DOI: 10.13718/j.cnki.xdzk.2017.06.020

物流大数据中支持属性撤销的访问控制机制①

龚戈淬[1]，　马　蕾[2]

1. 北京电子科技职业学院 示范校建设办公室，北京 100176；
2. 北京电子科技职业学院 电信工程学院，北京 100176

摘要： 物流大数据中包括顾客信息、物流状态等信息，对物流公司、制造商、经销商等企业都有着重要的作用. 然而，物流大数据的泄露会给用户和物流公司带来严重的安全隐患. 为了有效、安全地将这些数据分发给制造商、营销商等企业用户使用，本文基于可信审计中心和密文策略基于属性的加密技术，提出了一种支持属性撤销的细粒度访问控制方案. 安全分析表明，所提方案可以实现细粒度访问控制、隐私保护和安全属性撤销.

关　键　词： 物流大数据；访问控制；细粒度；属性撤销

中图分类号： TN309.2　　**文献标志码：** A　　**文章编号：** 1673-9868(2017)06-0128-07

近年来，作为新一代信息技术重要组成部分的大数据技术得到了飞速的发展，并已广泛应用于电网、交通、物流等领域，促使了“电网大数据”、“交通大数据”、“物流大数据”的产生. 物流大数据是指在货物流通过程中，通过 RFID、物联网、移动互联网等方式收集和汇聚的各种物流信息数据，主要包括以下方面：① 与物流顾客相关的姓名、地址、电话号码等数据；② 与货物相关的大小、质量、类型等数据；③ 与货物流通相关的包装、运输、仓储、配送等数据；④ 与物流企业相关的中心地址、人员配置、路径规划方案、计费方法等数据. 这些数据能够帮助物流企业做出系统层面的决策，实现市场预测、优化资源配置、提高企业竞争力等[1]. 此外，物流大数据对经销商、制造商等企业也具有极大的使用价值. 例如，通过分析特定区域某类产品的物流数据可以获悉该区域内用户的产品需求，这有助于调整生产规划和销售策略. 由于物流大数据中包含顾客信息、物流企业信息等隐私数据，物流企业在将这些数据交付给经销商、制造商等企业用户使用过程中应当确保数据的安全，避免因非授权访问导致的企业隐私泄露、用户隐私泄露等安全问题发生[2-3]. 因此，近年来针对物流大数据的访问控制成为了该领域中的一个研究热点.

针对物流大数据的访问控制，目前主要是通过利用加密机制对数据加密从而保护数据的机密性来实现的[4]. 传统的基于对称加密或非对称加密的访问控制机制无法兼顾安全性和效率的问题，目前较多学者从事基于任务的访问控制机制和基于角色的访问控制机制方面的研究. 文献[5]针对物流系统的分布式结构提出了一种基于角色的访问控制机制，通过改进角色层次关系和增加角色间静态约束来优化系统响应速度，但是当数据量比较大时系统性能会迅速下降，不适用于大数据的场景；文献[6]将任务的概念引入到基于角色访问的控制模型中，提出了基于任务角色访问的控制模型(Task and Role-Based Access Control，TRBAC)，实现了对用户访问控制权限的动态实时控制；文献[7]在 TRBAC 的基础上引入了角色互斥和角色基数原则，提出了扩展的 TRBAC 机制(Enhanced TRBAC，ETRBAC)；此外，文献

① 收稿日期：2016-11-30
基金项目：国家自然科学基金项目(61303251).
作者简介：龚戈淬(1969-)，女，北京人，副教授，硕士，主要从事数据挖掘、网络安全方面的研究.

[8]提出了一种基于回答集程序的三方协商机制，通过引入第三方使得原有的交易双方(数据提供者和数据使用者)之间达成纳什均衡，实现最优交易；文献[9]提出了一种基于动态重加密的权限撤销优化机制，能够在保证数据安全性的前提下降低访问控制权限撤销的计算代价和带宽代价；但是上述机制不能很好地支持动态授权和细粒度访问控制.

