Computer Science and Application 计算机科学与应用, 2018, 8(3), 296-304
Published Online March 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.83034

Hans汉斯

Attribute-Based Encryption Scheme with Hidden Access Policy

Xinglan Zhang, Jiannan Li

Department of Information, Beijing University of Technology, Beijing
Email: 154335680@qq.com

Received: Mar. 10th, 2018; accepted: Mar. 22nd, 2018; published: Mar. 28th, 2018

Abstract

In the traditional Ciphertext-Policy attributed-based encryption scheme, although the access policy can better implement attribute encryption, it will also bring the problem of data privacy leakage, and the large computation in the Ciphertext decryption stage. This paper proposes an outsourced encryption scheme to hide access policy, which generalizes the values of attributes. In the encryption process, the valid Ciphertext and the invalid Ciphertext are indistinguishable by hiding some subset values. In addition, outsourcing part of the Ciphertext decryption reduces the computing burden of the data receiver and greatly improves the efficiency of decryption. The analysis shows that the new scheme enhances the flexibility of the system while hiding the access policy, and it is proved to be safe under the assumption of DDH, which has certain theoretical and applied value.

Keywords

Attribute-Based Encryption, Access Policy, Hidden, Outsourced

隐藏访问策略的属性加密方案研究

张兴兰，李建楠

北京工业大学，北京
Email: 154335680@qq.com

收稿日期：2018年3月10日；录用日期：2018年3月22日；发布日期：2018年3月28日

摘　要

传统基于密文策略的属性加密方案中，访问策略虽然能较好的实现属性加密，但也会带来数据隐私泄露问题，并且密文解密阶段的计算开销大。文章提出一种隐藏访问策略的外包加密方案，对属性的取值进

文章引用: 张兴兰, 李建楠. 隐藏访问策略的属性加密方案研究[J]. 计算机科学与应用, 2018, 8(3): 296-304.
DOI: 10.12677/csa.2018.83034

行泛化处理，在加密过程中通过隐藏部分子集值使得有效密文和无效密文不可区分。此外，将密文解密的部分计算外包，减轻了数据接收方的计算负担，极大地提高了解密效率。分析表明，新方案在隐藏访问策略的同时增强了系统的灵活性，同时在DDH假设下证明是安全的，具有一定的理论和应用价值。

关键词

属性加密，访问策略，隐藏，外包

1. 引言

在传统的公钥加密体系中，通信采用“一对一”模型，使用特定公钥加密的数据，必须使用相应的私钥解密，例如基于身份的加密(IBE) [1]方案。实际上，许多加密系统采用的都是“一对多”的通信模型，例如共享数据库中的文档被多个用户访问，有线电视节目被多个订阅者观看等。属性加密(简称 ABE)采用一系列属性来描述用户身份，可以引入访问控制策略把用户私钥和密文同属性相关联，具有“一对多”良好特性，能够灵活地进行访问控制，可以实现对密文细粒度的访问控制。这个想法最早由 Sahai 和 Waters 作为模糊 IBE 方案[2]的应用引入，其中密钥和密文与属性集合关联，当且仅当密文和密钥的属性集相交的属性个数至少达到固定的阈值时才能解密。

近年来随着对属性加密方案研究[3] [4]的不断深入细化，又分为密钥策略的属性解密(简称 KP-ABE) [5]和密文策略的属性加密(简称 CP-ABE) [6] [7] [8]。其中，Bethencourt 等人提出第一个 CP-ABE 方案[7]，该方案要求访问控制策略在密文中公开，用于接收方完成属性对比和解密。考虑到某些隐私性,有些时候访问控制策略可能包含隐私信息，加密者需要将加密策略进行隐藏，但如果访问策略被隐藏，解密者将无法完成相应的解密工作。之后，Nishide 等人[9]提出了一种隐藏访问控制策略的基于属性加密方法，由于采用了较多的双线性对运算和指数运算，对算法效率的影响较大。Kapadia 等人[10]的方案要求一个在线的半可信服务器参与，且必须知道每个用户的属性值，发送方只具有发布密文的功能，当接收方检索密文时，半可信服务器重加密该密文，这一方案对第三方依赖太大，不能防止用户串谋。Shiet 等人[11]提出了一个基于大数范围查询的谓词加密方案，数据发送方在指定访问策略中的数字范围实现 CP-ABE，采用的安全概念较弱，且要求属性个数少，该方案在属性数量上成指数型。Boneh 和 Waters [12]提出基于隐藏向量的谓词加密方案，使用子集谓词相反的语义实现策略隐藏，但是需要处理两个大素数阶的双线性对，在系统建立时指定访问策略中的属性以及每个属性的可能取值。而在我们的方案中，即使公共参数系统建立后，也可以在密文策略中增加属性。Lai 等人[13]利用子群判定假设在合数阶群中提出了一个新的可以隐藏访问结构的加密方案，并证明是完全安全的。但是为了达到一定的安全级别，合数群的阶会取得比较大。Katz 等人[14]提出一种支持内积的谓词加密方案，该方案实现访问策略的隐藏且通用性强，可以同时满足 KP-ABE 和 CP-ABE 方案。但是，该方案需要采用一种特殊的具有三个大素数的双线组，访问控制结构固定且在强假设下证明安全性。

