdots,(\text{id}_1,S_1)$ 关联的用户私钥。

6) 猜测，攻击者输出对 η 的猜测 η'。

如果 $\eta'=\eta$ 并且用于询问的用户属性集合 $S_1,\cdots,S_q$ 不能满足访问结构 $\mathbb{A}^*$，攻击者赢得上述游戏。攻击者赢得上述游戏的优势定义为 $\left|\Pr[\eta'=\eta]-\frac{1}{2}\right|$。

定义 2　如果所有多项式时间的攻击者在上述安全游戏中至多有可忽略的优势，则本文方案是选择性安全和 IND-CPA 安全的。

4.3 可追踪性模型定义

本文采用文献[8]定义的可追踪性模型，其中可追踪性定义为挑战者与攻击者之间交互的安全游戏。具体描述如下。

1) 初始化。挑战者运行初始化算法，将公共参数 PK 传递给攻击者。

2) 密钥询问。攻击者向挑战者询问 $(\mathrm{id}_1,S_1),\cdots,(\mathrm{id}_q,S_q)$ 关联的用户私钥。

3) 密钥伪造。攻击者输出一个用户私钥 SK_*。

如果 $\mathrm{trace}(\mathrm{PK},\mathrm{SK}_*,T)\neq\top$（即 SK_* 是格式良好的），并且 $\mathrm{trace}(\mathrm{PK},\mathrm{SK}_*,T)\notin\{\mathrm{id}_1,\cdots,\mathrm{id}_q\}$，其中 id_i 为用于询问的用户身份（$i=1,\cdots,q$），攻击者赢得上述游戏。攻击者赢得上述游戏的优势定义为 $\Pr[\mathrm{trace}(\mathrm{PK},\mathrm{SK}_*,T)\notin\{\top\}\cup\{\mathrm{id}_1,\cdots,\mathrm{id}_q\}]$。

定义 3 如果所有多项式时间的攻击者在上述可追踪性游戏中至多有可忽略的优势，则本文方案是可追踪的。

可追踪性模型之所以没有考虑“实际恶意用户是 id_m，但追踪到的是 id_n（$m,n\in\{1,\cdots,q\}$ 且 $m\neq n$）”的情况，是因为本文方案的具体构造保证攻击者不能采用这种方式抗追踪，具体原因如下。由第 5 节可知，追踪算法利用参数 r 追踪用户 id，对应关系 (r,id) 存储于追踪表 T。假设用户 id_m 的私钥为

$$\mathrm{SK}^{(m)}=\left(K=g^{\frac{\beta}{d+r^{(m)}}}g^{\delta t^{(m)}},K'=r^{(m)},K_0=g^{t^{(m)}},\left\{K_i=g^{\frac{x_i^{(m)}}{t_i}}\right\}_{i\in S^{(m)}},\left\{K_i=g^{\frac{x_i^{(m)}}{t_{n+i}}}\right\}_{i\in\mathcal{U}\setminus S^{(m)}}\right)$$

用户 id_n 的私钥为

$$\mathrm{SK}^{(n)}=\left(K=g^{\frac{\beta}{d+r^{(n)}}}g^{\delta t^{(n)}},K'=r^{(n)},K_0=g^{t^{(n)}},\left\{K_i=g^{\frac{x_i^{(n)}}{t_i}}\right\}_{i\in S^{(n)}},\left\{K_i=g^{\frac{x_i^{(n)}}{t_{n+i}}}\right\}_{i\in\mathcal{U}\setminus S^{(n)}}\right)$$

如果攻击者用 id_n 代替 id_m，则会输出私钥

$$\mathrm{SK}_*=\left(K=g^{\frac{\beta}{d+r^{(n)}}}g^{\delta t^{(n)}},K'=r^{(n)},K_0=g^{t^{(m)}},\left\{K_i=g^{\frac{x_i^{(m)}}{t_i}}\right\}_{i\in S^{(m)}},\left\{K_i=g^{\frac{x_i^{(m)}}{t_{n+i}}}\right\}_{i\in\mathcal{U}\setminus S^{(m)}}\right)$$

显然，SK_* 中发生了参数 t 不匹配的情况，即 K 中是 $t^{(n)}$，而 K_0 和 $\{K_i\}$ 中是 $t^{(m)}$（$\{K_i\}$ 中隐含参数 t，参见第 5 节）。这样 SK_* 就不能用于正常的解密，SK_* 也就失去了被追踪的意义。实际上，设置参数 t 是为了保证 SK 中组件的“配套”，防止用户串谋。

由上述分析可知，攻击者不能采用“用 id_n 代替 id_m”的抗追踪方式，因此可追踪性模型没有考虑这种情况。

5 方案构造

本节主要展示方案的具体构造并对相关参数进行说明，其中每种算法的执行者已经在 4.1 节中明确指出。具体方案如下。

1) 初始化 $\mathrm{setup}(\kappa,\mathcal{U})\to(\mathrm{PK},\mathrm{MK})$

首先，运行群生成算法 $(p,g,\mathbb{G},\mathbb{G}_T,e)\leftarrow\mathcal{G}(\kappa)$，输入安全参数 κ，输出循环群的描述。其中，$\mathbb{G}$ 和 $\mathbb{G}_T$ 是阶为素数 p 的循环群，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是双线性映射，g 是群 $\mathbb{G}$ 的生成元。属性全集 $\mathcal{U}=\{1,\cdots,n\}$。

随机选取 $\alpha,\beta,\delta\leftarrow_R\mathbb{Z}_p$，$d\leftarrow_R\mathbb{Z}_p^*$，$t_1,\cdots,t_{2n}\leftarrow_R\mathbb{Z}_p$。计算 $h_1=g^{t_1}$，…，$h_n=g^{t_n}$，$h_{n+1}=g^{t_{n+1}}$，…，$h_{2n}=g^{t_{2n}}$ 和 $Y=e(g,g)^{\alpha+\beta}$。输出公共参数 $\mathrm{PK}=\left(g,g^d,Y,\{h_i\}_{i=1}^{2n}\right)$，主密钥 $\mathrm{MK}=\left(\alpha,\beta,\delta,d,\{t_i\}_{i=1}^{2n}\right)$。初始化追踪表 $T=\varnothing$。