基于属性的加密(Attribute-based encryption，ABE)是一种可以对加密数据进行细粒度访问控制的技术. Goyal等人[10]将ABE划分为2类：密钥策略基于属性的加密(Key Policy ABE，KP-ABE)和密文策略基于属性的加密(Ciphertext Policy ABE，CP-ABE). 但是这些机制需要一个可信授权中心来管理系统中所有用户和传送者的属性密钥. 由于授权中心可以解密所有的加密数据，如果授权中心被盗用，系统会崩溃. 此后，Lewko等人[11]提出了多授权中心CP-ABE机制. 然而，他们的研究都没有考虑属性撤销问题.

为克服当前物流大数据中访问控制机制的不足，本文基于可信审计中心和密文策略基于属性的加密技术(Ciphertext Policy-Attribute-based encryption，CP-ABE)提出了一种支持属性撤销的细粒度访问控制机制(Fine Grained Access Control with Attribute Revocation，FAC-AR)，以实现对物流大数据进行高效、安全的数据分发. 安全分析表明，所提机制可以实现细粒度访问控制、抵抗共谋攻击、隐私保护和属性撤销等功能.

1 系统模型和安全需求

1.1 系统模型

如图1所示，本文的FAC-AR模型主要包含数据管理中心、数据存储中心、企业用户、审计中心、属性管理中心和认证中心6个组成部分.

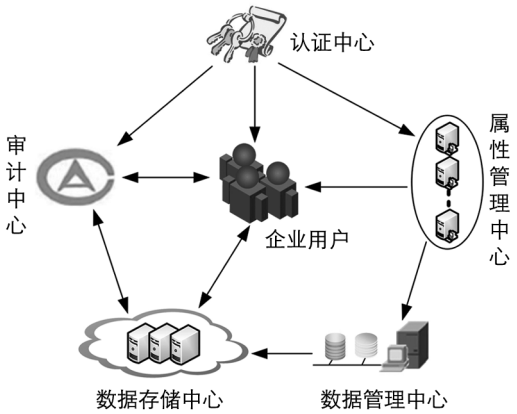

图1 系统模型

数据管理中心(Data Management Center，DMC)负责收集和汇聚物流数据，并对数据进行加密.

数据存储中心(Data Storage Center，DSC)负责存储来自DMC的加密数据，并与企业用户和审计中心通信以向企业用户提供安全的数据访问服务.

企业用户(Enterprise User，EU)是对物流大数据感兴趣的企业(制造商、经销商等)，可以根据预定义的属性请求相应的物流数据.

审计中心(Audit Center，AC)负责对EU进行合法性审查，并帮助合法的EU解密数据.

认证中心(Certificate Authority，CA)是一个可信的认证机构，负责系统初始化、属性管理中心配置和属性撤销.

属性管理中心(Attribute Management Center，AMC)包含多个属性管理服务器(Attribute Management Server，AMS)，每个AMS管理一组属性. AMS分别为DMC和EU生成公共属性密钥(Public Attribute Key，PAK)和EU属性密钥(EU Attribute Key，EAK).

1.2 系统安全需求

在上述模型中，CA，AC，AMC，DMC一般部署在物流企业内部或者由物流企业负责维护，因此我们假设它们都是可信的；DSC可能会部署在物流企业内部或者外包给云服务提供商，因此DSC是不完全可信的；EU是不可信的，可能会通过共谋攻击来非授权访问DSC中的数据.

为了保证物流大数据使用过程中的安全性、可控性，所采取的访问控制机制需要满足以下条件：

1) 细粒度访问控制：访问控制策略应当支持“与”门和“或”门，且只有具有正确属性密钥的EU能解密

该数据；

2）可以抵抗共谋攻击：2 个或多个 EU 无法联合它们的属性密钥来访问那些它们独自无法访问的数据；

3）隐私保护：EU 的身份应当对 DSC 和 AC 保密；

4）安全属性撤销：EU 不能使用已撤销的属性密钥来解密它们不应当访问的数据.