本文在文献[6]所构造的高效属性加密方案基础上，通过扩展每个属性的可能取值，在加密的过程中隐藏部分属性值的子集值，要求所有接收方都不知道发送方采用了何种访问策略加密数据。对比已有的

方案，本文在实现策略隐藏的同时支持策略灵活、安全变更；在解密过程中加入了外包转换计算，提高解密效率。

2. 预备知识

2.1. 双线性映射

关于双线性映射的研究是当前密码学的一个重要课题，自提出后被应用到各种加密、签名等方案中，一些密码学上的难题得到了很好的解决。

设 p 是一个素数，G_1, G_2 是两个阶为 p 的乘法循环群，g 为 G_1 的生成元，e 是一个双线性映射：$e: G_1 \times G_1 \to G_2$。双线性映射 e 满足如下 3 个性质：

1) 双线性性质。对于任意的 $a,b \in Z_p, h \in G_1$，满足 $e\left(g^a, h^b\right) = e(g,h)^{ab}$。

2) 非退化性。$e(g,g) \neq 1$。

3) 可计算性。对于任意的 $g, h \in G_1$,存在有效算法可在多项式时间内计算出 $e(g,h)$ 的值。

注意：$e(*,*)$ 运算是一个对称操作，即 $e\left(g^a, h^b\right) = e(g,h)^{ab} = e\left(g^b, h^a\right)$；另外有 $e(g_1 \cdot g_2, h) = e(g_1, h) \cdot e(g_2, h)$，其中 $g_1, g_2, h \in G_1$。

定义 1 (计算 Diffie-Hellman (CDH)问题)随机选择 $a,b \in Z_p$，给定三元组 $\left(g, g^a, g^b\right)$，计算 g^{ab}。

定义 2 (判定 Diffie-Hellman (DDH)问题)随机选择 $a,b,c \in Z_p$ 且未知，g 为循环群 G_1 的一个生成元，给定一个元组 $\left(g, g^a, g^b, g^c\right)$，判定 $g^c = g^{ab}$ 是否成立。

2.2. 访问控制结构

在 CP-ABE 方案中，数据发送方制定访问策略，若接收方的属性密钥满足发送方制定的访问策略，则可以解密密文。例如，访问结构 $T = (A \text{ AND } B) \text{OR} (C \text{ AND } D)$，接收方满足最小属性集合 $\{A,B\}$ 或 $\{C,D\}$，则可以解密访问控制结构 T 加密后的数据。

本文对访问控制结构做如下定义：属性外部之间用与门，属性内部之间用或门。假设属性系统中的属性总个数为 n，相应的索引为 $\{\Lambda_1, \Lambda_2, \cdots, \Lambda_n\}$，每个属性拥有多个取值，数据接收方的属性列表定义为 $L = [L_1, L_2, \cdots, L_n]$，$W = [W_1, W_2, \cdots, W_n]$ 表示访问控制策略，使用通配符*表示访问策略中无关属性的取值，W 中的每个 W_i 是 Λ_i 所有可能取值的子集。当 $1 \le i \le n, L_i = W_i$ 或 $W_i = *$ 时，属性列表 L 满足访问控制策略 W，否则 L 就不满足访问控制结构 W。

具体来说，例如 Λ_i 有 n_i 个可能取值，用集合 $S_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$ 表示，接收方的属性列表 $L = \{L_1, L_2, \cdots, L_i, \cdots, L_n\}$，$L_i \in S_i$，加密使用的访问控制策略 $W = [W_1, W_2, \cdots, W_i, \cdots, W_n], W_i \in S_i$，这就意味着：当 $\left(\Lambda_1 = v_{1,1} \vee \Lambda_1 = v_{1,4}\right) \wedge \left(\Lambda_2 = v_{2,3}\right) \wedge \cdots \wedge \left(\Lambda_i = v_{i,2} \vee \Lambda_i = v_{i,5} \vee \Lambda_i = v_{n_i}\right) \wedge \cdots \wedge \left(\Lambda_n = v_{i,1} \vee v_{i,5}\right)$ 加密者为 Λ_i 指定属性值，即为 Λ_i 指定了 $W_i = S_i$，当且仅当 $1 \le i \le n, L_i \in W_i$ 时，满足该属性列表 L 的接收方才可以解密。访问结构中 W_i 隐藏每个属性 Λ_i 的部分取值，即访问控制结构中与门结构里所有属性的部分取值。

