doi:10.11959/j.issn.1000-436x.2015211

云存储环境下的密文安全共享机制

姚文斌，韩司，李小勇
（北京邮电大学 智能通信软件与多媒体北京市重点实验室，北京 100876）

摘 要：云存储环境为海量数据的存储和共享提供方便的同时也带了安全隐患。为保证数据安全，用户将自己的隐私数据加密后存储在开放的云存储环境中，如何建立云存储环境下的密文访问控制机制是亟需解决的问题。基于 CP-ABE 算法的密文安全共享机制主要解决云存储环境下的密文访问控制问题。共享机制使用 2 个半可信中心进行密钥的生成和分发，降低访问控制对第三方的依赖性。同时，在用户密钥中加入标识信息，抵抗来自非法用户的串谋攻击。此外，提出用户密钥撤销算法，增强动态安全性。安全分析和实验结果表明，安全共享机制在保障云存储环境下数据安全共享的同时，适用于实际的云存储环境。
关键词：云存储；属性加密；访问控制；数据共享
中图分类号：TP393 **文献标识码**：A

Security sharing scheme for encrypted data in cloud storage

YAO Wen-bin, HAN Si, LI Xiao-yong
（Beijing Key Lab of Intelligent Telecommunication Software and Multimedia,
Beijing University of Posts and Telecommunications, Beijing 100876, China）

Abstract: With the convenient of storing and sharing data in cloud storage environment, the concerns about data security arised as well. To achieve data security on untrusted servers, user usually stored the encrypted data on the cloud storage environment. How to build a cipertext-based access control scheme became a pot issue. For the access control problems of ciphertext in cloud storage environment, a CP-ABE based data sharing scheme was proposed. Novel key generation and distribution strategies were proposed to reduce the reliance on a trusted third party. Personal information was added in decryption key to resistant conclusion attacks at the same time. Moreover, key revocation scheme was proposed to provide the data backward secrecy. The security and implement analysis proves that proposed scheme is suit for the real application environment.
Key words: cloud storage; attribute-based encryption; access control; data sharing

1 引言

云存储是一种新兴的网络应用模式，它将大量计算资源和存储资源链接在一起，形成巨大的共享虚拟存储池为用户提供服务[1]。用户可将自己的数据远程存储在云存储中心，按需访问。然而，由于云存储环境的动态复杂性和开放性等特征，用户完全依赖不可信的云存储提供商进行数据的存储和管理。不可避免地引起了用户对数据安全性与隐私性方面的担忧。如何进行开放式云存储环境下的数据共享安全是云存储应用亟需解决的问题。

在不可信云存储环境中，用户将共享数据加密后存储，并通过对解密密钥的获取来实现密文访问控制。使用传统的对称、非对称密钥进行数据的保护虽然可以数据隐私性，但是密钥协商和管理过程复杂，增加了密钥动态更新和用户细粒度访问控制的难度。针对开放式的云存储环境，Sahai[2]提出了属性基(ABE)的加密机制解决了细粒度的访问控制

收稿日期：2014-10-09；**修回日期**：2015-03-09
基金项目：国家自然科学基金资助项目（61370069）；国家高技术研究发展计划（“863”计划）基金资助项目（2012AA012600）
Foundation Items: The National Natural Science Foundation of China (61370069); The National High Technology Research and Development Program of China (863 Program) (2012AA012600)

和大规模的用户动态扩展问题。ABE 在非对称密码中引入访问结构，它并非使用特定的单一密钥加密数据，而是将密文、用户私钥与用户属性关联，通过制定访问控制策略限定用户的访问权限。ABE 只需根据属性即访问结构加解密数据，无需关注用户规模和身份信息，具有高效性、灵活性的特点。属性加密机制根据属性和访问策略所属位置的不同主要分为 2 类：密钥属性策略(KP-ABE)[3]和密文属性策略(CP-ABE)[4,5]。

KP-ABE 使用树结构描述访问策略，并将访问策略嵌入在用户私钥中，密文则关联多个用户属性，只有当密文中的属性满足用户私钥中的访问策略时，用户才能解密密文。同KP-ABE相反，CP-ABE使用一个属性集合来表示一个用户，并依据其属性集合生成用户私钥。而密文则与访问控制策略相关联，仅当用户私钥中的属性满足密文中的访问控制策略时，用户才能解密密文。KP-ABE 由用户规定对接收数据的要求，适用于查询类的应用。CP-ABE 将数据针对满足一定条件的群体用户进行加密，并且加密时不要求逐一地确定群体用户。相对于一对一的传统加密方式，CP-ABE 更适用于云存储环境下的密文访问控制。

在 CP-ABE 的密钥分发过程中，由用户属性集合生成的相关联私钥是解密共享数据的关键，而其私钥的生成与分发需要依赖可信的密钥托管中心，无法满足开放式云存储中信任分散的安全需求。同时，CP-ABE 中的访问结构是由属性集合与逻辑运算组成，在共享数据解密过程中，多个非授权用户可以联合自己在访问结构中的合法属性的相关联私钥，以联合形成满足访问结构的解密私钥，进而解密密文以实施非法访问。此外，由于用户私钥与用户属性集合关联，不同用户的属性集合间存在共有属性，云存储环境下用户的离开将导致多个用户私钥的更新，增加了密钥撤销的复杂性。