2) 加密 $\mathrm{encrypt}(\mathrm{PK},\mathbb{A},m)\to\mathrm{CT}$

消息 $m\in\mathbb{G}_T$，访问结构 $\mathbb{A}=\underset{i\in W}{\wedge}i$，其中，$W$ 为加密者指定的 $\mathcal{U}$ 的一个子集，i 表示一个属性。随机选取 $s\leftarrow_R\mathbb{Z}_p$，$s$ 为欲分享的秘密。输出密文

$$\mathrm{CT}=\left(\bar{C}=mY^s,C_0=g^s,C_0'=g^{ds},\{C_i=h_i^s\}_{i\in W},\{C_i=h_{n+i}^s,C_i'=h_i^s\}_{i\in\mathcal{U}\setminus W},\mathbb{A}\right)$$

3) 用户私钥生成 $\mathrm{KeyGen}(\mathrm{PK},\mathrm{MK},\mathrm{id},S)\to\mathrm{SK}$

随机选取 $r\leftarrow_R\mathbb{Z}_p^*$，$t\leftarrow_R\mathbb{Z}_p$，其中 r 关联用户身份 id 作为追踪参数。随机选取 $x_1,\cdots,x_{n-1}\leftarrow_R\mathbb{Z}_p$，并计算 $x_n=\alpha-(d+r)(\delta t+t)-x_1-\cdots-x_{n-1}\in\mathbb{Z}_p$。

输出用户私钥

$$\mathrm{SK}=\left(K=g^{\frac{\beta}{d+r}}g^{\delta t},K'=r,K_0=g^t,\left\{K_i=g^{\frac{x_i}{t_i}}\right\}_{i\in S},\left\{K_i=g^{\frac{x_i}{t_{n+i}}}\right\}_{i\in\mathcal{U}\setminus S}\right)$$

其中，$\frac{1}{d+r}$ 表示 $(d+r)$ 模 p 下的逆元，当“r 已经在 T 中”发生时，随机选取新的 $r\in\mathbb{Z}_p^*$ 并重复上述操作。最后，将对应关系 (r,id) 存入 T 中。

4) 解密 $\mathrm{decrypt}(\mathrm{PK},\mathrm{CT},\mathrm{SK})\to m$ or $\perp$

解析 CT 和 SK 中的参数，CT 中的访问结构 $\mathbb{A}=\underset{i\in W}{\wedge}i$，SK 中的用户属性集合 S，如果 $W\subseteq S$，则算法进行解密过程；否则，算法输出 $\perp$，表示解密失败。解密过程如下。计算 F 和 J。

$$F=\prod\nolimits_{i\in W\cup\{\mathcal{U}\setminus S\}}e(K_i,C_i)\prod\nolimits_{i\in S\setminus W}e(K_i,C_i')=$$

$$\prod\nolimits_{i\in W}e(K_i,C_i)\prod\nolimits_{i\in\mathcal{U}\setminus S}e(K_i,C_i)\prod\nolimits_{i\in S\setminus W}e(K_i,C_i')=$$

$$\prod\nolimits_{i\in S}e\left(g^{\frac{x_i}{t_i}},g^{t_i s}\right)\prod\nolimits_{i\in\mathcal{U}\setminus S}e\left(g^{\frac{x_i}{t_{n+i}}},g^{t_{n+i}s}\right)=$$

$$\prod\nolimits_{i\in\mathcal{U}}e(g,g)^{sx_i}=e(g,g)^{s\sum_{i\in\mathcal{U}}x_i}=$$

$$e(g,g)^{\alpha s}\,e(g,g)^{-(d+r)\delta ts}\,e(g,g)^{-(d+r)ts}$$

$$J=e\left(KK_0,C_0^{K'}C_0''\right)=e\left(g^{\frac{\beta}{d+r}}g^{\delta t}g^t,g^{(d+r)s}\right)=$$

$$e(g,g)^{\beta s}\,e(g,g)^{(d+r)\delta ts}\,e(g,g)^{(d+r)ts}$$

通过 $\frac{\bar{C}}{FJ}$，恢复消息 m。

5) 追踪 $\mathrm{trace}(\mathrm{PK},\mathrm{SK},T)\to\mathrm{id}$ or $\top$

如果 SK 同时满足下述 2 个用户私钥格式检查条件，则 SK 是格式良好的；否则，SK 不是格式良好的，算法输出 $\top$。

用户私钥格式检查条件如下。

① $K'\in\mathbb{Z}_p$，$K,K_0,K_i\in\mathbb{G}$。

② $e\left(K\cdot K_0,g^{K'}g^d\right)\prod\limits_{i\in S}e(K_i,h_i)\prod\limits_{i\in\mathcal{U}\setminus S}e(K_i,h_{n+i})=Y\neq 1$。

当 SK 格式良好时，算法在 T 中查询 r（$K'=r$），如果 r 存在，则输出对应的 id；否则，输出特殊的符号 $\mathrm{id}_\varnothing$（表示在 T 中没有存储）。

6　方案分析

6.1　方案安全性证明

定理 1　如果 DBDH 假设成立，则本文方案在 4.2 节的安全模型中是选择性安全和 IND-CPA 安全的。

证明　假设存在一个概率多项式时间敌手 $\mathcal{A}$ 可以以不可忽略的优势 ε 攻破本文方案，那么能够构造一个概率多项式时间算法 $\mathcal{B}$ 可以以不可忽略的优势 $\frac{\varepsilon}{2}$ 攻破 DBDH 假设。

挑战者设置阶为素数 p 的群 $\mathbb{G}$ 和 $\mathbb{G}_T$，双线性映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$，$\mathbb{G}$ 的一个生成元 g，随机选取 $a,b,c,z\leftarrow_R\mathbb{Z}_p$。挑战者掷一枚随机均匀的硬币 $\mu\in\{0,1\}$，如果 $\mu=0$，则设置 $(A,B,C,Z)=\left(g^a,g^b,g^c,e(g,g)^{abc}\right)$；否则，设置 $(A,B,C,Z)=\left(g^a,g^b,g^c,e(g,g)^z\right)$。设属性全集 $\mathcal{U}=\{1,\cdots,n\}$。模拟者 $\mathcal{B}$ 收到四元组 (A,B,C,Z) 后，与敌手 $\mathcal{A}$ 进行下面的游戏。