2.3. 安全模型

本方案的安全模型可以通过攻击者和挑战者之间的游戏过程来描述，若最终攻击者给出正确的猜测，则攻击者胜利，反之，挑战者胜利。游戏过程如下：

Init：攻击者向挑战者发送访问控制策略 W_0 和 W_1。

Setup：挑战者运行初始化过程 Setup，将公钥 PK 发送给攻击者。

Phase 1：攻击者发送属性列表 L 可以进行多次相关密钥查询，要求 L 同时满足或者不满足访问控制策略 W_0 和 W_1。挑战者运行密钥生成算法 KeyGen，将密钥 SK_L 返还给攻击者。

Challenge：攻击者向挑战者提交两个数据 M_0 和 M_1。如果攻击者的属性列表 L 在 Phase1 满足访问策略 W_0 和 W_1，则得到密钥 SK_L 并要求 $M_0 = M_1$。挑战者随机抛币得到 $b \in \{0,1\}$，随机选择一个 M_b，用 W_b 进行加密，将密文信息返回给攻击者。

Phase2：重复 Phase1。

Guess：攻击者输出对 b 的猜测 b'。

攻击者获得游戏胜利的优势为：$\Pr[b' = b] - 1/2$。

定义 3 在多项式时间内所有的攻击者，赢得上述游戏的优势都是可以忽略不计的，则称该方案是安全的。

3. 具体方案

在文献[6]的基础上，本方案的参与方包括：可信授权方、数据发送方和数据接收方，本文系统模型如图 1 所示：

其中，可信授权方负责监管和颁发属性公钥；数据发送方使用访问策略加密数据并将密文发送给服务器；数据接收方使用自己的属性私钥解密满足规定访问策略下密文。此外，本文在解密阶段将部分密文解密任务外包，减轻接收方的解密计算负担，提高解密效率。方案过程包括：初始化过程 Setup、加密过程 Encrypt、密钥提取过程 KeyGen、外包转换计算 OutSCC 和解密过程 Decrypt 五个算法。以下是详细描述：

1) 初始化过程 Setup (1^k)。

输入：公共参数 K。

过程：可信授权方产生一个元组 $G = [p, G_1, G_2, G_T, g_1 \in G_1, g_2 \in G_2, e]$，其中，$G_1, G_2$ 为 p 阶的乘法循环群，其中 g_1, g_2 分别是 G_1, G_2 的生成元，e 是双线性映射，结构如下：$G_1 \times G_2 \to G_T$。系统随机产生 $\alpha, \beta \in Z_p^*$，对于每个属性 $1 \le i \le n$，可信授权方产生随机值 $\{a_{i,t} \in Z_p^*, 1 \le t \le n_i\}$，并计算 $\{A_{i,t} = g_1^{a_{i,t}}, 1 \le t \le n_i\}$。可信授权方继续计算 $Y = e(g_1, g_2)^{\alpha}$ 和 $h = g_1^{\beta}$。

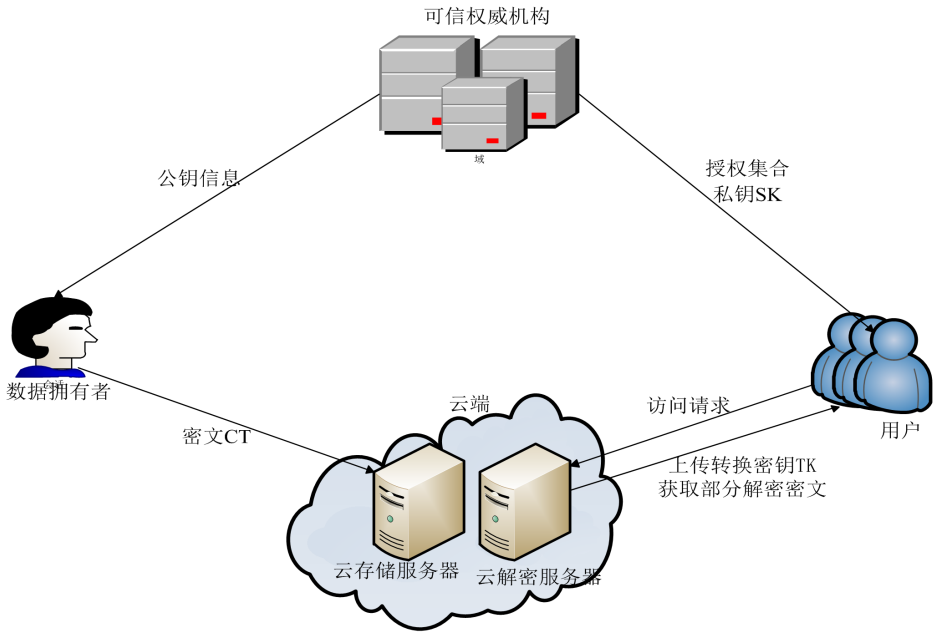

Figure 1. System model diagram
图 1. 系统模型图

输出：系统公钥 $PK=\left\{Y,h,p,G_1,G_2,G_T,g_1,g_2,e,\left\{A_{i,t},1\le t\le n_i\right\}_{1\le i\le n}\right\}$，主密钥 $MK=\left\{\alpha,\beta,\left\{a_{i,t},1\le t\le n_i\right\}_{1\le i\le n}\right\}$。

