doi:10.3969/j.issn.1000-436x.2014.04.007

基于隐含格结构 ABE 算法的移动存储介质情境访问控制

陈波[1]，于泠[1]，强小辉[1]，王岩[2]
(1. 南京师范大学 计算机学院，江苏 南京 210023；2. 麦考瑞大学 计算机学院，悉尼 2109)

摘 要：研究了如何增强可信终端对移动存储介质的访问控制能力，以有效避免通过移动存储介质的敏感信息泄露。首先在隐含密文策略的属性加密方法的基础上，提出了基于格结构的属性策略描述方法。将每个属性构成线性格或子集格，属性集构造成一个乘积格，并利用基于格的多级信息流控制模型制定访问策略。证明了新方法的正确性和安全性。新方法在保持已有隐藏访问策略属性加密算法优点的同时，还能有效简化访问策略的表达，更符合多级安全中敏感信息的共享，能够实现细粒度的访问控制。进一步地，通过将移动存储设备和用户的使用情境作为属性构建访问策略，实现了动态的、细粒度的情境访问控制。最终设计了对移动存储介质进行接入认证、情境访问控制的分层安全管理方案。分析了方案的安全性和灵活性，并通过比较实验说明了应用情境访问控制的方案仍具有较好的处理效率。该方案同样适用于泛在环境下敏感信息的安全管理。

关键词：属性加密；移动存储介质；隐藏访问结构；格安全模型；情境访问控制
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1000-436X(2014)04-0053-12

Contextual access control based on attribute-based encryption with hidden lattice structure for removable storage media

CHEN Bo[1], YU Ling[1], QIANG Xiao-hui[1], WANG Yan[2]
(1. School of Computer Science, Nanjing Normal University, Nanjing 210023, China;
2. Department of Computing, Macquarie University, Sydney 2109, Australia)

Abstract: To prevent data breaches via removable storage media, the way to enhance the access control capability of hosts within trusted zone with removable storage media attached was explored. Firstly, based on traditional Cipher-text-Policy hiding Attribute-Based Encryption (CP-ABE) schemes, an expression with lattice for attributes was proposed. Each attribute was described as a linear lattice or a subset lattice, and an attribute set was described as a product lattice. Furthermore, the lattice-based multi-level access control model was applied to construct access policies. The new scheme was proven fully secure under the standard model. It effectively simplifies the expression of access policies and satisfies fine-grained access control of sensitive information shared in the context of multi-level security. Secondly, considering the ubiquitous usage of removable storage media, some security attributes associating with the context of use were adopted to construct a lattice structure. Then a dynamic access control could be achieved. Finally, based on authorization and dynamic access control, a layered security solution providing multi-level protection for removable storage media was presented. Security and flexibility of proposed solution was analyzed, and a comparison experiment shows that it still has pretty good efficiency. It also can be applied to information security management in other ubiquitous environments.

Key words: attribute-based encryption; removable storage media; hidden access structures; lattice security model; contextual access control

收稿日期：2013-10-13；**修回日期**：2014-01-24
基金项目：江苏省教育科学“十二五”规划重点基金资助项目(B-a/2013/01/013)；江苏省自然科学重大基金资助项目(产学研联合创新基金)(BY2011108)
Foundation Items: The Major Program of the 12th Five Years Education Science Plans of Jiangsu Province(B-a/2013/01/013); The Major Program of Natural Science Foundation of Jiangsu Province(BY2011108)

1 引言

移动存储介质主要是指通过 USB 端口与计算机相连的 U 盘、移动硬盘、存储卡、iPod 等[1]，它们具有体积小、容量大、价格低廉、方便携带、即插即用等特点，不仅在信息交换的过程中得到了广泛应用，也可以作为启动盘创建计算环境[2]。因此，移动存储介质在政府、企事业单位及个人有着广泛的应用。

移动存储介质在给人们带来极大便利的同时，由于它们的丢失、被盗以及滥用也带来了敏感(机密)信息泄露、感染和传播恶意代码以及与操作系统隐蔽交互等安全威胁[3,4]。

通过移动存储介质泄露敏感信息是当前一个非常突出的问题。内、外网物理隔离等安全技术从理论上来说构筑了一个相对封闭的网络环境，使攻击者企图通过网络攻击来获取重要信息的途径被阻断了。而移动存储介质在内、外网计算机间频繁的数据交换，使内、外网“隔而不离、藕断丝连”，很容易造成内网敏感信息的泄露。例如，一种运行在 iPod 等移动存储设备中的 Pod Slurping 隐蔽程序，非法从企业计算机系统中下载敏感数据，给企业造成了巨大的损失[5]。2010 年 4 月起，“维基解密”网站相继公开了近十万份关于伊拉克和阿富汗战争的军事文件，给美国和英国等政府造成了极大的政治影响。经美国军方调查，这些文件的泄露均是由美军前驻伊情报分析员通过移动存储介质非法拷贝所致[6]。2013 年的斯诺登事件更是让大家关注敏感信息泄露问题[7]。