2　理论基础

2.1　双线性映射

设 G，G_T 都是 q 阶（q 为大素数）的乘法循环群，g 为群 G 的生成元. 如果映射 e：$G\times G\rightarrow G_T$ 满足

1）双线性：对于任意的 a，$b\in Z_q$ 和任意的 P_1，$Q_1\in G$，有 $e(P_1^a, Q_1^b)=e(P_1, Q_1)^{ab}\in G_T$；

2）非退化性：映射 e 不是把 $G\times G$ 所有的元都映射到 G_T 的单元上，则 $e(g, g)$ 是 G_T 的生成元；

3）可计算性：对于任意的 P_1，$Q_1\in G$，都存在有效的算法计算 $e(P, Q)$.

则称 e 是一个双线性映射.

2.2　CP-ABE

CP-ABE 属于基于属性的加密的一种，在 CP-ABE 中密文和访问结构（通常为访问树）关联，而密钥则和属性关联，当且仅当访问者的属性集合满足这个访问控制结构时才能解密. CP-ABE 通常包含以下过程：系统初始化、密钥生成、数据加密和解密.

3　FAC-AR 策略

本节主要介绍所提出的 FAC-AR 策略，该策略包含 6 个阶段：系统初始化、EAK 生成、DMC 加密、AC 审计、EU 解密、属性撤销. 该策略中的主要符号如表 1 所示.

表 1　符号对照表

符号	意　义	符号	意　义
x_i	属性 i 的全局标识	GEK	全局 EU 密钥
$Para$	系统参数	LEK	局部 EU 密钥
L_j	第 j 个 AMS(AMS_j)管理的属性集	EGK	EU 生成密钥
$SK_{x_i,j}$	属性 $x_i\in L_j$ 的私有属性密钥	I_m	第 m 个 EU(e_m)具有的属性
$PK_{x_i,j}$	属性 $x_i\in L_j$ 的公有属性密钥	eak	EU 属性密钥
v_e	EU 版本号		

3.1　系统初始化

1）CA 配置：在系统初始化时，CA 选定一个素数 q 和 2 个 q 阶的循环群 G 和 G_T，G 的生成元 g，映射 e：$G\times G\rightarrow G_T$，2 个函数 H：$\{0, 1\}^*\rightarrow G$ 和 F：$\{0, 1\}^*\rightarrow Z_q$，以及一个安全的对称加密算法 $Enc()$. 此外，CA 为每个属性 i 生成一个全局属性标识 x_i；然后，CA 选择 2 个随机数 β，$\gamma\in Z_q$ 作为系统的主密钥，并计算 $e(g, g)^\beta$，$e(g, g)^\gamma$；最后，CA 发布系统参数，即

$$Para=\{g, G, G_T, q, e, H, F, Enc(), e(g, g)^\beta, e(g, g)^\gamma\} \tag{1}$$

2）AMS 配置：CA 向每个 AMS 分发一组属性，且任意 2 个 AMS 不会同时管理相同的属性. 用 L_j 表示 AMS_j 管理的属性集. 对于每个属性 $x_i\in L_j$，AMS_j 选择 2 个随机数 α_{x_i}，$y_{x_i}\in Z_q$ 为秘密属性密钥

$$SK_{x_i,j}=\{\alpha_{x_i}, y_{x_i}\} \tag{2}$$

然后 AMS 计算每个属性 $x_i\in L_j$ 的公开属性密钥

$$PK_{x_i,j}=\{e(g, g)^{\alpha_{x_i}}, g^{y_{x_i}}\} \tag{3}$$

3）EU 注册：CA 向合法的 EU 分配一个全局 EU 标识 e_m，并选择一个随机数 $z_m\in Z_q$ 和一个随机 EU 版本号 $v_e\in Z_q$. 然后，CA 为 e_m 生成一对全局 EU 密钥 GEK 和局部 EU 密钥 LEK，

$$GEK=\{z_m,\ g^{\frac{1}{z_m}}\}\qquad LEK=g^{\frac{\beta}{z_m v_e}}\cdot g^{\frac{\gamma}{v_e}} \tag{4}$$