2) 加密过程 Encrypt (PK,M,W)。

输入：系统公钥 PK，待加密的消息 $M\in G_T$ 以及密文策略 $W=\left[W_1,W_2,\cdots,W_n\right]$。

过程：加密方用随机值 $s\in Z_p$，设定 $\tilde{C}=MY^s$ 以及 $C_0=h^s$，用随机值 $s_i\in Z_p\left(s=\sum_{i=1}^{n}s_i\right)$，设定 $C_{i,1}=g_1^{s_i}$，并按如下方式计算 $\left\{C_{i,t,1}\right\}_{1\le t\le n_i}$：

$$C_{i,t,1}=\begin{cases}A_{i,t}^{s_i},v_{i,t}\in W_i\\ random,\text{否则}\end{cases}$$

输出：密文 $CT=\left\{\tilde{C},C_0,\left\{C_{i,1},\left\{C_{i,t,1}\right\}_{1\le t\le n_i}\right\}_{1\le i\le n}\right\}$。

3) 密钥提取过程 KeyGen (MK,L)。

输入：主密钥 MK，数据接收方属性列表 $L=\left[L_1,L_2,\cdots,L_n\right]=\left[v_{1,t_1},v_{2,t_2},\cdots,v_{n,t_n}\right]$。

过程：可信授权方产生随机值 $r,r_i\in Z_p,1\le i\le n$，并且计算 $D_0=g_2^{\frac{\alpha+r}{\beta}}$，$D_1=g_2^r$，当 $L_i=v_{i,t_i}$ 时，计算 $D_{i,1}=g_2^{r_i},1\le i\le n$。数据接收方生成转换密钥 $TK=\left\{r,\left\{D_{i,1}\right\}_{1\le i\le n}\right\}$。

输出：私钥 $SK_L=\left\{D_0,D_1,\left\{D_{i,1}\right\}_{1\le i\le n}\right\}$，转换密钥 $TK=\left\{r,\left\{D_{i,1}\right\}_{1\le i\le n}\right\}$。

4) 外包转换计算 OutSCC (PK,L,TK,CT)。

输入：转换密钥 TK，数据接收方属性列表 $L=\left[L_1,L_2,\cdots,L_n\right]=\left[v_{1,t_1},v_{2,t_2},\cdots,v_{n,t_n}\right]$，系统公钥 PK，密文 $CT=\left\{\tilde{C},C_0,\left\{C_{i,1},\left\{C_{i,t,1}\right\}_{1\le t\le n_i}\right\}_{1\le i\le n}\right\}$。

过程：接收方将自己的属性列表中的 L_i 以及转换密钥 TK 发送给外包服务器，服务器首先判断这个接收方属性字符串是否满足 $L_i=v_{i,t_i}$，若不满足，则终止服务；若满足，则针对数据接收方所选的密文开始为其提供计算服务，即对密文进行转换计算。从 PK 中提取 $\left\{A_{i,t},1\le t\le n_i\right\}_{1\le i\le n}$，计算 $D_{i,2}=g_2^r\cdot D_{i,1}^{\log_{g1}^{A_{i,t}}}$，然后进行转换密文，首先计算 $CD=\prod_{i=1}^{n}e\left(C_{i,1},D_{i,2}\right)=e\left(g_1,g_2\right)^{rs+\sum_{i=1}^{n}a_{i,t}\cdot s_i\cdot r_i},1\le t\le n_i,1\le i\le n$，然后进行转换计算 $C'=\tilde{C}\cdot CD$。

输出：转换密文 $CT'=\left\{C',C_0,CD,\left\{C_{i,1},\left\{C_{i,t,1}\right\}_{1\le t\le n_i}\right\}_{1\le i\le n}\right\}$。

5) 解密过程 Decrypt (CT',SK_L)。

输入：转换密文 $CT'=\left\{C',C_0,CD,\left\{C_{i,1},\left\{C_{i,t,1}\right\}_{1\le t\le n_i}\right\}_{1\le i\le n}\right\}$，私钥 $SK_L=\left\{D_0,D_1,\left\{D_{i,1}\right\}_{1\le i\le n}\right\}$。

过程：当 $L_i=v_{i,t_i},1\le i\le n$ 时，用户计算 $E=\prod_{i=1}^{n}e\left(C_{i,t,1},D_{i,1}\right)=e\left(g_1,g_2\right)^{\sum_{i=1}^{n}a_{i,t}\cdot s_i\cdot r_i}$，用于验证等式 $\frac{CD}{\prod_{i=1}^{n}e\left(C_{i,1},D_1\right)}=E$ 是否成立。若不成立，说明外包服务器计算过程有误；否则，运行解密算法，得到 $M=\frac{C'}{e\left(C_0,D_0\right)\cdot E}$。