如何有效保护移动存储介质中的敏感信息，已经成为一项重要的课题。

本文将目前针对移动存储介质安全的研究分为两大类：1）安全性改造，主要是将安全控制功能集成到存储设备或专用设备中，例如将智能卡芯片和动态隔离机制绑定到存储设备中[8,9]，或是增加带 USB 接口和可信运行环境的安全板卡[10]；2）安全性增强，主要是通过软件增强可信终端对存储设备的安全控制能力。本文的研究属于后一类。

移动存储介质的安全性增强研究包括 2 个方面：接入前的认证机制和接入后对敏感信息的访问控制。DeviceLock[11]、北信源[12]、中兴通信[13]等公司开发的移动存储介质安全管理产品中通常都采用了基于移动存储介质唯一性标识[14]的认证机制。即通过识别移动存储介质的生产厂商号(VID)、产品号(PID)以及硬件序列号(HSN)等能唯一标识移动存储介质身份的属性，来完成对移动存储介质的接入认证。Yang 等人[15]提出了一种基于 Schnorr 协议的对移动存储介质的用户进行认证的方案。然而，不论是基于移动存储介质的硬件唯一性标识还是针对用户的认证方案，都仍然存在一定的安全风险，在文献[16]中分析了这 2 类方案的安全问题。Lee 等人[17]提出了一种利用移动设备的存储和计算能力，将设备标识及用户身份信息加密存储在设备端，由设备端发起认证和处理的方案。该方案对于无计算能力的存储介质不适用，同时不能有效限定移动设备在内网中的使用。文献[16]提出了一种将移动存储介质与用户身份绑定的安全认证协议，通过可信内网认证服务器有效管理内网中使用的移动存储介质并能限定其接入的范围。

移动存储设备通过接入认证后，对其中敏感信息的保护目前主要采用加密的方法[15, 17~19]。加密后的敏感信息只有通过接入认证的用户才能打开。数据加密方法主要是采用对称加密机制，即为每一合法用户分配一个对称加密密钥，当用户接入认证合法后，认证服务器分配相应的密钥，该用户便可利用该密钥对需要输出到移动存储介质上的敏感信息进行加密，也可以用该密钥打开移动存储介质上已有的加密信息。采用对称加密方法在一定程度上可以避免信息的泄露，但是对于移动存储设备这类应用而言，由于具有存储的资源文件众多、资源使用者不确定和身份可变、使用环境多样等特点，应用对称加密方法存在以下 2 个主要安全问题。

1) 无法适应对每个文件进行细粒度访问控制的要求。已有方法中，由于每位用户拥有一个对称密钥，因此该用户所拷贝的文件均采用同一密钥进行加密，无法做到对不同密级的文件区别对待，不能满足多密级交互的安全需求。即使采用基于公钥基础设施 PKI 的集中式访问控制方式，用户直接与存储设备交互前要先通过认证服务器获取相应的权限证书(密钥)，同时认证服务器必须将授权信息传送给存储设备。这对于移动存储设备的应用而言，效率问题将极大影响移动存储介质的使用，而且资源提供方很难一次获取所有用户的规模与身份，列举用户身份还会侵犯用户的隐私。

2) 无法适应移动存储设备使用环境多变对动态访问控制的要求。已有方法中，只要移动存储介

质接入认证成功后，就可以进行文件的加解密，这是一种静态访问控制方式。为了控制移动存储介质使用的环境，通常采用后台绑定的方式，即在系统初始化阶段为每个移动存储介质建立允许使用该介质的主机 Mac 地址表，一旦策略发生变化，必须人工修改此表。无法做到在移动存储介质安全使用中根据使用人(用户)、使用地点(接入主机安全级别)、使用时间等可能发生的变化动态控制用户的访问权限，因而无法在保证安全性的同时又具有灵活性。

为了解决上述已有访问控制存在的问题，并满足人们对移动存储设备便捷、灵活的使用需求，需要一种新型的更适应泛在应用环境的访问控制方案。Sahai 和 WatersSahai 提出的属性加密(ABE, attribute-based encryption)算法[20]提供了新思路。本文在隐含密文策略的属性加密方法的基础上，通过引入格结构描述属性取值，并将移动存储介质以及用户的使用情境用格结构属性的形式表达。这样，当移动存储介质接入认证成功之后，根据用户的安全级、接入主机的安全级以及使用时间等不同的安全情境，得到不同的属性值集合，根据由此制定的访问策略对移动存储介质上存取的数据进行保护，从而实现细粒度的、动态的访问控制。

2　隐含格结构的属性加密算法

2.1　属性加密算法

属性加密(ABE, attribute-based encryption)算法在细粒度访问控制领域具有广阔的应用前景[21]。这是因为，加密用户无需知道解密用户的具体身份信息，而只需掌握解密用户的一组属性，然后在加密过程中以属性为公钥，将密文和用户私钥与属性相关联，解密时只有符合密文属性要求的解密用户才能解密消息。ABE 算法不再使用传统公钥密码体制中的公钥证书，能够灵活地表示访问控制策略，从而极大地降低了数据共享细粒度访问控制带来的处理开销，比基于身份的密码机制具有更强的适应性和更好的灵活性。