初始化之前 $\mathcal{A}$ 将欲挑战的访问结构 $\mathbb{A}^*=\underset{i\in W^*}{\wedge}i$ 传递给 $\mathcal{B}$，其中 $W^*\subseteq\mathcal{U}$。

初始化　$\mathcal{B}$ 随机选取 $\delta,\theta\leftarrow_R\mathbb{Z}_p$，$d\leftarrow_R\mathbb{Z}_p^*$，$\lambda_1,\cdots,\lambda_n\leftarrow_R\mathbb{Z}_p$，$\gamma_1,\cdots,\gamma_n\leftarrow_R\mathbb{Z}_p$。$\mathcal{B}$ 计算 $h_i|_{i\in\mathcal{U}}=g^{\lambda_i}$，$h_{n+i}|_{i\in W^*}=B^{\gamma_i}=g^{b\gamma_i}$，$h_{n+i}|_{i\in\mathcal{U}\setminus W^*}=g^{\gamma_i}$ 和 $Y=e(A,B)e(g,B)e(g,g^\theta)=e(g,g)^{ab+(b+\theta)}$，其中对 $i\in\mathcal{U}$，令 $t_i=\lambda_i$；对 $i\in W^*$，令 $t_{n+i}=b\gamma_i$；对 $i\in\mathcal{U}\setminus W^*$，令 $t_{n+i}=\gamma_i$；令 $\alpha=ab$，$\beta=b+\theta$（注意，这里在模拟 β 时令 $\beta=b+\theta$，通过加上随机数 θ，使尽管 α 和 β 的模拟中都含有参数 b，但它们仍然满足真实方案中的独立随机性）。然后 $\mathcal{B}$ 将公共参数 $\mathrm{PK}=\left(g,g^d,Y,\{h_i\}_{i=1}^{2n}\right)$ 传递给 $\mathcal{A}$，初始化追踪表 $T=\varnothing$。

阶段 1　$\mathcal{A}$ 向 $\mathcal{B}$ 提交 (id,S)，询问关联的用户私钥，并且要求 $W^*\not\subset S$。$\mathcal{B}$ 随机选取 $r\leftarrow_R\mathbb{Z}_p^*$，计算 $\bar{K}=\left(Bg^\theta\right)^{\frac{1}{d+r}}=g^{\frac{b+\theta}{d+r}}=g^{\frac{\beta}{d+r}}$，$K'=r$，其中 $\frac{1}{d+r}$ 表示 $(d+r)$ 模 p 下的逆元，当“r 已经在 T 中”发生时，随机选取新的 $r\in\mathbb{Z}_p^*$ 并重复上述操作。

因为 $W^*\not\subset S$，所以必定存在一个属性 $k\in W^*$ 使 $k\notin S$，$\mathcal{B}$ 选择这样一个属性 k。$\mathcal{B}$ 随机选取

$t' \leftarrow_R \mathbb{Z}_p$，令 $t = bt'$，计算 $K = \bar{K}B^{\delta t'} = g^{\frac{\beta}{d+r}} g^{\delta b t'} = g^{\frac{\beta}{d+r}} g^{\delta t}$ 和 $K_0 = B^{t'} = g^{bt'} = g^t$。$\mathcal{B}$ 随机选取 $x_1', \cdots, x_{n-1}' \leftarrow_R \mathbb{Z}_p$，并计算 $x_n' = -\sum_{i=1}^{n-1} x_i'$。对 $i \in \mathcal{U} \setminus \{k\}$，令 $x_i = bx_i'$；对 $i = k$，令 $x_k = ab - b(d+r)(\delta t' + t') + bx_k'$。$\mathcal{B}$ 按以下 4 种情况进行计算。

① $\forall i \in S$，$K_i = B^{\frac{x_i'}{\lambda_i}} = g^{\frac{bx_i'}{\lambda_i}} = g^{\frac{x_i}{t_i}}$。

② $\forall i \notin S, i \in W^*, i \neq k$，$K_i = g^{\frac{x_i'}{\gamma_i}} = g^{\frac{bx_i'}{b\gamma_i}} = g^{\frac{x_i}{t_{n+i}}}$。

③ $\forall i \notin S, i \in W^*, i = k$，$K_k = A^{\frac{1}{\gamma_k}} g^{\frac{-(d+r)(\delta t' + t')}{\gamma_k}} g^{\frac{x_k'}{\gamma_k}} = g^{\frac{ab}{b\gamma_k}} g^{\frac{-b(d+r)(\delta t' + t')}{b\gamma_k}} g^{\frac{bx_k'}{b\gamma_k}} = g^{\frac{x_k}{t_{n+k}}}$。

④ $\forall i \notin S, i \notin W^*$，$K_i = B^{\frac{x_i'}{\gamma_i}} = g^{\frac{bx_i'}{\gamma_i}} = g^{\frac{x_i}{t_{n+i}}}$。

$\mathcal{B}$ 传递给 $\mathcal{A}$ 用户私钥

$$\mathrm{SK} = \left(K, K', K_0, \left\{ K_i = g^{\frac{x_i}{t_i}} \right\}_{i \in S}, \left\{ K_i = g^{\frac{x_i}{t_{n+i}}} \right\}_{i \in \mathcal{U} \setminus S} \right)$$

最后将对应关系 (r, id) 存入 T 中。

这里指出 $\mathcal{B}$ 对 x_i（$i \in \mathcal{U}$）模拟的正确性，具体如下。

$$\sum_{i \in \mathcal{U}} x_i = \sum_{i \in \mathcal{U}, i \neq k} x_i + x_k =$$
$$b \sum_{i \in \mathcal{U}, i \neq k} x_i' + ab - b(d+r)(\delta t' + t') + bx_k' =$$
$$ab - b(d+r)(\delta t' + t') = \alpha - (d+r)(\delta t + t)$$