输出：信息 M。

4. 安全性分析及证明

4.1. 正确性

当数据接收方的属性列表满 L 足访问控制策略 W 时，接收方利用获得的用户私钥 SK_L，可以成功运行解密算法，从而获得数据的明文信息。下面从两个方面验证计算的正确性：

1) 验证外包计算。

$$\frac{CD}{\prod_{i=1}^{n} e\left(C_{i,1}, D_1\right)} = \frac{\prod_{i=1}^{n} e\left(C_{i,1}, D_{i,2}\right)}{\prod_{i=1}^{n} e\left(g_1^{s_i}, g_2^{r}\right)} = \frac{e\left(g_1, g_2\right)^{rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}{e\left(g_1, g_2\right)^{\sum_{i=1}^{n} s_i \cdot r}}$$

$$= \frac{e\left(g_1, g_2\right)^{rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}{e\left(g_1, g_2\right)^{rs}} = e\left(g_1, g_2\right)^{\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i} = E$$

2) 验证解密计算。

$$\frac{C'}{e\left(C_0, D_0\right)\prod_{i=1}^{n} e\left(C_{i,t,1}, D_{i,1}\right)} = \frac{\tilde{C} \cdot CD}{e\left(h^s, g_2^{\frac{\alpha+r}{\beta}}\right)\prod_{i=1}^{n} e\left(A_{i,t}^{s_i}, g_2^{r_i}\right)}$$

$$= \frac{\tilde{C} \cdot \prod_{i=1}^{n} e\left(C_{i,1}, D_{i,2}\right)}{e\left(g_1^{\beta s}, g_2^{\frac{\alpha+r}{\beta}}\right)\prod_{i=1}^{n} e\left(g_1^{a_{i,t} \cdot s}, g_2^{r_i}\right)} = \frac{MY^s \cdot \prod_{i=1}^{n} e\left(C_{i,1}, D_{i,2}\right)}{e\left(g_1^{\beta s}, g_2^{\frac{\alpha+r}{\beta}}\right)\prod_{i=1}^{n} e\left(g_1^{a_{i,t} \cdot s}, g_2^{r_i}\right)}$$

$$= \frac{M \cdot e\left(g_1, g_2\right)^{\alpha s} \cdot e\left(g_1, g_2\right)^{rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}{e\left(g_1, g_2\right)^{\alpha s+rs} \prod_{i=1}^{n} e(g_1^{a_{i,t} \cdot s}, g_2^{r_i})} = \frac{M \cdot e\left(g_1, g_2\right)^{\alpha s+rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}{e\left(g_1, g_2\right)^{\alpha s+rs} e\left(g_1, g_2\right)^{\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}$$

$$= \frac{M \cdot e\left(g_1, g_2\right)^{\alpha s+rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}}{e\left(g_1, g_2\right)^{\alpha s+rs+\sum_{i=1}^{n} a_{i,t} \cdot s_i \cdot r_i}} = M$$

4.2. 安全性

本方案在安全模型下达到了选择明文攻击的不可区分性安全。证明如下：

Proof：假设攻击者 A 在游戏 G_0 和 G 中有不可忽略的优势差异ε，构造一个能以ε的优势打破 DDH 假设的模拟器 B。

首先给出 DDH 假设模型，挑战者随机选取 $a,b,c \in Z_p$，设置一个四元组 $\left(g, g^a, g^b, g^c\right)$。挑战者随机抛币，任选 $u \in (0,1)$，如果 $u=0$，令 $e\left(g_1, g_2\right)^c = e\left(g_1, g_2\right)^{ab}$，选择 G 游戏；否则 $u=1$，令 $e\left(g_1, g_2\right)^c \in G_T$ 为随机值，进行 G_0 游戏。

Init：模拟器 B 与攻击者 A 进行初始化交互。攻击者 A 选择两个要挑战的密文策略 $W_0 = \left[W_{0,1}, W_{0,2}, \cdots, W_{0,n}\right]$，$W_1 = \left[W_{1,1}, W_{1,2}, \cdots, W_{1,n}\right]$ 提交给模拟器 B，B 随机选取 $u \in \{0,1\}$。

Setup：B 任意选取 $x' \in Z_p$，设置 $\alpha = \frac{ab}{c} + x'$，则 $Y = e\left(g_1, g_2\right)^{\frac{ab}{c}+x'}$，对于每个属性 $i\left(1 \le i \le n\right)$，模拟器 B 计算 $A_{i,t}$，计算方法如下：

$$A_{i,t} = \begin{cases} g_1^{a_{i,t}}, v_{i,t} \in W_{i,t_i} \\ g_1^{b \cdot a_{i,t}}, v_{i,t} \notin W_{i,t_i} \end{cases} \quad (1 \le t \le n_i)$$，然后向攻击者 A 发送公钥 PK。