最初提出的基本 ABE 算法仅能支持门限访问控制策略，即只有解密用户属性集与密文属性集相交的元素数量达到系统规定的门限参数时才能解密。为了表示更灵活的访问控制策略，文献[22]提出由接收方(解密用户)制定访问策略的密钥策略 ABE(KP-ABE)，文献[23]提出由发送方(加密用户)规定密文访问策略的密文策略 ABE(CP-ABE)。2 类算法分别适用于查询类的应用和访问控制类应用[21]。

CP-ABE 算法中，加密用户连同密文一起发送给解密用户的访问策略本身也属于敏感信息，应当加以保护，同时为了避免用户攻击系统，文献[24~26]分别在合数群、素数群上提出了一种隐藏访问策略的 ABE 算法。在该类算法中，加密用户事先知道每个属性的所有可能取值，在加密过程中通过隐藏部分子集值以达到使授权用户有效密文和非授权用户无效密文的不可区分性。在解密时，解密用户只需根据密文、自己的属性集以及私钥就能确定是否可以解密成功，而无需知道加密时所用的访问策略，因为只有授权用户的属性对应的密文是良性的，才能解密成功。但是，该算法要求加密用户罗列访问策略所允许的全部属性的取值，这使访问策略的描述冗长且可理解性差，而且对于加密用户而言也显繁琐，如果用户稍有疏漏，少列举一个本应允许的属性取值，将造成系统的误阻止访问；多列举一个本不允许的属性取值，将造成系统的漏阻止访问，从而使整个访问控制系统失效。

在隐藏访问策略的基础上，如何使加密用户便捷地制定出一个可理解的、安全的访问策略，提高隐藏访问策略的 ABE 算法的实用性，是本文工作的一个重点。为此，将格结构引入访问控制策略中，提出了一个隐含格结构的新的 ABE 算法。新机制将每个属性构成线性格或子集格，属性集构造成一个乘积格，利用作者曾经提出的基于格的多级信息流控制模型[27]制定访问策略。该方法在保持已有隐藏访问策略 ABE 算法优点的同时，能有效简化访问控制策略的表达，更符合多级安全中敏感信息的共享，能够实现细粒度的访问控制。

2.2　改进的 CP-ABE 算法

首先给出算法基本概念的形式化定义。

2.2.1　理论基础

定义 1　双线性映射[28]。

设 G_1，G_2 是阶为素数 p 的乘法循环群，g 是 G_1 的生成元，把满足下面性质的映射 e: $G_1\times G_1\to G_2$ 称为双线性映射。

1) 双线性。对任意 $g,h\in G_1$，$a,b\in Z_p$，都有 $e(g^a, h^b)=e(g,h)^{ab}$。

2) 非退化性。$e(g,g)\neq 1$。

3) 可计算性。对 G_1 中任意的元素 g,h，存在有效的算法可计算 $e(g,h)$。

定义 2 拉格朗日插值[20]。

对于 $i \in Z_p$，集合 $\boldsymbol{S} \subseteq Z_p$，拉格朗日系数定义为 $\Delta_{i,\boldsymbol{S}}(x) = \prod_{i \in S, j \neq i} \frac{x-j}{i-j}$。对于 d–1 次的一个多项式 $p(x)$，如果已知集合 $\boldsymbol{S}$ 中包含 d 个数，且对于 $\boldsymbol{S}$ 中任意的 i 都已知 $p(i)$，可以通过插值还原出 $p(x) = \sum_{i \in \boldsymbol{S}} p(i)\Delta_{i,\boldsymbol{S}}(x)$。

定义 3 DBDH(decisional bilinear diffie-hellman assumption)问题[24]。

假定挑战者 $\mathcal{B}$ 通过安全参数 k 可以得到阶为素数 p 的乘法群 G_1, G_2，e: $G_1 \times G_1 \to G_2$ 为双线性映射，g 是 G 的生成元。对随机选取的 $x, y, z \in Z_p^*$，$Z \in G_2$，给定 (g, g^x, g^y, g^z, Z)，要求攻击者 $\mathcal{A}$ 区分 Z 与 $e(g,g)^{xyz}$ 的问题称为(G_1, G_2, e)中的判定双线性 Diffie-Hellman 问题，即 DBDH 问题。

设攻击者 $\mathcal{A}$ 解决上述 DBDH 问题的优势为 ε，如果 $\Pr[\mathcal{A}(g, g^x, g^y, g^z, e(g,g)^{xyz}) = 1] - \Pr[\mathcal{A}(g, g^x, g^y, g^z, Z) = 1] \geqslant \varepsilon$。

定义 4 属性格结构。

设 $\boldsymbol{A}$={$A_1, A_2, \cdots, A_n$}是所有属性的集合，其中 n 是属性的个数。每个属性 A_i 有 n_i 个取值，用 $V_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$ 表示。设 $\leqslant$ 是定义在任意属性 A_i 上的偏序关系，表述属性 n_i 个取值之间的小于等于关系，若 $v_{i,1} \leqslant v_{i,2} \leqslant \cdots \leqslant v_{i,n_i}$，则$(V_i, \leqslant)$是一个线性格，$(V, \leqslant)$是一个乘积格，$V = \{(v_{1,*}, v_{2,*}, \cdots, v_{i,*}) \mid v_{1,*} \in V_1 \wedge v_{2,*} \in V_2 \wedge \cdots \wedge v_{i,*} \in V_i\}$。