挑战 $\mathcal{A}$ 将 2 个等长的消息 m_0、m_1 提交给 $\mathcal{B}$。$\mathcal{B}$ 随机选取 $\eta \leftarrow_R \{0,1\}$，然后传递给 $\mathcal{A}$ 挑战密文，具体如下。

$$\mathrm{CT}^* = \left(\bar{C} = m_\eta Z e(C, B) e(C, g^\theta), \right.$$
$$C_0 = C = g^c, C_0' = C^d = g^{dc},$$
$$\left\{ C_i = C^{\lambda_i} = h_i^c \right\}_{i \in W^*},$$
$$\left. \left\{ C_i = C^{\gamma_i} = h_{n+i}^c, C_i' = C^{\lambda_i} = h_i^c \right\}_{i \in \mathcal{U} \setminus W^*}, \mathcal{A}^* \right)$$

其中，令秘密 $s = c$。

阶段 2 $\mathcal{A}$ 与 $\mathcal{B}$ 的交互过程同阶段 1。

猜测 $\mathcal{A}$ 将对 η 的猜测 η' 提交给 $\mathcal{B}$。如果 $\eta' = \eta$，则 $\mathcal{B}$ 输出 $\mu' = 0$，表示 $\mathcal{B}$ 收到四元组 $(A, B, C, Z) = \left(g^a, g^b, g^c, e(g,g)^{abc} \right)$；如果 $\eta' \neq \eta$，则 $\mathcal{B}$ 输出 $\mu' = 1$，表示 $\mathcal{B}$ 收到四元组 $(A, B, C, Z) = \left(g^a, g^b, g^c, e(g,g)^z \right)$。

$\mathcal{B}$ 模拟的公共参数、用户私钥和挑战密文与实际方案中的分布是相同的。下面分析 $\mathcal{B}$ 的优势。

当 $\mu = 1$ 时，$\mathcal{A}$ 不能获得 m_η 的有效密文，$\mathcal{A}$ 只能纯粹猜测 η 的值，因此 $\Pr[\eta' \neq \eta \mid \mu = 1] = \frac{1}{2}$。而当 $\eta' \neq \eta$ 时，$\mathcal{B}$ 输出 $\mu' = 1$，所以 $\Pr[\mu' = \mu \mid \mu = 1] = \frac{1}{2}$。

当 $\mu = 0$ 时，$\mathcal{A}$ 可以获得 m_η 的有效密文，由前面的假设可知，$\mathcal{A}$ 攻破本文方案（即解密）的优势是 ε，因此 $\Pr[\eta' = \eta \mid \mu = 0] = \frac{1}{2} + \varepsilon$。而当 $\eta' = \eta$ 时，$\mathcal{B}$ 输出 $\mu' = 0$，所以 $\Pr[\mu' = \mu \mid \mu = 0] = \frac{1}{2} + \varepsilon$。

$\mu = 1$ 发生的概率为 $\frac{1}{2}$，$\mu = 0$ 发生的概率为 $\frac{1}{2}$，$\mathcal{B}$ 纯粹猜测 μ'（使 $\mu' = \mu$）的概率为 $\frac{1}{2}$。综上所述，$\mathcal{B}$ 攻破 DBDH 假设的优势为

$$\mathrm{Adv}_{\mathcal{B},\mathrm{DBDH}} = \left| \Pr[\mu' = \mu] - \frac{1}{2} \right| =$$
$$\Pr[\mu' = \mu \mid \mu = 1] \Pr[\mu = 1] +$$
$$\Pr[\mu' = \mu \mid \mu = 0] \Pr[\mu = 0] - \frac{1}{2} =$$
$$\frac{1}{2} \times \frac{1}{2} + \left(\frac{1}{2} + \varepsilon \right) \times \frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}$$

证毕。

6.2 可追踪性证明

定理 2 如果 l-SDH 假设成立，则本文方案是可追踪的（$q < l$，q 是敌手询问的次数）。

证明 假设存在一个概率多项式时间敌手 $\mathcal{A}$ 在进行 q 次（不妨设 $l = q + 1$）密钥询问后可以以不可忽略的优势 ε 赢得 4.3 节给出的可追踪游戏，那么能够构造一个概率多项式时间算法 $\mathcal{B}$ 可以以不可忽略的优势攻破 l-SDH 假设。

设置 $\mathbb{G}$ 和 $\mathbb{G}_T$ 是阶为素数 p 的循环群，$e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 是双线性映射，$\hat{g} \in \mathbb{G}$ 和 $d \in \mathbb{Z}_p^*$。给出实例 $\mathrm{IN}_{\mathrm{SDH}} = \left(p, \mathbb{G}, \mathbb{G}_T, e, \hat{g}, \hat{g}^d, \cdots, \hat{g}^{d^l} \right)$，$\mathcal{B}$ 的目标

是输出 $\hat{r}\in\mathbb{Z}_p$ 和 $\hat{w}\in\mathbb{G}$ 并满足 $\hat{w}=\hat{g}^{\frac{1}{d+\hat{r}}}$，从而解决 l-SDH 假设。$\mathcal{B}$ 设置 $A_i=\hat{g}^{a^i}$，$i=0,1,\cdots,l$。$\mathcal{B}$ 将 $\left(p,\mathbb{G},\mathbb{G}_T,e,\{A_i\}_{i=0}^{l}\right)$ 作为输入与 $\mathcal{A}$ 进行可追踪游戏。

初始化 $\mathcal{B}$ 随机选取 q 个不同值 $r_1,\cdots,r_q\in\mathbb{Z}_p^*$。令多项式 $f(y)=\prod_{i=1}^{q}(y+r_i)$。展开 $f(y)$，可以得到形式如 $f(y)=\sum_{i=0}^{q}\alpha_i y^i$ 的表达式，其中 $\alpha_0,\alpha_1,\cdots,\alpha_q\in\mathbb{Z}_p$ 是多项式 $f(y)$ 展开式中各项的系数。$\mathcal{B}$ 计算 g 和 g^d。

$$g=\prod_{i=0}^{q}(A_i)^{\alpha_i}=\prod_{i=0}^{q}(\hat{g})^{\alpha_i a^i}=\hat{g}^{f(a)}$$

$$g^d=\prod_{i=1}^{q+1}(A_i)^{\alpha_{i-1}}=\prod_{i=0}^{q}(\hat{g})^{\alpha_i a^i d}=\hat{g}^{f(a)d}$$