接下来，CA将GEK和LEK秘密地发送给EU，其中GEK用于EU解密密文，LEK用于检查EU属性密钥eak的有效性. 然后，CA将$\{e_m,\ v_e\}$秘密地发送给AC. 此外，CA计算该EU生成的密钥EGK为

$$EGK=\{g^{\frac{1}{v_e}},\ H(e_m)^{\frac{1}{v_e}}\} \tag{5}$$

最后，将EGK发布给AMC.

3.2 EU属性密钥生成

AMC根据EU的角色向其分配属性集I_m，对于每个属性$x_i\in I_m$，AMC使用EU的EGK生成相应的EU属性密钥$eak_{x_i,\ e_m}$为

$$eak_{x_i,\ e_m}=\{g^{\frac{\alpha_{x_i}}{v_e}}H(e_m)^{\frac{y_{x_i}}{v_e}},\ g^{\frac{F(e_m)y_{x_i}}{v_e}}\} \tag{6}$$

3.3 DMC加密

DMC通过使用对称加密密钥κ加密物流大数据，加密后的Data表示为$Enc_\kappa(Data)$. DMC根据预先制定的访问策略构造线性秘密共享机制(Linear Integer Secret Sharing，LSSS)矩阵$\boldsymbol{R}$[9]，$\boldsymbol{R}$的每一行都和一个与访问策略相关的属性相关联. 然后，DMC定义一个映射π将矩阵$\boldsymbol{R}$的行映射为属性，DMC使用相应的公共属性密钥和系统参数加密对称密钥κ. 步骤为：

S1：DMC选择一个随机数$s\in Z_q$和一个以s为第一个元素的随机向量$v\in Z_q^l$，其中，l表示$\boldsymbol{R}$中相应属性的个数且等于$\boldsymbol{R}$的行数.

S2：对于$\boldsymbol{R}$的每一行，DMC计算$\lambda_x=\boldsymbol{R}_x*v$，其中$\boldsymbol{R}_x$是矩阵$\boldsymbol{R}$的第$x$行. 然后，DMC选择一个以0为第一个元素的随机向量$w\in\boldsymbol{Z}_q^l$，并计算$w_x=R_x*w$

S3：对于$\boldsymbol{R}$的每一行，DMC选择一个随机数$k_x\in\boldsymbol{Z}_q$，并计算密文为

$$C=\kappa e(g,\ g)^{\beta_s} \tag{7}$$

$$C'=g^s \tag{8}$$

$$C_{1,x}=e(g,\ g)^{\gamma\lambda_x}e(g,\ g)^{\alpha_{\pi(x)}k_x},\ \forall x \tag{9}$$

$$C_{2,x}=g^{k_x},\ C_{3,x}=g^{y_{\pi(x)}k_x}g^{w_x},\ \forall x \tag{10}$$

其中$\pi(x)$将$\boldsymbol{R}$的第x行映射到属性x_i.

S4：密文C为

$$C=\langle\boldsymbol{R},\ \pi,\ C,\ C',\ \{C_{1,x},\ C_{2,x},\ C_{3,x},\ \forall x\}\rangle \tag{11}$$

最后，DMC将$CT=\langle Enc_\kappa(Data),\ C\rangle$发送至DSC.