定义 5 访问策略。

设用户 U 的属性集合为 $L^{\mathrm{U}} = \{l_1^{\mathrm{U}}, l_2^{\mathrm{U}}, \cdots, l_n^{\mathrm{U}} \mid l_i^{\mathrm{U}} \in V_i, 1 \leqslant i \leqslant n\}$，访问策略 $W = \{w_1, w_2, \cdots w_n \mid w_i \in V_i, 1 \leqslant i \leqslant n\}$。依据基于格的多级信息流控制模型的策略，信息只能由低密级流向高密级，因此只有当用户属性级别高于或等于密文级别时，文件才能被解密。所以，当 $W \leqslant L^{\mathrm{U}}$，即对任意 $1 \leqslant i \leqslant n$，均满足 $w_i \leqslant l_i^{\mathrm{U}}$ 时，称用户属性满足访问策略，记作 $L^{\mathrm{U}} \succ W$。

2.2.2 *算法描述*

执行本算法的实体包括 3 方：授权中心、加密用户和解密用户。算法共分 4 个步骤：初始化、加密、用户密钥生成、解密。详细描述如下。

步骤 1 初始化。

授权中心生成系统参数$(G_1, G_2, p, g \in G_1, e)$，其中，$G_1, G_2$ 是阶为素数 p 的乘法循环群，g 为 G_1 的生成元，e:$G_1 \times G_1 \to G_2$ 为双线性映射。

选取随机数 $\alpha \in Z_p^*$，计算 $Y = e(g,g)^{\alpha}$；选取一组随机数 $\{a_{i,t} \in Z_p^* \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\}$，使 $a_{i,t}$ 对应于属性 A_i 第 t 个取值，记作 $a_{i,t} \leftrightarrow v_{i,t}$。令 $A_{i,t} = g^{a_{i,t}}$，则：

$$PK = < Y, G_1, G_2, p, g, e, \{A_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\} >$$

$$EK = < \{E_{i,t} = A_{i,t}^{id} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\} >$$

id为加密用户标识的散列值。

$$MK = < \alpha, \{a_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\} >。$$

其中，MK 为系统主密钥，PK 为公开密钥。

步骤 2 加密 WM=Encrypt(PK, EK, M, W)。

加密用户使用 PK、EK 和访问策略 $W = \{w_1, w_2, \cdots, w_n \mid w_i \in V_i, 1 \leqslant i \leqslant n\}$，加密明文 M，加密后的密文为 WM。

选取随机数 $r \in Z_p^*$，计算 $C_0 = g^r, \overline{C} = MY^r$：

当 $v_{i,t} = w_i$ 时，$C_{i,t} = A_{i,t}^{r_i}$，其中随机数 r_i 满足 $\sum_{i=1}^{n} r_i = r$；

当 $w_i < v_{i,t}$ 时，$C_{i,t} = E_{i,t}$；当 $v_{i,t} < w_i$ 时，$C_{i,t}$ 取随机值 $X_{i,t}$。

则 $WM = (C_0, \overline{C}, \{C_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\})$。

步骤 3 用户密钥生成 SK_{U}=KeyGen(MK, L^{U})。

授权中心使用 MK，解密用户 U 的属性集合 $L^{\mathrm{U}} = \{l_1^{\mathrm{U}}, l_2^{\mathrm{U}}, \cdots l_n^{\mathrm{U}} \mid l_i^{\mathrm{U}} \in V_i, 1 \leqslant i \leqslant n\}$ 以及加密用户 id，生成用户的私钥 SK_{U}。

选取随机数 $s \in Z_p^*$，计算 $D_0 = g^{\alpha - s}, E = e(g, g)^{s \cdot id}$。

对于所有 $t \in [1, n_i]$，当 $v_{i,t} \leqslant l_i^{\mathrm{U}}$ 时，取 $D_{i,t} = g^{\frac{s}{a_{i,t}}}$；否则，取 $D_{i,t}$ 为随机值。

则 $SK_{\mathrm{U}} = < D_0, E, \{D_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\} >$。

步骤 4 解密 M=Decrypt(WM, SK_U)。

解密用户 U 无需知道访问策略 W，只要使用自己的属性集合 L^{U} 和私钥 SK_{U} 解密密文 WM，得到明文 M。

对于所有 $t_j \in [1, n_i]$，取 $t = \max(t_j)$，使得 $v_{i,t} \leqslant l_i^{\mathrm{U}}$ 且 $e(C_{i,t}, D_{i,t}) \neq E$ 时，则 $C_i = \{C_{i,t} \mid 1 \leqslant i \leqslant n\}$，$D_i = \{D_{i,t} \mid 1 \leqslant i \leqslant n\}$。