针对以上安全问题，本文提出了一种基于 CP-ABE 的数据安全共享机制。安全共享机制将用户的私钥分为对称密钥和非对称密钥两部分，分别交由授权机构和云存储中心管理，降低访问控制对可信第三方的依赖性。在用户私钥中加入私人标识，抵抗用户串谋攻击。最后，提出属性撤销算法，在保证后向安全性的基础上，提高性能。

2 相关工作

访问控制是进行用户数据隐私保护的重要手段。基于属性的访问控制解决了细粒度访问和大规模用户动态扩展的问题，为开放式云存储环境提供了理想的访问控制方案[3]。文献[4,5]提出的 CP-ABE 机制利用访问用户的不同属性制定访问策略，灵活地满足云存储环境中需要数据属主自定义访问策略的要求。为解决 CP-ABE 方案中的密钥托管和动态扩展问题，主要进行了如下研究。

Dong[6]和 Yang[7]分别提出了多授权机构的 CP-ABE 方案以解决密钥托管问题。方案将单个授权机构的信任和工作量分散到系统的多个授权机构上。但是，在多授权机构 CP-ABE 方案中，每个授权机构使用相同的主密钥为用户生成私钥，具有足够多属性的用户将能够重构主密钥，多个非授权用户串谋[8]则可恢复出系统主密钥，进而威胁系统安全性。

Jung[9]提出一种云存储环境下的多授权机构 CP-ABE 访问控制方案，该方案采用用户全局唯一标识来防止用户串谋。Wan[10]提出了多层次的云存储资源访问控制机制，将授权机构分为不同等级进行用户私钥的生成，解决了用户串谋问题。在 Jung 和 Yang 的方案中，当新增加授权机构时，初始化计算复杂并且系统公钥会随之改变，用户需要向所有的授权机构重新申请密钥，开销随用户数目呈线性增长。并且在 2 个方案中，为提高数据加解密性能，首先选用对称密钥对数据加密，然后使用 CP-ABE 方案控制对称密钥的获取以实现数据的访问控制功能。文献[9,10]所提出的属性撤销算法无法进行对称密钥的更新，已获取对称密钥的用户即使在属性失效后仍可解密共享数据，不能保证方案的后向安全性。

文献[11]结合 CP-ABE 和两方安全计算的思想解决了密钥托管问题，用户私钥由不可信的机构和云存储中心使用两方安全计算完成，在解决用户串谋和密钥托管问题的同时，降低了计算复杂性。

Yang 等[12]提出了云存储环境下的 CP-ABE 属性撤销算法，当发生属性撤销时，更新用户私钥和与该属性相关的加密数据，保障了数据的前向和后向安全性。

3　数据共享模型与安全假设

3.1　数据共享模型

在云存储的数据共享环境中，主要包括 4 类用户：数据属主、数据共享者、云存储中心和授权机构。数据共享系统模型如图 1 所示。

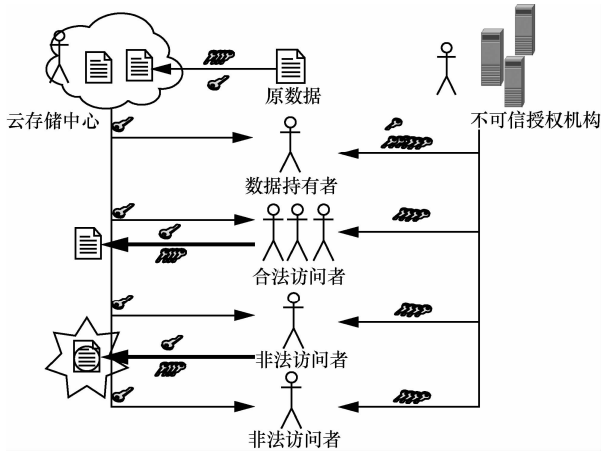


图 1　数据共享系统模型

云存储中心：提供云存储环境，永久在线管理用户的存储数据。它与授权机构一起管理系统属性集合和用户密钥。云存储中心正常执行共享机制分配的任务，但是出于获利的考虑，可能泄露用户存储的数据。

授权机构：永久在线与云存储中心一起管理系统属性集合和用户密钥。同样，出于获利考虑可能泄露用户密钥。

数据属主为共享数据的来源方，将分享的数据按照访问结构进行加密后存储在云环境中。

数据分享者为共享数据的获取方，从云存储中心获取加密的共享数据后使用自己的密钥解密数据。数据共享者为云存储的所有使用者，可能混杂非法用户。

3.2　安全假设

云存储的开放式环境中，基于 CP-ABE 的密文安全共享机制主要面临以下 3 个安全问题。

密钥托管：用户依赖不可靠的云存储中心和授权机构完成共享数据的访问控制，致使数据的机密性和隐私性遭受威胁。

串谋攻击[8,13]：数据属主根据属性集合和访问控制结构加密数据，非授权用户可能通过联合属性解密数据。

后向安全性：离开共享群组的用户，仍可使用自己的原有属性密钥解密共享数据，对后续数据进行非法访问。

4　数据安全共享机制

4.1　预备知识

1) 拉格朗日插值法

设某个次数为 n 的多项式，如给定多项式的 $n+1$ 个不同点 x_i, y_i,则可以唯一确定一个 x 对应的多项式 $L(x)=\sum_{j=0}^{k} y_j l_j(x)$,其中，每个 $l_j(x)$ 为拉格朗日基本多项式，其表达式为