Phase 1：攻击者 A 在一次密钥查询中提交一个属性列表 $L=[L_1,\cdots,L_n]$，我们仅考虑 L 同时不满足 W_0 和 W_1 的情况(如果 L 同时满足 W_0 和 W_1，则挑战的信息 M_0 和 M_1 相同，即游戏 G 和 G_0 就会相同，因此攻击者 A 在这两个游戏中的优势将没有区别)，SK_L 中的参数如下：$D_0=g_2^{\frac{\frac{ab}{c}+x'+r}{\beta}}$，$D_1=g_2^r$,当 $L_i\notin W_i$ 时，$D_{i,1}=g_2^{r_i}$，密钥 SK_L 返回给攻击者 A，转换密钥 $TK=\left\{r,\left\{D_{i,1}\right\}_{1\le i\le n}\right\}$ 发送给外包服务器。

Challenge：攻击者 A 选择两个挑战信息 M_0 和 M_1。模拟器 B 对 $\left\{M_u\right\}_{u\in\{0,1\}}$ 进行加密，令 $s=c$，则密文为：$\tilde{C}=M_uY^s=M_ue(g_1,g_2)^{\left(\frac{ab}{c}+x'\right)c}=M_ue(g_1,g_2)^{ab}\cdot e(g_1,g_2)^{x'c}=M_ue(g_1,g_2)^c\cdot e(g_1,g_2)^{x'c}$，$C_0=h^s=h^c$。当 $u=0$ 时，$e(g_1,g_2)^c=e(g_1,g_2)^{ab}$；当 $u=1$ 时，$e(g_1,g_2)^c$ 为随机值，因此，$\tilde{C}$ 为 G_T 群中的随机值。模拟器 B 选取随机值 $s_i\in Z_p^*\left(s=\sum_{i=1}^n s_i\right)$，计算 $\left\{C_{i,t,1}\right\}_{1\le t\le n_i}=A_{i,t}^{s_i}=g_1^{b\cdot a_{i,t}\cdot s_i}$ 和 $C_{i,1}=g_1^{s_i}$，把密文 $CT=\left\{\tilde{C},C_0,\left\{C_{i,1},\left\{C_{i,t,1}\right\}_{1\le t\le n_i}\right\}_{1\le i\le n}\right\}$ 发送给外包服务器，外包服务器通过转换密钥 TK 将密文 CT 进行转换，首先计算 $CD=\prod_{i=1}^n e\left(C_{i,1},D_{i,2}\right)=e\left(g_1,g_2\right)^{rs+\sum_{i=1}^n b\cdot a_{i,t}\cdot s_i\cdot r_i}=e\left(g_1,g_2\right)^{rc+\sum_{i=1}^n b\cdot a_{i,t}\cdot s_i\cdot r_i}$，$1\le t\le n_i$，$1\le i\le n$，然后将转换后的密文 $C'=\tilde{C}\cdot CD$ 发送给攻击者 A。

Phase 2：重复 Phase 1 的过程，继续进行私钥问询。

Guess：攻击者 A 输出对 u 的猜测 u'。如果 $u'=u$,挑战者输出 1；否则，输出 0。通过我们之前的假设，攻击者 A 在游戏 G 中猜测正确 u 的可能性相比在游戏 G_0 中正确猜出 u 有 ε 的优势。当 $e(g_1,g_2)^c=e(g_1,g_2)^{ab}$ 时，攻击者 A 猜测游戏为 G；当 $e(g_1,g_2)^c$ 是随机值时，攻击者 A 猜测游戏为 G_0。因此，模拟器 B 在 DDH 游戏中有 ε 的优势，即最后攻破了 DDH 问题。

5. 性能分析

将本文与文献[9]和文献[13]对比分析，本文不仅在加密过程中实现访问策略的隐藏，并且支持访问控制结构中属性的安全、灵活添加，同时，系统效率优于其他方案。

1) 隐藏访问控制策略。本方案对每个属性的取值进行泛化，增加其可能取值，通过隐藏每个属性包含部分可能取值的子集，使用通配符表示那些与访问策略不相关的属性，如此便达到了隐藏部分策略属性的目的。保证了包括合法接收方在内的所有接收方都不能猜测出加密时采用的访问控制策略，而接收方需要从可信授权方获取自己的属性私钥，若与此属性私钥相关联的属性列表不满足发送方指定的访问策略时，则此接收方就不是合法的，不能完成解密。