解密得 $M = \dfrac{\overline{C}}{e(C_0, D_0) \prod_{i=1}^{n} e(C_i, D_i)}$。

2.2.3 算法分析

1) 正确性

解密时，解密用户出示自己的属性集合 $L^{\mathrm{U}}=\{l_1^{\mathrm{U}},l_2^{\mathrm{U}},\cdots,l_n^{\mathrm{U}}\,|\,l_i^{\mathrm{U}}\in V_i,1\leqslant i\leqslant n\}$，获得私钥 $SK_{\mathrm{U}}=<D_0,E,\{D_{i,t}\,|\,1\leqslant i\leqslant n,1\leqslant t\leqslant n_i\}>$。

如果该解密用户的属性集合满足访问策略 $W=\{w_1,w_2,\cdots w_n\,|\,w_i\in V_i,1\leqslant i\leqslant n\}$，则必存在集合 $T=\{V_{i,t_j}\,|\,V_{i,t_j}\leqslant l_i^{\mathrm{U}},1\leqslant i\leqslant n,1\leqslant t_j\leqslant n_i\}$，使得 $w_i\in T$。又因为当 $w_i<v_{i,t}$ 时，$C_{i,t}=E_{i,t}$，因此，在集合 T 中，满足 $t=\max(t_j)$ 且 $e(C_{i,t},D_{i,t})\neq E$ 的 $v_{i,t}$ 定等于 w_i。因此，取到

$$C_i=\{C_{i,t}=A_{i,t}^{r_i}=g^{a_{i,t}r_i}\,|\,1\leqslant i\leqslant n\}$$

$$D_i=\{D_{i,t}=g^{\frac{s}{a_{i,t}}}\,|\,1\leqslant i\leqslant n\}$$

则

$$\frac{\overline{C}}{e(C_0,D_0)\prod_{i=1}^{n}e(C_i,D_i)}=\frac{MY^r}{e(g^r,g^{\alpha-s})\prod_{i=1}^{n}e(g^{a_{i,t}r_i},g^{\frac{s}{a_{i,t}}})}$$

$$=\frac{Me(g,g)^{r\alpha}}{e(g,g)^{r(\alpha-s)}\prod_{i=1}^{n}e(g,g)^{sr_i}}=\frac{Me(g,g)^{r\alpha}}{e(g,g)^{r(\alpha-s)}e(g,g)^{\sum_{i=1}^{n}sr_i}}$$

$$=\frac{Me(g,g)^{r\alpha}}{e(g,g)^{r(\alpha-s)}e(g,g)^{rs}}=M$$

所以解密成功。

如果该解密用户的属性集合不满足访问策略，则 $w_i\notin T$，取到

$C_i=\{C_{i,t}=X_{i,t}\,|\,1\leqslant i\leqslant n\}\}$，$X_{i,t}$ 为随机数，$1\leqslant i\leqslant n$，因此无法正确解密。

2) 安全性

① 安全模型。本文采用文献[24]的方法，通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{B}$ 之间的游戏(博弈)来定义安全模型。

预备阶段：攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 提交需要挑战的两个访问控制策略 W^0 和 W^1。

初始化阶段：挑战者 $\mathcal{B}$ 运行系统初始化算法生成 PK。

第一阶段：攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 进行有关属性集合 $L^{\mathcal{A}}$ 的私钥询问。挑战者 $\mathcal{B}$ 向攻击者 $\mathcal{A}$ 返回私钥 $SK_{\mathcal{A}}$。此阶段要求 $L^{\mathcal{A}}\succ W^0$ 和 $L^{\mathcal{A}}\succ W^1$ 或者 $L^{\mathcal{A}}\not\succ W^0$ 和 $L^{\mathcal{A}}\not\succ W^1$，同时攻击者 $\mathcal{A}$ 可做重复询问。

挑战：攻击者 $\mathcal{A}$ 提交 2 个消息 M_0 和 M_1，挑战者 $\mathcal{B}$ 随机选择 $ga\in\{0,1\}$,在访问策略 W^{ga} 的条件下，对 M_{ga} 进行加密 Encrypt(PK,EK, M_{ga},W^{ga})，并将密文返回给攻击者 $\mathcal{A}$。在此阶段，如果 $L^{\mathcal{A}}\succ W^0$ *and* $L^{\mathcal{A}}\succ W^1$，则要求 M_0=M_1。

第二阶段：重复第一阶段。

猜测：攻击者 $\mathcal{A}$ 输出对 ga 的猜测 ga'。

攻击者 $\mathcal{A}$ 获得游戏胜利的优势为 Pr[ga'=ga]−1/2。

定义 6 隐含格结构的 ABE 算法是安全的，当且仅当在多项式时间内，所有的有效攻击者最多能以不可忽略的优势赢得上述游戏。

② 安全性证明。假设攻击者 $\mathcal{A}$ 在游戏 Game_1 和 Game_0 中的优势有不可忽略的差异 ε，则可以构造一个挑战者 $\mathcal{B}$ 以 ε 的优势解决 DBDH 问题。类似文献[24]的方法，挑战者 $\mathcal{B}$ 构造方法如下。