$$l_j(x)=\prod_{\substack{0\leqslant m\leqslant k\\ m\neq j}}\frac{x-x_m}{x_j-x_m}=\frac{x-x_0}{x_j-x_0}\cdots$$

$$\frac{(x-x_{j-1})(x-x_{j+1})}{(x_j-x_0)(x_j-x_{j+1})}\cdots\frac{x-x_k}{x_j-x_k},0\leqslant j\leqslant k$$

2) 双线性

设 G 和 G_1 是阶为素数 p 的群，g 为 G 的生成元。存在这样一个映射 $e:G\times G\to G_1$ 具有以下性质。

双线性：如果存在 $\forall a,b\in Z$，有

$e(g^a,g^b)=e(g^b,g^a)=e(g,g)^{ab}$

$e(u_1\times u_2,v)=e(u_1,v)e(u_2,v)$

非退化性：$\forall a,b\in G$，使 $e(a,b)\neq 1$，其中，1 为 G_1 的单位元。

可计算性：有一个多项式时间计算 $e(g^a,g^b)$。

3) CP-ABE 算法

CP-ABE 数据共享机制主要包括 3 个部分。

属性组：设 $A=\{A_1,A_2,\cdots,A_n\}$ 为所有属性的集合，每个用户的属性集合 S 是 A 的一个非空子集。

访问结构：访问结构是由一系列属性和门限逻辑运算符（如 AND,OR）组成的判断条件 T。满足 T 的属性集合称为授权集，不满足判断条件 T 的属性集合称为非授权集。

访问树：访问树 T_R 用于描述访问结构，T_R 的每个叶子节点 x 代表一个属性 λ_x，叶子节点的门限值为 1；每个非叶子节点 x 是由其子节点和逻辑运算符组成的门限关系函数，子节点从 $1-n$ 编码且非叶子节点的门限值 k_x 小于其子节点总数 num_x，即 $0<k_x<num_x$。

当访问结构为{((学院：计算机)OR(专业：通信工程))AND((年级≤大四)AND(成绩<60))}时，其访问树结构如图 2 所示。

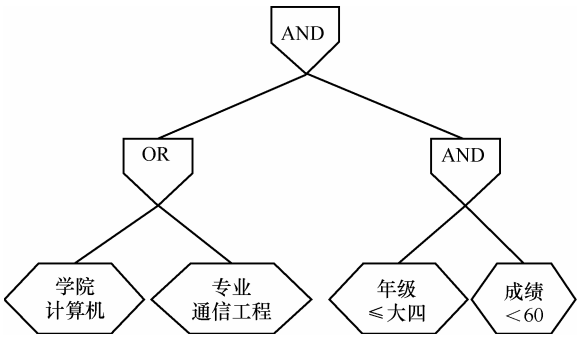


图2 访问树实例

4.2 数据安全共享机制

本文提出的数据安全共享机制首先由授权机构和云存储中心结合用户唯一标识共同产生用户密钥；其次用户混合使用授权机构产生的非对称密钥和云服务商产生的对称密钥完成数据的加解密；最后，当用户注销时完成相关密钥和密文的更新，保护共享数据的后向安全性。

1) 初始化算法

授权机构产生共享系统的安全参数，首先随机生成元为 g，阶为 p 的双线性群 G 和双线性映射 $e:G\times G\to G_1$，随机选取散列函数 H 和 $\alpha,\beta\in \mathrm{Z}_p$ 生成主密钥 $\left(g^{\alpha},\beta\right)$ 和公钥 $\left(G,g,g^{\beta},H,e(g,g)^{\alpha}\right)$。

云存储中心产生对称密钥 $\varepsilon\in \mathrm{Z}_p$ 和全体属性集 $\Omega=\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$。

2) 密钥生成算法

当有用户注册进入云存储系统时，云存储中心为其生成唯一标识 g^{u_i}、对称密钥 ε 和属性集 $S=\{\lambda_1,\cdots,\lambda_k,\cdots,\lambda_m\}$。

用户将自己的属性集 $S=\{\lambda_1,\cdots,\lambda_k,\cdots,\lambda_m\}$ 和标识 $g^{\varepsilon u_i}$ 发送给授权机构申请属性关联私钥。

授权机构为注册用户属性集中的每个属性 λ_k 随机选取参数，并使用式(1)计算私钥 $SK_{u_i}^{G}$ 后发送给注册用户。

通过以上步骤，注册用户所获取的私钥为

$$SK_{u_i}=(D=g^{\frac{\alpha+u_i\varepsilon}{\beta}},\varepsilon;\forall\lambda_j\in S:D_k=g^{u_i}H(\lambda_j)^{r_j},D_k^{'}=g^{r_j})$$