$\mathcal{B}$ 随机选取 $\alpha,\beta,\delta\leftarrow_R\mathbb{Z}_p$，$t_1,\cdots,t_{2n}\leftarrow_R\mathbb{Z}_p$（设属性全集 $\mathcal{U}=\{1,\cdots,n\}$）。$\mathcal{B}$ 计算 $h_1=g^{t_1}$，…，$h_n=g^{t_n}$，$h_{n+1}=g^{t_{n+1}}$，…，$h_{2n}=g^{t_{2n}}$ 和 $Y=e(g,g)^{\alpha+\beta}$，然后将公共参数 $\mathrm{PK}=\left(g,g^d,Y,\{h_i\}_{i=1}^{2n}\right)$ 传递给 $\mathcal{A}$，并初始化追踪表 $T=\varnothing$。

密钥询问 $\mathcal{A}$ 提交 (id_i,S_i) 给 $\mathcal{B}$，询问关联的用户私钥 SK_i。假设这是 $\mathcal{A}$ 的第 i 次询问（$i\leqslant q$）。令多项式 $f_i(y)=\frac{f(y)}{y+r_i}=\prod_{j=1,j\neq i}^{q}(y+r_j)$。展开 $f_i(y)$，可以得到形式如 $f_i(y)=\sum_{j=0}^{q-1}\beta_j y^j$ 的表达式，其中 $\beta_0,\beta_1,\cdots,\beta_{q-1}\in\mathbb{Z}_p$ 是多项式 $f_i(y)$ 展开式中各项的系数。$\mathcal{B}$ 计算

$$w_i=\prod_{j=0}^{q-1}(A_j)^{\beta_j}=\prod_{j=0}^{q-1}(\hat{g})^{\beta_j a^j}=\hat{g}^{\frac{f(a)}{a+r_i}}=g^{\frac{1}{a+r_i}}$$

$\mathcal{B}$ 随机选取 $t\leftarrow_R\mathbb{Z}_p$，$x_1',\cdots,x_{n-1}'\leftarrow_R\mathbb{Z}_p$，并计算 $x_n'=\alpha-x_1'-\cdots-x_{n-1}'\in\mathbb{Z}_p$。然后计算用户私钥组件

$$K=(w_i)^{\beta}g^{\delta t}=g^{\frac{\beta}{d+r_i}}g^{\delta t},\quad K'=r_i,\quad K_0=g^t,$$

$$\left\{K_k=\left(g^{x_k'}\left(g^d g^{r_i}\right)^{\frac{-(\delta t+t)}{n}}\right)^{\frac{1}{t_k}}=g^{\frac{x_k'-\frac{(d+r_i)(\delta t+t)}{n}}{t_k}}\right\}_{k\in S_i},$$

$$\left\{K_k=\left(g^{x_k'}\left(g^d g^{r_i}\right)^{\frac{-(\delta t+t)}{n}}\right)^{\frac{1}{t_{n+k}}}=g^{\frac{x_k'-\frac{(d+r_i)(\delta t+t)}{n}}{t_{n+k}}}\right\}_{k\in\mathcal{U}\setminus S_i},$$

其中，令 $x_k=x_k'-\frac{(d+r_i)(\delta t+t)}{n}$。这里指出 $\mathcal{B}$ 对 x_k（$k\in\mathcal{U}$）模拟的正确性如下。

$$\sum_{k\in\mathcal{U}}x_k=\sum_{k\in\mathcal{U}}\left(x_k'-\frac{(d+r_i)(\delta t+t)}{n}\right)=$$

$$\sum_{k\in\mathcal{U}}x_k'-n\left(\frac{(d+r_i)(\delta t+t)}{n}\right)=$$

$$\alpha-(d+r_i)(\delta t+t)$$

$\mathcal{B}$ 将对应关系 (r_i,id_i) 存入 T 中，并将用户私钥 $\mathrm{SK}_i=\left(K,K',K_0,\{K_k\}_{k\in S_i},\{K_k\}_{k\in\mathcal{U}\setminus S_i}\right)$ 传递给 $\mathcal{A}$。SK_i 表示 $\mathcal{A}$ 第 i 次询问得到的用户私钥。

密钥伪造 $\mathcal{A}$ 将用户私钥 SK_* 提交给 $\mathcal{B}$。

注意到，可追踪游戏中 $\mathcal{B}$ 模拟的公共参数和用户私钥与实际方案中的分布是相同的。

令 $E_{\mathcal{A}}$ 表示 $\mathcal{A}$ 赢得可追踪游戏，即 SK_* 满足第 5 节中用户私钥格式检查的 2 个条件，并且 SK_* 中的 $K'\notin\{r_1,\cdots,r_q\}$。由证明开始时的假设，有 $\Pr[E_{\mathcal{A}}]=\varepsilon$。下面讨论 $E_{\mathcal{A}}$ 的发生对 $\mathcal{B}$ 解决 l-SDH 假设的帮助。

当 $E_{\mathcal{A}}$ 发生时，$\mathcal{B}$ 做多项式除法 $\frac{f(y)}{y+K'}$，商为 $\varphi(y)=\sum_{i=0}^{q-1}\gamma_i y^i$，余项 $\bar{\gamma}\in\mathbb{Z}_p$（$\bar{\gamma}\neq 0$，因为 $f(y)=\prod_{i=1}^{q}(y+r_i)$，$r_1,\cdots,r_q\in\mathbb{Z}_p^*$ 且 $K'\notin\{r_1,\cdots,r_q\}$，即 $(y+K')$ 不能整除 $f(y)$），进而 $f(y)$ 可以写作 $f(y)=\varphi(y)(y+K')+\bar{\gamma}$。因为 p 为素数，$\bar{\gamma}\in\mathbb{Z}_p$ 且 $\bar{\gamma}\neq 0$，所以 $\bar{\gamma}$ 与 p 互素，即它们的最大公约数 $\gcd(\bar{\gamma},p)=1$。因此 $\bar{\gamma}$ 在模 p 下存在逆元 $\frac{1}{\bar{\gamma}}\bmod p$。此时 $\mathcal{B}$ 可以按照以下方式计算 $(\hat{r},\hat{w})$。