3.4 AC审计

所有已注册的EU可以从DSC查询任何感兴趣的加密数据. 然而，只有当属性满足嵌入密文中的访问策略且属性密钥eak包含正确EU版本号v_e的企业用户e_m才可以在AC协助下解密密文. AC审计过程包含以下步骤：

S1：企业用户e_m将其属性密钥eak和局部EU密钥LEK发送至AC. AC首先通过使用在EU注册过程中生成的EU版本号v_e^*来检查eak的有效性. 其方法为，将v_e^*带入式(6)，计算

$$(g^{\frac{F(e_m)y_{x_i}}{v_e}})^{v_e^*}\overset{?}{=}(g^{y_{x_i}})^{F(e_m)} \tag{12}$$

若式(12)成立，即$v_e^*=v_e$，说明eak有效；否则，eak无效.

S2：如果式(12)成立，AC计算属性集$\{\pi(x):\ x\in X\}\cap I_m$，其中$I_m$和$X$分别表示企业用户$e_m$包含的属性和密文$CT$中LSSS矩阵$\boldsymbol{R}$的行向量集. AC检查这些属性是否存在由(1，0，0，…，0)线性组合构成的子集X'，如果是，计算一组$c_x=\boldsymbol{Z}_q$，使得

$$\sum_{x\in X'}c_x\boldsymbol{R}_x=(1,\ 0,\ 0,\ \cdots,\ 0)$$

其中 $\boldsymbol{R}_x$ 表示 $\boldsymbol{R}$ 的第 x 行. 否则，EU 的属性不满足密文 CT 的访问策略，从而无法解密加密数据.

S3：AC 根据式(13)为每个 $x\in X'$ 计算 $dec(x)$，为

$$dec(x)=\frac{C_{1,x}e(H(e_m),C_{3,x})}{e((g^{\frac{\alpha_{x_i}}{v_e}}H(e_m)^{\frac{y_{x_i}}{v_e}})^{v_e},C_{2,x})},\ \forall x\in X' \tag{13}$$

将式(9)和式(10)代入式(13)，则

$$dec(x)=\frac{e(g,g)^{\gamma\lambda_x}e(g,g)^{\alpha_{\pi(x)}k_x}e(H(e_m),g^{y_{\pi(x)}k_x}g^{\omega_x})}{e((g^{\frac{\alpha_{x_i}}{v_e}}H(e_m)^{\frac{y_{x_i}}{v_e}})^{v_e},g^{k_x})}=$$

$$\frac{e(g,g)^{\gamma\lambda_x}e(g,g)^{\alpha_{\pi(x)}k_x}e(H(e_m),g^{y_{\pi(x)}k_x})e(H(e_m),g^{\omega_x})}{e((g^{\alpha_{x_i}},g^{k_x})e(H(e_m)^{y_{x_i}},g^{k_x})}=$$

$$e(g,g)^{\gamma\lambda_x}e(H(e_m),g)^{w_x} \tag{14}$$

S4：根据文献[11]，

$$\sum_{x\in X'}\lambda_x c_x=s \text{ 和 } \sum_{x\in X'}w_x c_x=0.$$

AC 计算 Token(其值用 T_{Token} 表示)为

$$T_{\text{Token}}=\frac{e(C',LEK^{v_e})}{\prod_{x\in X'}(dec(x))^{c_x}} \tag{15}$$

将式(4)、式(8)和式(14)代入式(15)，得到

$$T_{\text{Token}}=\frac{e(g^s,(g^{\frac{\beta}{z_m v_e}}\cdot g^{\frac{\gamma}{v_e}})^{v_e})}{\prod_{x\in X'}(e(g,g)^{\gamma\lambda_x}e(H(e_m),g)^{w_x})^{c_x}}=$$

$$\frac{e(g,g)^{\frac{\beta s}{z_m}}e(g,g)^{\gamma s}}{e(g,g)^{\gamma\sum_{x\in X'}\lambda_x c_x}e(H(e_m),g)^{\sum_{x\in X'}w_x c_x}}=$$

$$e(g,g)^{\frac{\beta s}{z_m}} \tag{16}$$

然后 AC 将 T_{Token} 发送至 EU.