在密钥生成算法中，用户在授权机构获取私钥和公钥中加入了由云存储中心为其分配的唯一标识 $g^{\varepsilon u_i}$，解决了 CP-ABE 方案中的密钥托管和串谋攻击问题。

$$SK_{u_i}^{G}=(D=g^{\frac{\alpha}{\beta}}g^{\frac{u_i\varepsilon}{\beta}};\forall\lambda_j\in S:D_k=g^{u_i\varepsilon}H(\lambda_j)^{r_j},D_k^{'}=g^{r_j})$$
$$=(D=g^{\frac{\alpha+u_i\varepsilon}{\beta}};\forall\lambda_j\in S:D_k=g^{u_i\varepsilon}H(\lambda_j)^{r_j},D_k^{'}=g^{r_j}) \quad (1)$$

3) 共享数据加密算法

数据属主在上传共享数据前，构造访问树并使用访问树、CP-ABE 公钥和对称密钥完成共享数据的加密。

①访问树构造算法

数据属主设置访问结构，以访问结构中的属性作为叶子节点，门限逻辑运算符作为中间节点构建访问树 T_R。

从根节点开始，数据属主为访问树 T_R 中的每个非叶子节点 x 定义一个 (k_x-1) 次多项式 f_x 并随机选取 $s\in Z_p$ 作为根节点 R 的节点值，设置 $f_R(0)=s$；为每一个非叶子节点 x，设置 $f_x(0)=f_{\mathrm{parent}(x)}(index(x))$，其中 $index(x)$ 为节点的编码值。

②数据加密算法

如果访问树中的属性集合为 $\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$，数据属主使用式(2)对共享数据 M 加密。数据属主将加密后的数据 CT 存放在云存储中心。

$$CT=Encrypt(M,\Gamma,PK,s)$$
$$=(\Gamma,Me(g,g)^{\alpha\varepsilon s},g^{\beta s};$$
$$\forall\lambda_k\in Leaf:C_k=g^{f_k(0)},C_k^{'}=H(\lambda_k)^{f_k(0)}) \quad (2)$$

4) 数据解密算法

所有的云存储用户均可向云存储中心查询下载加密后的共享数据，并使用自己的密钥解密数据。数据的解密操作分为 2 个部分：使用嵌套方式计算访问树根节点 R 的节点值，然后使用根的节点值解密数据。

对访问树的每个叶子节点 x，请求用户使用 CP-ABE 私钥 SK_{u_i} 执行解密操作。

步骤 1 如果 $\lambda_x\in S$，则使用式(3)计算 T_x，否则设置 $T_x=0$。

$$T_x=\frac{e(D_x,C_x)}{e(D_x^{'},C_x^{'})}=\frac{e(g^{u_i\varepsilon}H(\lambda_x)^{r_x},g^{f_x(0)})}{e(g^{r_x},H(\lambda_x)^{f_x(0)})}$$
$$=\frac{e(g^{u_i\varepsilon},g^{f_x(0)})e(H(\lambda_x)^{r_x},g^{f_x(0)})}{e(g,H(\lambda_x))^{r_x f_x(0)}}$$
$$=e(g,g)^{u_i\varepsilon f_x(0)} \quad (3)$$

步骤 2 对访问树的每个非叶子节点 y 自底向上依次执行解密操作。

如果 y 的所有子节点集合 N 中满足条件 $|(z\in N)\Lambda(T_z\neq 0)|\geqslant k_y$，则使用式(4)计算，否则设置 $T_y=0$。

$$T_y=\prod_{z\in N}T_z^{\prod_{j\in N,j\neq N}\frac{index(j)}{index(z)-index(j)}}$$
$$=\prod_{z\in N}e(g,g)^{u_i\varepsilon f_{\text{parent}(z)}(index(z))\prod_{j\in N,j\neq N}\frac{index(j)}{index(z)-index(j)}}$$
$$=e(g,g)^{u_i\varepsilon\sum_{z\in N}(f_y(index(z))\prod_{j\in N,j\neq N}\frac{index(j)}{index(z)-index(j)})}$$
$$=e(g,g)^{u_i\varepsilon f_y(0)} \tag{4}$$

嵌套执行式(4)，当用户私钥满足访问树，最后可获取根的节点值为 $T_R=e(g,g)^{u_i\varepsilon s}$。否则，计算得到根的节点值为 0。

步骤 3　根据根的节点值和用户私钥，使用式(5)可恢复共享数据。

$$M=\frac{Me(g,g)^{\alpha\varepsilon s}}{\left[\frac{e((g^{\beta})^s,g^{\frac{\alpha+u_i\varepsilon}{\beta}})}{V_R}\right]^{\varepsilon}}=\frac{Me(g,g)^{\alpha\varepsilon s}}{\left[\frac{e((g^{\beta})^s,g^{\frac{\alpha+u_i\varepsilon}{\beta}})}{\mathrm{e(g,g)}^{u_i\varepsilon s}}\right]^{\varepsilon}} \tag{5}$$