在预备阶段：

攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 提交 2 个访问控制策略 W^0 和 W^1。

初始化阶段：

挑战者 $\mathcal{B}$ 设置 G_1,G_2，双线性映射 e 以及生成 g。随机选取 $x,y,z\in Z_p^*,ga\in\{0,1\}$：

当 ga=0 时，进行游戏 Game_0，此时取 $(g^x,g^y,g^z,e(g,g)^{xyz})$；

当 ga=1 时，进行游戏 Game_1，此时取 $(g^x,g^y,g^z,e(g,g)^{\delta})$，其中 δ 为随机数。

挑战者 $\mathcal{B}$ 随机选取任意 $\alpha'\in Z_p^*$，记 $\alpha=xy+\alpha'$，则 $Y=e(g,g)^{xy+\alpha'}$。

对于每个属性 A_i，随机选取值 $k_{i,t}$ ($1\leqslant i\leqslant n$, $1\leqslant t\leqslant n_i$)，记 $a_{i,t}=\dfrac{y}{k_{i,t}}$，则 $A_{i,t}=g^{\frac{y}{k_{i,t}}}=(g^y)^{\frac{1}{k_{i,t}}}$，将公钥 PK 返回给攻击者 $\mathcal{A}$。

第一阶段：攻击者 $\mathcal{A}$ 选择属性集合 $L^{\mathcal{A}}$ 进行私钥询问。此时若 $L^{\mathcal{A}}\succ W^0 and\ L^{\mathcal{A}}\succ W^1$，则在下一步挑战阶段，$M_0$=$M_1$，攻击者 $\mathcal{A}$ 在 Game_0 和 Game_1 中就无优势差异，因此此阶段仅需考虑 $L^{\mathcal{A}}\not\succ W^0 and\ L^{\mathcal{A}}\not\succ W^1$ 的情况。

挑战者 $\mathcal{B}$ 随机选取任意 $s'\in Z_p^*$，记 $s=xy+s'y$，计算私钥 $SK_{\mathcal{A}}$。

$D_0=g^{\alpha-s}=g^{\alpha'-s'y}=g^{\alpha'}(g^y)^{-s'}$；

$E=e(g,g)^{s\cdot id}=(e(g,g)^{xy+s'y})^{id}=(e(g^x,g^y)e(g,g)^{s'y})^{id}=(e(g^x,g^y)^{id})e(g,g^y)^{s'\cdot id}$；

当 $v_{i,t} \leqslant l_i^A$ 时，计算 $D_{i,t} = (g^x)^{k_{i,t}} g^{s' \cdot k_{i,t}} = g^{x \cdot k_{i,t} + s' \cdot k_{i,t}} = g^{(x+s')k_{i,t}} = g^{\frac{(xy+s'y)k_{i,t}}{y}} = g^{s \cdot \frac{k_{i,t}}{y}} = g^{\frac{s}{a_{i,t}}}$；否则 $D_{i,t}$ 取随机值。

将私钥 $< D_0, E, \{D_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\} >$ 返回给 $\mathcal{A}$。

挑战：

攻击者 $\mathcal{A}$ 选择 2 个消息 M_0 和 M_1，挑战者 $\mathcal{B}$ 随机选取 $ga \in \{0,1\}$ 对 M_{ga} 进行加密。

计算 $C_0 = g^z, \overline{C} = M_{ga} Y^{\alpha z} = M_{ga} e(g,g)^{xyz} e(g,g)^{\alpha' z} = M_{ga} Ze(C, g\alpha')$。当 ga=0 时，Z=$e(g, g)^{xyz}$；当 ga=1 时，$Z = e(g,g)^{\delta}$。因此 $\overline{C}$ 是 G_1 群上的随机值。

当 $v_{i,t} = w_i^{ga}$ 时，$C_{i,t} = A_{i,t}^{u_i} = (g^y)^{\frac{u_i}{k_{i,t}}}$，其中随机数 u_i 满足 $\sum_{i=1}^{n} u_i = z$；

当 $w_i^{ga} < v_{i,t}$ 时，$C_{i,t} = A_{i,t}^{id} = (g^y)^{\frac{id}{k_{i,t}}}$；当 $v_{i,t} < w_i^{ga}$ 时，$C_{i,t}$ 取随机值。

挑战者将密文 $(C_0, \overline{C}, \{C_{i,t} \mid 1 \leqslant i \leqslant n, 1 \leqslant t \leqslant n_i\})$ 返回给攻击者 $\mathcal{A}$。

第二阶段：与第一阶段相同，继续私钥的询问。

猜测：

攻击者 $\mathcal{A}$ 输出对 ga 的猜测 ga'，如果 $ga' = ga$，挑战者 $\mathcal{B}$ 输出 1；否则，挑战者 $\mathcal{B}$ 输出结果为 0。根据假设，在游戏 Game_1 中攻击者 $\mathcal{A}$ 猜测正确的概率比在 Game_0 中猜测正确的概率有 ε 优势，因此构造的挑战者 $\mathcal{B}$ 可以 ε 的优势解决 DBDH 假设。