3.5　EU 解密

根据收到的 T_{Token}，企业用户 e_m 通过使用 GEK 可以很容易地解密密文 C 以获得对称密钥 κ，即

$$\kappa=\frac{C}{T_{\text{Token}}^{z_m}} \tag{17}$$

然后，企业用户 e_m 可以使用该对称密钥以进一步解密加密数据 $Enc_\kappa(Data)$.

3.6　属性撤销

当 EU 的角色发生变化且被撤销了一些属性后，AMC 需要为该 EU 重新计算一组 eak. 首先，CA 选择一个新的随机 EU 版本号 v'_e，并秘密地将$\{e_m,v'_e\}$发送给 AC；然后，CA 计算新的局部 EU 密钥，

$$LEK'=g^{\frac{\beta}{z_m v'_e}}\cdot g^{\frac{\gamma}{v'_e}} \tag{18}$$

并将其发送至该 EU. 然后，CA 计算该 EU 的生成密钥 $EGK'=\{g^{\frac{1}{v'_e}},H(e_m)^{\frac{1}{v'_e}}\}$ 并将 EGK' 发送至 AMC. 最后，AMC 使用该 EU 的新 EGK' 为企业用户 e_m 的每个非撤销属性重新计算新的 eak，即

$$eak_{x_i,e_m}=\{g^{\frac{\alpha_{x_i}}{v'_e}}H(e_m)^{\frac{y_{x_i}}{v'_e}},g^{\frac{F(e_m)y_{x_i}}{v'_e}}\} \tag{19}$$

因此，由于 EU 版本号 v_e 已经过期，被撤销的 EU 属性密钥也变得无效. AC 使用已撤销的 EU 属性密钥无法为该 EU 计算出正确的 T_{Token}.

4 安全分析

本节在CA,AC,AMC,DMC可靠以及DSC,EU不可信的情况下，分析本文所提出的FAC-AR机制的功能.

1) 细粒度访问控制

在将数据发送给DSC之前，DMC首先定义访问策略并使用相应的公共属性密钥来加密对称密钥. 由于LSSS矩阵中定义的访问策略支持“与”门和“或”门，访问控制是细粒度的. 考虑到在没有企业用户属性密钥和企业用户版本号 e_m 时，DSC不能解密数据，因此只有属性满足访问策略的企业用户能够解密密文. 此外，尽管AC为EU承担了很多解密工作，但是在没有全局EU密钥 GEK 时，仍无法单独访问物流大数据. 因此，FAC-AR可以实现细粒度访问控制.

2) 抵抗共谋攻击

在FAC-AR中，2个或多个企业用户无法通过结合他们的属性密钥来共谋访问他们独自都无法访问的数据. 企业用户属性密钥和企业用户身份与该EU的版本号 v_e 相关，假设2个或多个企业用户结合他们的属性密钥能够满足密文的访问策略. 由于不同企业用户的 eak 包含不同的版本号和不同的 $H(e_m)$，无法正确计算出 $(g^{\frac{F(e_m)y_{x_i}}{ve}})^{v'e} \neq (g^{y_{x_i}})^{F(e_m)}$ 和 $dec(x)$，进而导致AC不能为那些共谋企业用户计算出 T_{Token}. 因此这些EU无法进一步解密密文. 即，FAC-AR可以实现抵抗企业用户的共谋攻击.

3) 保护企业用户隐私

包含企业用户属性信息的属性密钥由不同的AMS单独分配，每个AMS只知道EU的部分属性. 因此，单个AMS无法得到EU的全部属性信息. 此外，企业用户使用他们的全局标识与AMS或AC通信，即只有CA知道EU的真实身份. 因此，EU的隐私可以得到很好的保护.