5) 用户撤销算法

在实际的云存储环境中，用户的动态更新频繁。为保护共享数据不被注销后的用户获取，共享机制提出用户撤销算法，保护共享数据的后向安全性。

当有用户注销时，云存储中心重新生成对称密钥 ε' 并使用式(6)对所存储的共享数据进行重加密。

$$[Me(g,g)^{\alpha\varepsilon s}]^{\frac{\varepsilon'}{\varepsilon}}=Me(g,g)^{\alpha\varepsilon' s} \tag{6}$$

当有用户请求下载共享数据时，云存储中心将最新的对称密钥 ε' 分配给未注销的请求用户，用户更新自己的私钥为

$$SK_{u_i}=(D=g^{\frac{\alpha+u_i\varepsilon}{\beta}},\varepsilon';\forall\lambda_j\in S:D_k=g^{u_i}H(\lambda_j)^{r_j},D_k'=g^{r_j})$$

获取新对称密钥的用户可使用数据解密算法还原共享数据。

5　安全性及性能分析

5.1　安全性分析

本节通过对 4 个定理的证明验证数据共享机制不仅可以低抗选择明文攻击、串谋攻击，而且解决了 CP-ABE 方案中的密钥托管问题，保障了数据的后向安全性。

定义 1　DBDH 问题（判定双线性问题[14]）。设 G 和 G_1 是阶为素数 p 的群，g 为 G 的生成元。存在这样一个映射 $e:G\times G\to G_1$，判定 DBDH 问题是：已知 g,g^a,g^b,g^c,Z，判定是否有 $Z=e(g,g)^{abc}$ 成立，若等式成立，则 $\{g,g^a,g^b,g^c,Z\}$ 为一个 DBDH 元组，其中，$a,b,c\in Z_p,Z\in G_1$。

若有一个概率多项式算法解决上述问题的概率为 ε，那么称该算法解决 DBDH 问题的优势为 ε。

定义 2　CP-ABE 选择明文攻击游戏[15,16]。

在 CP-ABE 选择明文攻击游戏中，敌手和挑战者进行如下交互。

建立阶段：挑战者对加密方案进行系统建立，输出公私钥对，并将公钥交给敌手。

第一阶段：敌手可以向挑战者查询属性集对应的用户私钥。

质询阶段：敌手选择 2 个长度相同的明文 M_0,M_1 和访问树 Γ，第一阶段已查询的属性集都不满足该访问树。敌手将明文和访问树发送给挑战者。挑战者随机生成 $b\in\{0,1\}$，对 M_b 进行加密并将密文 C 并发送给敌手。

第二阶段：敌手可以继续向挑战者进行一些属性集对应私钥的查询，但是属性集仍不满足访问树。

猜测阶段：挑战者必须回答 $b'=0$ 或 $b'=1$，作为对密文 C 的猜测。

如若 $b'=b$，则敌手获胜，其优势定义为 $\Pr[b'=n]-\frac{1}{2}$。

定理 1　如果任意概率多项式时间的敌手在 DBDH 游戏中的优势是可忽略的，则数据安全共享机制是选择明文安全的。

证明　首先，假设存在一个多项式敌手 A 可以攻破安全共享机制，那么可以构造一个模拟器 B（同时为 DBDH 的攻击者）能以 ε 的优势攻破 DBDH 问题。

建立阶段：DBDH 模拟器 B 从授权机构获取安全机制算法的公钥 $\{G,g,g^{\beta},h,e(g,g)^{\alpha}\}$，生成随机数 $a,b,c\in Z_p$，并计算 x 为：$ab+x=\alpha$。

第一阶段：攻击者 A 向模拟器 B 提交查询的属性集 S 以及用户标识 $g^{u_i\varepsilon}$。B 为 S 中的每个属性选取随机数 r_j，并计算得到的用户私钥为

$$\{g^{\frac{ab+x+u\varepsilon}{b}},\forall\lambda_j\in S:g^{u\varepsilon}H(\lambda_j)^{r_j},g^{r_j}\}$$

模拟器 B 将计算的用户私钥返回给攻击者 A，这样模拟器 B 完美模拟了一个授权机构。

质询阶段：攻击者 A 选择访问结构 Γ 和 2 个长度相同的明文 M_0、M_1，第一阶段已查询的属性集不满足访问树。模拟器 B 将攻击者 A 选择的明文以及访

问树根节点值c发送给授权机构进行数据加密。授权中心随机生成$b=0$或1，对明文进行加密，得到$M_b e(g,g)^{\alpha s}$和$M_{\bar{b}} e(g,g)^{zs}$，其中$z\in Z_p$为随机选取。

第二阶段：重复第一阶段。

猜测阶段：攻击者A输出一个猜测值b'，模拟器B根据攻击者A结果做出相应的猜测，如果猜测正确，则可通过式(7)计算判定。

$$M_{b'} e(g,g)^{\alpha c} = M_{b'} e(g,g)^{(ab+x)c} = M_{b'} e(g,g)^{abc} e(g^x, g^c) \quad (7)$$