3) 访问策略的简洁性

与文献[24~26]相比，本文给出的算法简化了访问策略，缩短了策略长度。

在文献[28]中，访问策略中用操作符“与”连接不同的属性，用“或门”连接同一个属性的不同取值，如

$$w = ((A_1 = v_{1,1} \vee A_1 = v_{1,2}) \wedge (A_2 = v_{2,3}) \wedge \cdots \wedge (A_n = v_{n,2} \vee \cdots A_n = v_{n,t} \vee \cdots))$$

在这种表达策略的方式下，由于属性取值间没有内在关系，因此必须罗列出所有允许的属性取值，这势必增加访问策略的长度，且容易造成本文 2.1 节所指出的误阻止访问和漏阻止访问问题。

本文借鉴基于格的多级信息流控制模型中对主体和客体安全级别的表达方式，在定义 4 中将属性集组成一个格结构，根据信息由低密级流向高密级时不会发生信息泄露的原则，可以看出只有当用户 U 的属性级别高于等于密文级别时，文件能被解密才是安全的。由此，在访问策略中仅需给出每个属性所允许的最小取值即可，如上述访问控制策略就可简化为

$$w = ((A_1 = v_{1,1}) \wedge (A_2 = v_{2,3}) \wedge \cdots \wedge (A_n = v_{n,2}))$$

本文提出的算法在保持传统隐藏访问策略 CP-ABE 算法的优点的同时，能有效简化访问控制策略的制定，并在一定程度上减少加密时的指数运算。表 1 给出了在最坏情况下本文算法与文献[24~26]中隐藏访问策略 CP-ABE 算法的比较，其中 $|A|$表示属性总个数，$|V|$表示$|A|$个属性所有可能的取值，$|W|$表示策略长度，有$|V| \geqslant |W| \geqslant |A|$。

3 移动存储介质的情境访问控制

移动存储设备这类应用具有存储的资源文件众多、资源使用者不确定和身份可变、使用环境多样等特点。目前对移动存储介质所采用的、接入认证后对敏感信息进行加密的访问控制方法是一种粗粒度的、静态的访问控制方法，已不能满足人们对移动存储设备的安全性兼顾便捷性和灵活性的

表 1 **本文算法与文献[24~26]的比较(最坏情况下)**

	策略长度	初始阶段		加密		生成密钥		解密	
		指数运算	Pair	指数运算	Pair	指数运算	Pair	指数运算	Pair
文献[24]	$\|W\|$	$2\|V\|+1$	1	$2\|W\|+2$	0	$3\|A\|+1$	0	0	$3\|A\|+1$
文献[25]	$\|W\|$	$\|V\|+1$	1	$\|V\|+2$	0	$\|V\|+\|A\|+1$	0	0	$\|A\|+1$
文献[26]	$\|W\|$	0	1	$2\|W\|+1$	0	$4\|A\|$	0	0	$4\|A\|$
本文	$\|A\|$	$\|V\|+1$	1	$\|A\|+2$	0	$\|A\| \times \|V\|+1$	1	0	$2\|A\|+1$

需求。为此，本文提出了情境访问控制的方法，并应用于移动存储介质的安全性管理。

3.1　情境访问控制方法

3.1.1　情境访问控制

CP-ABE 算法颠覆了传统公私钥加密算法中，明文公钥加密后只能由唯一的私钥才能解密的思想。算法中，由数据创建者利用访问控制策略对数据进行加密，而每个数据访问者均有一个与自身特质相对应的解密密钥，只要该数据访问者的特质与访问控制策略相符，那他所拥有的密钥就能进行解密操作。

资源创建者在将敏感文档写入到移动存储设备之前，利用访问控制策略对文档进行加密；资源访问者首先根据自身的属性产生解密密钥，然后对密文资源进行解密，此时只有访问者自身属性满足访问控制策略时，解密才能成功，从而实现了对资源的访问控制。例如，资源创建者采用树形结构来定义访问控制策略，他要求只有属于部门 1 的经理或销售员才能解密文件。若访问者 UA 的属性是{部门 1，经理}，访问者 UB 的属性是{部门 1，销售}，因此访问者 UA、UB 均可以解密文件正常访问，而若访问者 UC 的属性是{部门 2，经理}，其属性不符合访问控制策略，从而无法正常解密访问文件。从上述描述可以看出 CP-ABE 算法最突出的优点是明文加密后，可有多个符合解密访问策略的解密密钥进行解密，因此这样的算法适用于移动存储介质这种泛在环境下的应用情况。

在 CP-ABE 算法的应用中，通常选取访问者固有的属性来表达访问者的特质，如访问者单位、身份等，而不考虑访问操作执行时的情境。为了满足移动存储设备既安全又灵活的使用需求，需要在不同情境下动态控制用户的访问权限。为此，本文采用第 2 节提出的隐含格结构 ABE 算法，选取移动存储设备和用户的使用情境作为属性构建访问策略。当移动存储介质接入认证成功之后，根据它当时所处的安全情境(例如用户的安全级别、接入主机的安全级别以及接入时间等)，得到实时的属性值集合，从而实现基于用户安全级别、使用时间、使用环境等情境的动态的访问控制，本文称之为情境访问控制。这样可在无需修改访问控制策略的基础上，访问控制随着用户所处实时情境进行适应性变化，以动态控制用户的访问权限，在保证安全性的同时又具有很高的灵活性。