4) 安全属性撤销

当发生属性撤销时，CA选择一个新的随机EU版本号 v'_e 并将其发送给AC. 然后，AMC为该EU没有被撤销的属性重新计算企业用户属性密钥. 假设一个EU试图使用已撤销的属性密钥解密密文，然而，在AC审计阶段，由于已撤销的EU属性密钥不包含正确的版本号 v'_e，则无法正确地计算 $(g^{\frac{F(e_m)y_{x_i}}{ve}})^{v'e} \neq (g^{y_{x_i}})^{F(e_m)}$ 和 $(eak_{x_i,e_m})v'_e$. 因此，FAC-AR可以实现企业用户的属性撤销.

5 总 结

本文针对物流大数据应用过程中由于非授权访问导致的信息泄露问题，提出了一种基于审计中心和CP-ABE的访问控制机制. 安全分析表明，所提机制不仅可以实现细粒度访问控制，还支持抵抗共谋攻击、隐私保护和属性撤销. 受篇幅所限，接下来的工作将对该机制的计算开销、通信开销、存储开销等进行分析推导.

参考文献：

[1] 田 雪，司维鹏，刘莹莹. 大数据在物流企业中的应用 [J]. 电子商务，2015(1)：36－37.

[2] 闫 智，詹 静. 大数据应用模式及安全风险分析 [J]. 计算机与现代化，2014(8)：58－61.

[3] 李嘉诚. 大数据环境下物流企业的数据信息安全保障策略 [J]. 物流工程与管理，2016，38(4)：168－169，175.

[4] 魏凯敏，翁 健，任 奎. 大数据安全保护技术综述 [J]. 网络与信息安全学报，2016，2(4)：1－11.

[5] 栗 龙. 分布环式环境中基于角色访问控制的物流信息系统研究与应用 [D]. 北京：北京邮电大学，2014.

[6] 于莹莹. 基于TRBAC的访问控制模型在物流系统中的研究与应用 [D]. 大连：大连海事大学，2012.

[7] 陈 肖. 物流平台中安全问题的研究与应用实现 [D]. 镇江：江苏科技大学，2014.

[8] 陈 武，周 敏，李虎阳. 一种基于回答集程序的三方协商新机制 [J]. 西南大学学报(自然科学版)，2014，36(5)：

209－213.

[9] 张　晓，秦志光，罗亚东，等. 一种低代价的云计算存储权限管理机制 [J]. 西南师范大学学报(自然科学版)，2015，40(7)：33－40.

[10] GOYAL V，PANDEY O，SAHAI A，et al. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data [C] //Proceedings of the 13th ACM Conference on Computer and Communications Security. New York，NY，USA：ACM，2006：89－98.

[11] LEWKO A，WATERS B. Decentralizing Attribute-Based Encryption [C] // Proceeding of the 30th Annual International Conference of the Theory and Applications of Cryptographic Techniques. Tallinn，Estonia：Springer Verlag，2011：568－588.

An Access Control Scheme with Attribute Revocation for Logistics Big Data

GONG Ge-cui[1]，　MA　Lei[2]

1. *Construction Office of Demonstrational School，Beijing Polytechnic，Beijing 100176，China*；

2. *College of Telecom Engineering，Beijing Polytechnic，Beijing 100176，China*

Abstract：Logistics big data，which contains information such as customer profile and logistic status，is of great use for logistics companies，manufacturers，dealers and other enterprises. Nevertheless，leak of logistics big data may bring serious security risk to the customer and the logistics company. To ensure that the logistics big data is securely and effectively delivered to enterprise users such as manufacturers and dealers，a fine-grained access control scheme with attribute revocation is proposed in this paper，based on the audit center and CP-ABE (ciphertext policy attribute-based encryption) technology. A security analysis demonstrates that the proposed scheme can achieve fine-grained access control，collusion resistance，privacy preservation and secure attribute revocation.

Key words：logistics big data；access control；fine grained；attribute revocation

责任编辑　崔玉洁