这样，模拟器B以$\frac{1}{2}$的概率分析出密文信息。如果猜测错误，由于z为随机数，模拟器B无法对密文进行判断。如上所述，敌手可以$\frac{1}{2}$概率攻破数据安全共享机制。

因此，在DBDH安全的条件下，数据安全共享机制是可以抵抗选择明文攻击的。

定理 2 数据安全共享机制可以抵抗来自非法用户、云存储中心和授权机构的非法访问，进而解决密钥托管问题。

证明 对于非法用户，可利用的消息包括用户私钥中的D、$g^{u_i\varepsilon}$以及密文$g^{\beta s}$。使用式(8)进行双线性映射。根据映射结果可知，要解密数据，必须获取根的节点值s。当非法用户的属性无法满足访问结构时，不可解密s还原共享数据。

$$e(D, g^{\beta s}) = e(g^{\frac{\alpha + u_i \varepsilon}{\beta}}, g^{\beta s}) = e(g,g)^{\alpha s} e(g,g)^{u_i \varepsilon s} \quad (8)$$

云存储中心维护的对称密钥仅用来加密数据，而与访问树根的节点值s的获取无关，云存储中心无法解密共享数据。

授权机构可以伪造合法用户的密钥解密s，根据式(8)，授权机构可还原$e(g,g)^{\alpha s}$，由于加密的共享数据为$Me(g,g)^{\alpha\varepsilon s}$，要解密数据授权机构必须获取$\varepsilon$，故其无法解密共享数据。

综上所述，无论是非法用户、云存储中心还是授权机构都无法进行数据的非法解密，定理2得证。

定理 3 安全共享机制可抵抗用户串谋攻击。

证明 不同的用户可以联合自己的属性私钥来解密共享数据，假设有2个非法用户u_i、u_j结合自己的属性利用式(3)进行叶子节点的解密过程中，获取的叶子节点值集合为

$$\{e(g,g)^{u_i f_x(1)}, \cdots, e(g,g)^{u_i f_x(m)},$$
$$e(g,g)^{u_j f_x(n)}, \cdots, e(g,g)^{u_j f_x(k_x)}\}$$

由于叶子节点的分别由u_i和u_j标识，因此无法使用式(4)进行非叶子节点值的还原。

综上所述，非授权的用户无法进行属性串谋，所以数据安全共享机制能够抵抗串谋攻击。

定理 4 数据安全共享机制可保护共享数据的后向安全性。

证明 当发生用户撤销时，云存储中心更新对称密钥的更新并对共享数据进行重加密，保证撤销用户无法进行原有共享数据的访问，进而保证共享数据的后向安全性。

5.2 仿真及性能分析

本章通过仿真实验综合对比了安全共享机制与Jung[9]提出的云访问控制机制在密钥生成、数据加密、数据解密以及用户撤销4个方面的性能。实验环境为IntelCore2 Duo 2.93 GHz，2 GB内存，操作系统为Ubuntu 12.04。

1) 密钥生成

密钥生成算法中，需要为用户的每个属性生成随机数，算法复杂性为$O(N)$,N为属性个数。图3为安全共享机制与Jung所提机制的用户私钥生成时间与属性数量间的变化关系。从图中可看出，2个机制的密钥生成时间与属性个数呈线性增长，由于Jung使用多授权机构完成密钥的生成，其密钥生成时间要稍高数据安全共享机制。

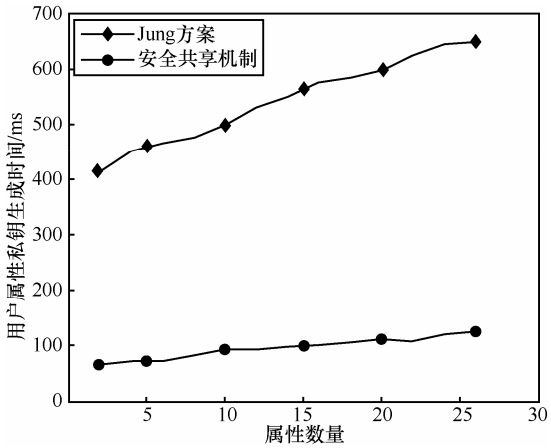
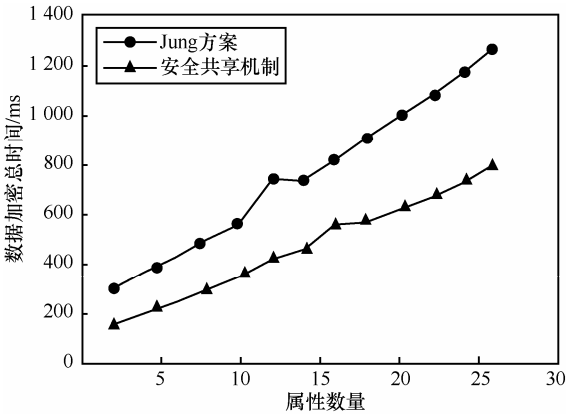