举例来说，若访问控制策略为 $W=[W_1,W_2,\cdots,W_i,\cdots,W_n]$，其中 $W_1=\left(\Lambda_1=\nu_{1,1}\text{ or }\Lambda_1=\nu_{1,3}\right)$，$W_2=\left(\Lambda_2=\nu_{2,2}\right)$，$\cdots$，$W_i=\left(\Lambda_i=\nu_{i,5}\text{ or }\Lambda_i=\nu_{i,n_i}\right)$，$\cdots$，$W_n=\left(\Lambda_n=\nu_{n,1}\text{ or }\Lambda_n=\nu_{n,2}\text{ or }\Lambda_n=\nu_{n,3}\right)$ 则访问策略 $W=\left(\nu_{1,1}\text{ or }\nu_{1,3}\right)\text{and }\nu_{2,2}\text{ and}\cdots\text{and}\left(\nu_{i,5}\text{ or }\nu_{i,n_i}\right)\cdots\text{and}\left(\nu_{n,1}\text{ or }\nu_{n,2}\text{ or }\nu_{n,3}\right)$，当接收方的属性列表 L 满足访问结构意味着：当且仅当 $L_i\in W_i,1\le i\le n$ 时，如果 $L_i=\left(\nu_{1,1}\text{ and }\nu_{2,2}\cdots\text{and }\nu_{i,n_i}\cdots\text{and }\nu_{n,2}\right)$，则满足该访问策略；若 $L_i=\left(\nu_{1,1}\text{ and}\cdots\text{and }\nu_{i,n_i}\text{ and}\cdots\text{and }\nu_{n,2}\right)$，则不满足访问控制结构。因此，任何满足访问控制结构的合法接收方，他的属性列表不需要满足访问控制元素 W_i 的所有子属性值 $\nu_{i,t}$。

2) 支持访问结构中属性的动态添加。对比文献[6]和[12]中要求密文中的访问策略在初始化之前就指定好属性个数和每个属性的取值且不能随意更改访问策略中相关属性的信息；文献[7]中，首先执行初始化算法，然后在密文中的访问策略中添加新属性。由于公共参数没有变，运行初始化算法 Setup 之后，接收方已经可以获得用户私钥，这时再在访问策略中添加属性，对于某些用户来说仍然具备解密能力。例如，访问策略 $W=[W_1,W_2,W_3]$，用户属性列表为 $L=[L_1,L_2,L_3]=[1,1,0]$，与用户属性列表相关联的密钥

是 SK_L，若改变访问策略使其变为 $W=[W_1,W_2,W_3,W_4]$，这时要求合法的解密者拥有的密钥 SK_L 必须具有 W_4 相关属性成分，但是对于 $W_4=0$ 来说，由于 L 仍然满足 W，因此某些用户仍然具备解密能力。

本方案要求即使是在接收方获得私钥之后，访问控制策略中添加属性，接收方必须再次从可信授权方获得包括新属性在内的新密钥才能解密密文，原用户私钥作废。方案设计添加属性时，相应的在公钥成分中也添加了该属性值的相关成分，并在加密过程中采用了分割的随机数 $s_i \in Z_p^*\left(s=\sum_{i=1}^{n} s_i\right)$ 的方法，密文 CT 中 $C_{i,1}$ 和 $C_{i,t,1}$ 的计算都依赖于 s_i。同时，s 也作为指数在 $\tilde{C}$ 和 C_0 中参与运算，即访问策略中的每个属性都在加密过程中生成随机值并参与运算，这就要求接收方解密时，必须具备满足策略属性序列中每个必须属性值。因此，原私钥不能用于更新后的访问策略解密，必须重新从可信授权方获得新私钥。

3) 提高系统效率。整个系统运行过程中，影响效率的主要因素体现在存储开销和系统计算时间上。为了方便下文的分析描述，令 $|g|,|g_T|$ 和 $|p|$ 分别代表 G,G_T,Z_p^* 中元素的大小，n 表示系统中的属性个数，N 代表 n 个属性的所有可能取值个数之和，Γ_e 表示执行一次双线性运算所需要的时间，Γ_Δ 表示执行一次指数运算花费的时间，$|A_c|$ 表示访问控制策略中所包含的属性个数。

方案存储开销的大小分析主要通过对比分析各个方案在加解密过程中得到的主密钥、系统公钥、密文和私钥的大小。表 1 给出不同方案中系统的存储开销：

由表 1 可知，相比于其它文献，本文所提出的方案中存储空间明显缩小了，相应的通信量也降低了，其中，密文的存储空间缩小将近一半，而密钥所占空间的大小降幅显著。

本方案涉及多种运算，但系统的执行时间主要花费在指数运算和双线性运算上，其中双线性配对运算的代价远远大于指数运算，因此，本文的效率分析主要针对这两种运算。表 2 给出了不同方案在计算时间上的对比：

通过表 2 的数据可知，本文加密阶段的花费计算时间与文献[13]持平，比文献[9]明显降低；与其他文献相比，本文在接收方解密密文之前，将部分解密计算任务交由外包服务器执行，把部分私钥(转换密钥) TK 发送给外包计算服务器，外包服务器判断属性列表 L_i 并对密文 $\tilde{C}$ 进行转换计算，将原有的 $\tilde{C}$ 转换成 C' (更易于解密)发送给接收方，然后接收方可以通过验证等式 $\frac{CD}{\prod_{i=1}^{n} e(C_{i,1},D_1)}=E$ 是否成立来确定