根据第 5 节用户私钥格式检查条件②，假设 SK_* 中 $K_0=g^t$，那么有 $K=g^{\frac{\beta}{d+K'}}g^{\delta t}$。$\mathcal{B}$ 计算 $\frac{1}{\bar{\gamma}}\bmod p$，然后计算

$$w=\left(\frac{K}{K_0^{\delta}}\right)^{\beta^{-1}\bmod p}=\left(\frac{g^{\frac{\beta}{d+K'}}g^{\delta t}}{\left(g^t\right)^{\delta}}\right)^{\beta^{-1}\bmod p}=$$

$$g^{\frac{1}{d+K'}}=\hat{g}^{\frac{f(a)}{d+K'}}=\hat{g}^{\frac{\varphi(a)(d+K')+\bar{\gamma}}{d+K'}}=\hat{g}^{\varphi(a)}\hat{g}^{\frac{\bar{\gamma}}{d+K'}}$$

$$\hat{w}=\left(w\prod_{i=0}^{q-1}(A_i)^{-\gamma_i}\right)^{\frac{1}{\bar{\gamma}}}=\left(\hat{g}^{\varphi(d)}\hat{g}^{\frac{\bar{\gamma}}{d+K'}}\prod_{i=0}^{q-1}\hat{g}^{-\gamma_i d^i}\right)^{\frac{1}{\bar{\gamma}}}=$$

$$\left(\hat{g}^{\varphi(d)}\hat{g}^{\frac{\bar{\gamma}}{d+K'}}\hat{g}^{-\varphi(d)}\right)^{\frac{1}{\bar{\gamma}}}=\hat{g}^{\frac{1}{d+K'}}$$

$$\hat{r}=K'\bmod p$$

因为 $e\left(\hat{g}^d\hat{g}^{\hat{r}},\hat{w}\right)=e\left(\hat{g}^d\hat{g}^{K'},\hat{g}^{\frac{1}{d+K'}}\right)=e\left(\hat{g},\hat{g}\right)$，所以 $(\hat{r},\hat{w})$ 是 l-SDH 假设的一个解。因此有 $\Pr\left[E_{\mathrm{SDH}}(\hat{r},\hat{w})\,|\,E_{\mathcal{A}}\right]=1$，其中 $E_{\mathrm{SDH}}(\hat{r},\hat{w})$ 表示 $(\hat{r},\hat{w})$ 是 l-SDH 假设的一个解。

综上可知，$\mathcal{B}$ 攻破 l-SDH 假设的概率为

$$\begin{aligned}&\Pr\left[E_{\mathrm{SDH}}(\hat{r},\hat{w})\right]=\\&\Pr\left[E_{\mathrm{SDH}}(\hat{r},\hat{w})\,|\,\overline{E_{\mathcal{A}}}\right]\Pr\left[\overline{E_{\mathcal{A}}}\right]+\\&\Pr\left[E_{\mathrm{SDH}}(\hat{r},\hat{w})\,|\,E_{\mathcal{A}}\right]\Pr\left[E_{\mathcal{A}}\right]=\\&0\times(1-\varepsilon)+1\times\varepsilon=\varepsilon\end{aligned}$$

其中，在没有任何帮助的情况下 $\mathcal{B}$ 解决 l-SDH 假设的概率被认为是可以忽略的，为方便计算，设其为 0。则 $\mathcal{B}$ 攻破 l-SDH 假设的优势为

$$\mathrm{Adv}_{\mathcal{B},\mathrm{SDH}}=\left|\Pr\left[E_{\mathrm{SDH}}(\hat{r},\hat{w})\right]-0\right|=|\varepsilon-0|=\varepsilon$$

因此，$\mathcal{B}$ 可以以不可忽略的优势 ε 攻破 l-SDH 假设。

证毕。

6.3 抗密钥委托滥用性证明

本文方案中，只有当敌手可以不利用全部属性而采用其他的方法重构出秘密参数 α 时，敌手才能实现密钥委托。但是，用户私钥中与 α 有关的参数只有 $\{K_i\}_{i\in\mathcal{U}}$，并且只有全部的 K_i 共同参与才能重构出 α。这意味着敌手不能仅由全部属性的子集或者其他不利用全部属性的方法将 α 重构出来，也就是说敌手不能实现密钥委托，所以抗密钥委托滥用性成立。

本文仅给出了证明抗密钥委托滥用性的基本思路，严格的证明过程见文献[7]。

6.4 性能分析

将本文方案与相关方案从性质和性能两方面进行比较。功能和安全性等性质对比如表 1 所示，通信代价和计算代价等性能对比如表 2 所示。为表述方便，将文献[7]中只实现抗密钥委托滥用性的方案称为基础方案，将文献[7]中同时实现抗密钥委托滥用性和可追踪性的方案称为扩展方案。

从表 1 可以看出，本文方案和文献[7]的 2 个方案建立在素数阶群上，而文献[8]方案建立在合数阶群上，有文献指出，素数阶群上的方案比合数阶群上的方案具有更好的执行效率[19]。在功能上，文献[8]方案仅支持可追踪，文献[7]基础方案仅支持抗密钥委托滥用，而本文方案和文献[7]扩展方案既支持抗密钥委托滥用又支持可追踪，因此本文方案和文献[7]扩展方案实现的功能更加全面。然而，本文方案与文献[7]扩展方案实现可追踪性的方法不同，一方面影响方案的性能（具体参见关于表 2 的分析）；另一方面也影响方案的安全性，主要体现在可追踪性证明上。文献[7]扩展方案的可追踪性证明基于一般双线性群模型，而本文方案的可追踪性证明利用标准模型上的安全游戏，相较而言，基于标准模型的证明比基于一般双线性群模型的证明更加严格，因此本文方案比文献[7]扩展方案在可追踪性证明上更具优势。

表 2 中，$|U|$ 表示属性全集的大小，ρ 表示用户身份标识编码后得到的二进制比特串的长度，ℓ 表示访问结构的大小，$|S|$ 表示用户持有属性集合的大小，$|I|$ 表示参与解密过程的属性的数目。公共参数大小、密文大小和用户私钥大小统计的是其中参数的个数。加密和解密计算量统计的是双线性运算 P 的个数、群 $\mathbb{G}$ 上指数运算 E 的个数，以及群 $\mathbb{G}_T$ 上指数运算 E_T 的个数。下面直接从数值上分析表 2 的对比结果。