图3 密钥生成时间与属性数量间的变化关系

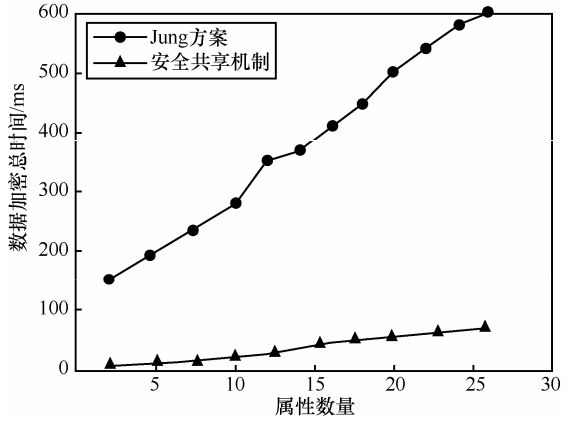
2) 数据加密

在数据安全共享机制的数据加密算法中，需要生成访问树后加密数据。生成访问树过程中需要对每个节点生成多项式，并为每个节点分配k_x个随机数，其算法复杂性与节点个数和k_x相关。图4(a)为数据安全共享机制和Jung机制中，访问树生成时间与数据加密时间的总时长与属性数量间的变化关系，

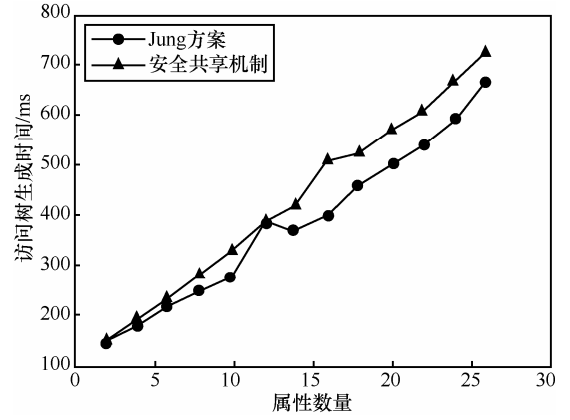
图 4(b)和图 4(c)分别为访问树生成时间和数据加密时间与属性数量间的变化关系。如图 4(b)所示，数据安全共享机制中绝大部分时间消耗在访问树生成过程中。相对于数据本身，安全共享机制的数据加密时间更多地取决于属性个数。在 Jung 的方案中，CP-ABE 用来加密对称密钥后再使用对称密钥来加密共享数据，其数据加密时间要高于安全共享机制。



(a) 数据加密总时耗与属性数量的变化关系



(b) 数据加密时间变化

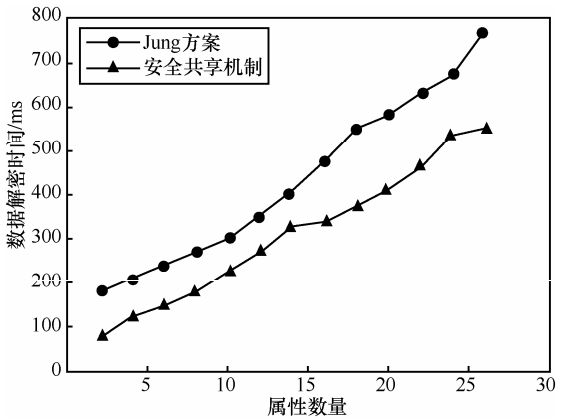


(c)访问树生成时间变化

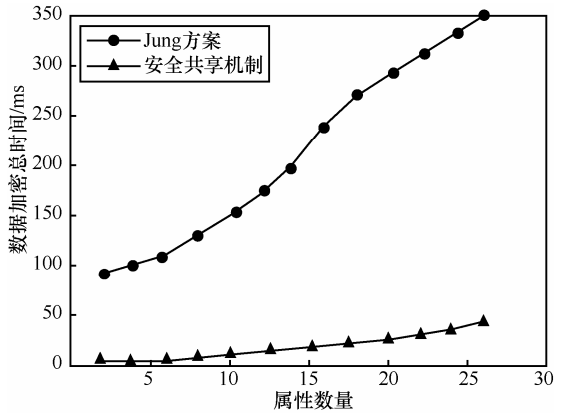
图 4　数据加密与属性数量间的变化关系

3) 数据解密

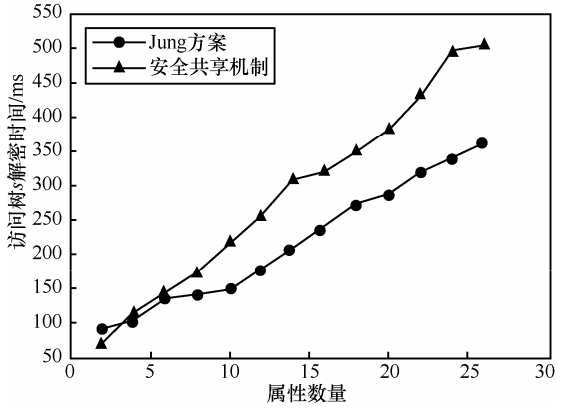
同数据加密算法相同，数据解密算法首先需要解密访问树的根节点参数 s，然后解密共享数据。解密参数 s 的算法复杂度与访问树节点和门限值相关。图 5(a)为共享机制算法中，数据解密时间同属性数量间的变化关系。图 5(b)和图 5(c)分别为访问树根节点值和数据加密的时间与属性数量间的变化关系。从图 5(c)可看出，数据解密的时间主要消耗在