Table 1. Storage cost comparison
表 1. 存储开销对比

方案	主密钥	公钥	密文	私钥
文献[9]	$(2N+1)\|p\|$	$(2N+1)\|g\|+\|g_T\|$	$(2n+1)\|g\|+\|g_T\|$	$(3n+1)\|g\|$
文献[13]	$(2N+1)\|p\|$	$(2N+1)\|g\|+\|g_T\|$	$(n+1)\|g\|+\|g_T\|$	$(2n+1)\|g\|+\|g_T\|$
本方案	$(N+2)\|p\|$	$(N+1)\|g\|+\|g_T\|$	$(n+1)\|g\|+\|g_T\|$	$(n+2)\|g\|$

Table 2. Computation of time contrast
表 2. 计算时间对比

方案	加密阶段	解密阶段
文献[9]	$E=(2\|A_c\|+3)\cdot\Gamma_\Delta$	$E=(3n+1)\cdot\Gamma_e$
文献[13]	$E=(\|A_c\|+2)\cdot\Gamma_\Delta$	$E=(n+1)\cdot\Gamma_e$
本方案	$E=(\|A_c\|+2)\cdot\Gamma_\Delta$	$E=\Gamma_e$

外包服务器计算的正确性，并用自己的部分私钥 SK_L 和属性列表 L_i 解密该转换密文，最终获得明文 M。过程在保证安全性的前提下，由于本方案将解密阶段部分计算任务外包给云服务器计算，因此，数据拥有者的计算消耗明显降低，解密效率优于现有的属性加密方案，进一步提升了系统整体效率。

6. 结语

本文通过对属性取值做泛化处理，构造可以隐藏访问策略的加密方案，并支持访问策略中属性的灵活添加，在 DDH 假设下可抵抗选择明文攻击，达到不可区分性安全。此外，将解密阶段的大部分操作转移给外包服务器执行，降低用户私钥对可信授权方的依赖，解密效率优于现有方案，随着属性和访问数据量的增加，本方案的优势越明显。

资助信息

经典可证明安全性理论在量子密码协议分析中的应用研究(10007016201201)。

参考文献

[1] Shamir, A. (1984) Identity-Based Cryptosystems and Signature Schemes. *Proceedings of CRYPTO'84 on Advances in Cryptology*, **21**, 47-53.

[2] Sahai, A. and Waters, B. (2005) Fuzzy Identity Based Encryption. *Advances in Cryptology-EUROCRYPT* 2005, **3494**, 457-473. https://doi.org/10.1007/11426639_27

[3] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1-12.

[4] 苏金树, 曹丹, 王小峰. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315.

[5] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of the ACM Conference on Computer and Communications Security*, October 30-November 3 2006, Alexandria, Virginia, 89-98. https://doi.org/10.1145/1180405.1180418

[6] Cheung, L. and Newport, C. (2007) Provably Secure Ciphertext Policy ABE. *CCS*'07: *Proceedings of the ACM Conference on Computer and Communications Security*, Alexandria, Virginia, 456-465. https://doi.org/10.1145/1315245.1315302

[7] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. *Proceedings of the IEEE Symposium on Security and Privacy*, 20-23 May 2007, Washington, DC, 321-334. https://doi.org/10.1109/SP.2007.11

[8] Emura, K., Miyaji, A. and Nomura, A. (2009) A Ciphertext-Policy Attribute Based Encryption Scheme with Constant Ciphertext Length. *ISPEC* 2009: *Information Security Practice and Experience*, **5451**, 13-23. https://doi.org/10.1007/978-3-642-00843-6_2

[9] Nishide, T., Yoneyama, K. and Ohta, K. (2008) Attribute-Based Eneryption with Partially Hidden Encryption-Specified Access Structure. *Proceedings of the Applied Cryptograph & Network Security*, **5037**, 111-129.

[10] Kapadi, A., Tsang, P. and Smith, W. (2007) Attribute-Based Publishing with Hidden Credentials and Hidden Policies. *Network & Distributed System Security Symposium*, 179-192.

[11] Shi, E., Bethncourt, J., Chan, S. and Perrig, A. (2007) Multi-Dimensional Range Query over Encrypted Data. *Proceedings of IEEE Symposium on Security and Privacy*, 20-23 May 2007, Berkeley, CA, 350-364. https://doi.org/10.1109/SP.2007.29

[12] Bonehd, D. and Waters, B. (2007) Conjunctive, Subset, and Range Queries on Encrypted Data. In: Vadhan, S.P., Ed., *TCC* 2007, Vol. 4392, 535-554.

[13] Lai, J., Deng, R.H. and Li, Y. (011) B-Ktlly Secure Cipertext-Policy Hiding CP-ABE. *ISPEC* 2011, **6672**, 24-39.

[14] Katz, J., Sahai, A. and Waters, B. (2008) Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. *Advances in Cryptology-EUROCRYPT* 2008, **4965**, 146-162. https://doi.org/10.1007/978-3-540-78967-3_9