表 1 不同方案性质对比

方案	抗密钥委托滥用	可追踪	群阶数	可追踪性证明
文献[8]方案	×	√	合数阶	标准模型
文献[7]基础方案	√	×	素数阶	—
文献[7]扩展方案	√	√	素数阶	一般双线性群模型
本文方案	√	√	素数阶	标准模型

表 2　　**相关方案性能对比**

方案	通信代价			计算代价	
	公共参数大小	密文大小	用户私钥大小	加密计算量	解密计算量
文献[8]方案	$\|U\|+4$	$2\ell+3$	$\|S\|+4$	$(3\ell+2)E+E_T$	$(2\|I\|+1)P+2E+\|I\|E_T$
文献[7]基础方案	$2\|U\|+1$	$2\|U\|-\ell+1$	$\|U\|$	$(2\|U\|-\ell)E+E_T$	$\|U\|P$
文献[7]扩展方案	$2(\|U\|+\rho)+1$	$2(\|U\|+\rho)-\ell+1$	$\|U\|+\rho$	$(2(\|U\|+\rho)-\ell)E+E_T$	$(\|U\|+\rho)P$
本文方案	$2\|U\|+3$	$2\|U\|-\ell+3$	$\|U\|+3$	$(2\|U\|-\ell+2)E+E_T$	$(\|U\|+1)P+E$

结合表 1 的性质对比，从表 2 可以看出，本文方案与文献[8]方案相比，虽然通信代价和计算代价更大，但是这些开销是为了使本文方案获得文献[8]方案所不具备的抗密钥委托滥用性，从而实现更好的安全保障，因此本文方案做出这样的性能牺牲是合理的。本文方案与文献[7]基础方案相比，公共参数大小增加了 2，密文大小增加了 2，用户私钥大小增加了 3；加密计算量中群 $\mathbb{G}$ 上指数运算增加了 2，解密计算量中双线性运算增加了 1 并增加了一个群 $\mathbb{G}$ 上指数运算，而功能上本文方案比文献[7]基础方案增加了可追踪性。也就是说与文献[7]基础方案相比，本文方案在获得可追踪性的同时虽然增加了性能开销，但是增加的性能开销仅仅是常数量。本文方案与文献[7]扩展方案相比，公共参数大小减小了 $2\rho-2$，密文大小减小了 $2\rho-2$，用户私钥大小减小了 $\rho-3$，加密计算量中群 $\mathbb{G}$ 上指数运算减小了 $2\rho-2$；解密计算量中双线性运算减小了 $\rho-1$，同时增加了一个群 $\mathbb{G}$ 上指数运算。显然在既支持抗密钥委托滥用又支持可追踪的方案中，本文方案具有比文献[7]扩展方案更好的性能。

此外，本文还通过实验仿真对表 2 中方案进行了性能评估。实验运行环境为 Intel(R) Core(TM) i5-7200U CPU @ 2.50 GHz，8.00 GB 内存，Windows10 操作系统。实验程序采用 Java 语言编写，基于 JPBC（Java pairing based cryptography）类库[20]实现双线性运算。由于文献[8]方案建立在合数阶群上，本文方案和文献[7]的 2 种方案建立在素数阶群上，通常在满足相同安全强度时，合数阶方案运行速度慢于素数阶方案运行速度[19]，因此实验只测试了本文方案和文献[7]的 2 种方案在加密和解密过程中的时间开销。实验中给定 $\ell=10$ 和 $\rho=20$，主要关注各方案计算时间开销随属性全集中属性数量（即 $|U|$）增加的变化趋势。具体实验结果如图 2 和图 3 所示。

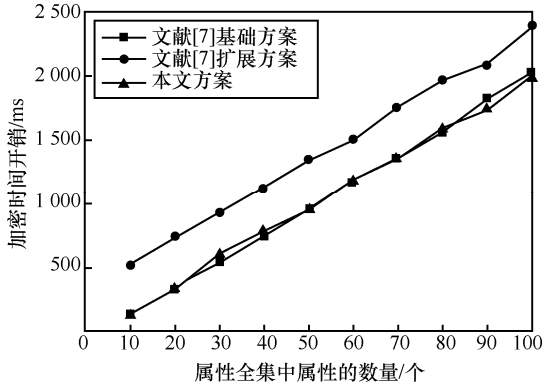


图 2　不同方案加密时间开销对比

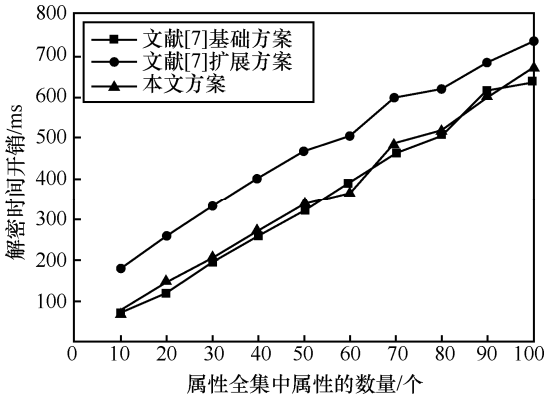


图 3　不同方案解密时间开销对比

从图 2 可以看出，随着属性全集中属性数量的增加，各方案加密时间开销基本呈线性增长。本文方案实验曲线位于文献[7]扩展方案实验曲线的下方，而与文献[7]基础方案实验曲线在多个节点处几乎重叠，这表明本文方案的加密时间开销小于文献[7]扩展方案的加密时间开销，而与文献[7]基础方案的加密时间开销大体相当。