(a) 数据解密总时耗与属性数量间的变化关系



(b) 数据解密时间变化



(c) 访问树根节点 s 解密时间

图 5　数据解密时间与属性数量间的变化关系

解密 s 的过程中，Jung 方案解密对称密钥后仍需使用对称密钥解密数据，其总的数据解密时间要长于数据安全共享机制。

4) 用户撤销

在安全共享机制的用户撤销算法中，需要完成密文的重加密和用户密钥的更新，其算法复杂性与存储数据数量和用户个数相关。并且重加密操作省去了 Jung 方案中的密文解密的过程。

共享机制使用云存储中心和一个授权机构完成密钥的生成，相对于多授权机的控制机制，在提高生成效率的同时解决了密钥托管问题。结合 CP-ABE 和对称密钥完成了数据的加解密，并通过对称参数的更新保护了数据的后向安全性，降低了用户撤销时的密钥更新代价。

6 结束语

本文针对云存环境下的加密数据访问控制问题，结合 CP-ABE 提出了一种数据安全共享机制。首先通过联合云存储中心的对称密钥和授权机构的非对称私钥解决了 CP-ABE 算法中的可信第三方依赖问题；其次，在用户的属性私钥中添加用户唯一标识使共享机制可以抵制来自非法用户的串谋攻击；最后，通过对称密钥的更新完成了用户的撤销，保证了共享数据的后向安全性并提高了更新效率。在下一步的工作中，会重点研究云存储对称密钥与用户的关联性，如何缩小单用户所影响的密文、密钥更新范围。

参考文献：

[1] MELL P, GRANCE T. The NIST Definition of Cloud Computing[R]. National Institute of Standards and Technology, Tech Rep, 2009.

[2] GOYAL V, PANDY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS)[C]. ACM, 2006. 89-98.

[3] YU S, WANG C, REN K, *et al*. Achieving secure, scalable, and fine grained data access control in cloud computing[A]. International Conference on Computer Communications (INFOCOM)[C]. 2010. 1-9.

[4] 孙国梓, 董宇, 李云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报, 2011, 32(7): 146-152.
SUN G Z, DONG Y, LI Y. CP-ABE based data access control for cloud storage[J]. Journal on Communications, 2011,32(7):146-152.

[5] ZHOU Z B, HUANG D J, WANG Z J. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2015,64(1):126-138.

[6] DONG X, YU J, LUO Y, *et al*. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing[J]. Computers & Security, 2014, 42: 151-164.

[7] YANG K, JIA X. DAC-MACS: effective data access control for multi-authority cloud storage systems[J]. Security for Cloud Storage Systems, 2014: 59-83.

[8] SUBRAMANIAN J V, PANDIAN A, KUMAR M. Improving security and efficiency in attribute-based data sharing[J]. Networking and Communication Engineering, 2012, 4(2): 76-83.

[9] JUNG T, LI X Y, WAN Z, *et al*. Privacy preserving cloud data access with multi-authorities[A].INFOCOM, 2013 Proceedings IEEE[C]. 2013. 2625-2633.

[10] WAN Z, LIU J, DENG R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. Information Forensics and Security, IEEE Transactions, 2012, 7(2): 743-754.

[11] SUBRAMANIAN J V, PANDIAN A, KUMAR M. Improving security and efficiency in attribute-based data sharing[J]. Networking and Communication Engineering, 2012, 4(2): 76-83.

[12] YANG K, JIA X. DAC-MACS: effective data access control for multi-authority cloud storage systems[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(11): 1790-1801.

[13] WAN Z, LIU J, ZHANG R, *et al*. A collusion-resistant conditional access system for flexible-pay-per-channel pay-TV broadcasting[J]. Multimedia, IEEE Transactions, 2013, 15(6): 1353-1364.

[14] 苏金树, 曹丹, 王小峰,等. 属性基加密机制[J].软件学报, 2011, 22(6):1299-1315.
SU J S, CAO D, WANG X F, *et al*. Auribate-based encryption schemes[J]. Journal of Software, 2011, 22(6):1299-1315.

[15] BELLARE M, DESAI A, POINTCHEVAL D. Relations among notions of security for public-key encryption schemes[J]. Lecture Notes in Computer Science, 1998, 1462:22-45.

[16] DOSHI N, JINWALA D C. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption[J]. Security and Communication Networks, 2014, 7(11): 1988-2002.

作者简介：

姚文斌（1973-），男，黑龙江哈尔滨人，北京邮电大学教授、博士生导师，主要研究方向为灾备技术、信息安全、可信计算等。

韩司（1988-），女，安徽砀山人，北京邮电大学博士生，主要研究方向为信息安全、系统容灾、可信计算。

李小勇（1975-），男，甘肃天水人，北京邮电大学副教授，主要研究方向为分布式计算、可信计算、网络安全等。