从图 3 可以看出，随着属性全集中属性数量的

增加，各方案解密时间开销也基本呈线性增长。其中本文方案实验曲线明显低于文献[7]扩展方案实验曲线，整体略高于文献[7]基础方案实验曲线。例如当$|U|=40$时，文献[7]扩展方案、本文方案和文献[7]基础方案的解密时间开销分别为401.45 ms、275.1 ms 和 255.4 ms。此时，本文方案的解密时间开销比文献[7]扩展方案减小了126.35 ms，但只比文献[7]基础方案增加了 19.7 ms。这表明，本文方案的解密效率明显优于文献[7]扩展方案的解密效率，而稍弱于文献[7]基础方案的解密效率。图 2 和图 3 的实验结果与表 2 的理论分析结果是一致的。

综上所述，本文方案同时具备抗密钥委托滥用性和可追踪性，并且可追踪性证明基于严格的标准模型。与同功能特点的文献[7]扩展方案相比，本文方案具有明显的性能优势。

7 结束语

属性基加密的推广和应用面临着密钥委托滥用和恶意用户追踪 2 个重要的安全问题，然而现有属性基加密方案对于同时解决这 2 个问题缺少充分的关注。为此本文结合文献[7]基础方案和文献[8]追踪方法，提出了一种新的抗密钥委托滥用的可追踪属性基加密方案。该方案与同样支持抗密钥委托滥用和可追踪的文献[7]扩展方案相比，在性能上更加高效，并且可追踪性证明基于更严格的标准模型。目前，本文方案仅支持由与门构成的访问结构，未来将进一步改进本文方案，使其能够支持任意的单调访问结构，从而表达更加灵活的访问策略。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 89-98.

[3] 齐芳, 李艳梅, 汤哲. 可撤销和可追踪的密钥策略属性基加密方案[J]. 通信学报, 2018, 39(11): 63-69.
QI F, LI Y M, TANG Z. Revocable and traceable key-policy attribute-based encryption scheme[J]. Journal on Communications, 2018, 39(11): 63-69.

[4] 李学俊, 张丹, 李晖. 可高效撤销的属性基加密方案[J]. 通信学报, 2019, 40(6): 32-39.
LI X J, ZHANG D, LI H. Efficient revocable attribute-based encryption scheme[J]. Journal on Communications, 2019, 40(6): 32-39.

[5] 于金霞, 何旭, 闫玺玺. 机构可验证的密文策略属性基加密方案[J]. 西安电子科技大学学报, 2019, 46(4): 49-57.
YU J X, HE X, YAN X X. Ciphertext-policy attribute-based encryption scheme with verifiability on authority[J]. Journal of Xidian University, 2019, 46(4): 49-57.

[6] JIANG Y, SUSILO W, MU Y, et al. Ciphertext-policy attribute-based encryption with key-delegation abuse resistance[C]//The 21st Australasian Conference on Information Security and Privacy. Berlin: Springer, 2016: 477-494.

[7] JIANG Y, SUSILO W, MU Y, et al. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing[J]. Future Generation Computer Systems, 2018, 78(2): 720-729.

[8] LIU Z, CAO Z, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[9] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]//The 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2013: 463-474.

[10] BONEH D, BOYEN X. Short signatures without random oracles[C]//The International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 56-73.

[11] NING J, CAO Z, DONG X, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability[C]//The 19th European Symposium on Research in Computer Security. Berlin: Springer, 2014: 55-72.

[12] YU S, REN K, LOU W, et al. Defending against key abuse attacks in KP-ABE enabled broadcast systems[C]//The 5th International Conference on Security and Privacy in Communication Networks. Berlin: Springer, 2009: 311-329.

[13] 张星, 文子龙, 沈晴霓, 等. 可追责并解决密钥托管问题的属性基加密方案[J]. 计算机研究与发展, 2015, 52(10): 2293-2303.
ZHANG X, WEN Z L, SHEN Q N, et al. Accountable attribute-based encryption scheme without key escrow [J]. Journal of Computer Research and Development, 2015, 52(10): 2293-2303.

[14] NING J, DONG X, CAO Z, et al. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud[C]//The 20th European Symposium on Research in Computer Security. Berlin: Springer, 2015: 270-289.

[15] YU G, MA X, CAO Z, et al. Accountable multi-authority ciphertext-policy attribute-based encryption without key escrow and key abuse[C]//The 9th International Symposium on Cyberspace Safety and Security. Berlin: Springer, 2017: 337-351.

[16] ZHANG Y, LI J, ZHENG D, et al. Towards privacy protection and malicious behavior traceability in smart health[J]. Personal and Ubiquitous Computing, 2017, 21(5): 815-830.

[17] LAI J, TANG Q. Making any attribute-based encryption accountable, efficiently[C]//The 23rd European Symposium on Research in Computer Security. Berlin: Springer, 2018: 527-547.

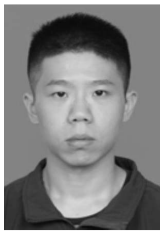
[18] LI Q, ZHU H, YING Z, et al. Traceable ciphertext-policy attribute-based encryption with verifiable outsourced decryption in eHealth cloud[J]. Wireless Communications and Mobile Computing, 2018(1): 1701675.

[19] QIAO H, REN J, WANG Z, et al. Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing[J]. Future Generation Computer Systems, 2018, 88(1): 107-116.

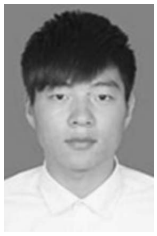
[20] CARO A D, IOVINO V. jPBC: Java pairing based cryptography[C]//The 16th IEEE Symposium on Computers and Communications. Piscataway: IEEE Press, 2011: 850-855.

[作者简介]

闫玺玺（1985– ），女，河南灵宝人，博士，河南理工大学副教授，主要研究方向为网络与信息安全、数字版权管理、数字内容安全。



何旭（1993– ），男，河北冀州人，河南理工大学硕士生，主要研究方向为网络与信息安全、密码学。



刘涛（1994– ），男，河南商丘人，河南理工大学硕士生，主要研究方向为网络与信息安全、软件定义网络。

叶青（1981– ），女，辽宁营口人，博士，河南理工大学讲师，主要研究方向为信息安全、格密码学、数字签名。

于金霞（1974– ），女，河南博爱人，博士，河南理工大学教授，主要研究方向为网络与信息安全、人工智能、智能信息处理。

汤永利（1972– ），男，河南孟州人，博士，河南理工大学教授，主要研究方向为网络与信息安全、密码学。