3.1.2　移动存储介质使用情境的格化

为了能根据当前使用移动存储介质的情境进行动态访问控制，需要将情境用一个格结构的属性集来表达。

定义 7　使用情境。

移动存储介质的使用情境由用户安全级、接入主机安全级以及使用时间安全级构成，即

$$Context=\{(a_u,a_l,a_t)\mid a_u\in A_u\wedge a_l\in A_l\wedge a_t\in A_t\}$$

其中，A_u为用户安全级别集合，$\leqslant$是定义在 A_u上的运算，表示安全级别之间的小于等于关系，则$(A_u,\leqslant)$是一个线性格，同时$(A_l,\leqslant)$和$(A_t,\leqslant)$也为线性格。使用情境$(Context,\leqslant)$为一个乘积格，$context^1\leqslant context^2$，当且仅当$a_u^1\leqslant a_u^2\wedge a_l^1\leqslant a_l^2\wedge a_t^1\leqslant a_t^2$。

根据基于格的多级信息流控制模型[27]，为使敏感信息不泄露，一个主体可以访问一个信息，当且仅当该主体的安全级别至少与该信息的安全级别一样高。因此，为了防止移动存储介质中的信息泄露，必须满足$Context^1\vdash File:W\leqslant Context^2\vdash File:R$，即：读取文件时的情境安全级别至少与该文件存入移动存储介质时情境的安全级别一样高。

表 2 给出了各情境属性的取值。将这些情境参数作为隐含格结构 ABE 算法中的属性，就可以进行信息的访问控制。

表 2　　**各情境属性的取值**

情境参数	取值
用户安全级 A_u	0(普通)，1(秘密)，2(机密)，3(绝密)
接入主机安全级 A_l	0(公开)，1(秘密)，2(机密)，3(绝密)
使用时间安全级 A_t	0(业余)，1(加班)，2(上班)

3.1.3　信息存取控制

为了提高效率，本文并未采用提出的隐含格结构 ABE 算法直接对文件进行加密，而是为每个需要加密的文件 File 生成一个基于 AES 的对称密钥 Key，用 Key 对 File 进行对称加密，然后用隐含格结构 ABE 算法对 Key 进行加密，最后将加密后的 Key 和加密后的文件作为一个密文整体存入移动存储介质中。解密时，首先利用隐含格结构 ABE 算法解密得到 Key，然后用 Key 再解密文件即可。

3.2　移动存储介质分层防护方案

本文运用系统安全的整体性及分层性防护的原则，将外接移动存储设备、终端用户、可信内网整体纳入安全管理和控制中，从以往的应用单点安

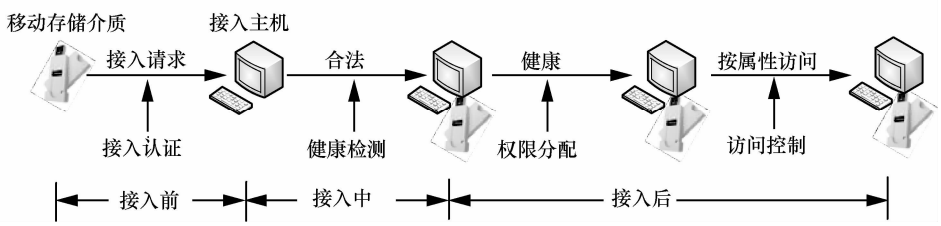

图 1　移动存储介质敏感信息分层防护

全设备控制拓展到整个可信域及边界的安全控制。如图 1 所示，将移动存储介质的使用分为接入的前、中、后 3 个阶段，通过对移动存储介质的接入认证、健康检测、权限管理以及最终的情境访问控制等安全措施，来完成多级安全中敏感信息的防护。

1) 接入前的阶段主要是进行接入认证。

2) 接入中的阶段是指移动存储介质通过合法身份认证后，可正常接入主机，但还不能进行任何操作的时间段。本阶段主要解决的问题是健康状态检测。健康状态包括对接入终端主机及移动存储介质双方的检测。这是因为，移动存储介质使用范围较广，不可避免地会出现在外网使用时感染计算机病毒的情况。同样，如果接入终端存在病毒或恶意程序，也会影响移动存储介质的安全性。

3) 接入后的阶段是指根据健康状态的检测结果，赋予移动存储介质相应的权限，包括拒绝、只读以及读写。

移动存储介质获得相应权限后，就可以进行正常的操作。鉴于移动存储介质主要的功能是进行信息的存取，因此，对移动存储介质中信息的访问控制是确保移动存储介质安全使用的关键点。当将接入终端上的文件存入移动存储介质时，对文件进行加密；当从移动存储介质中读取文件时，只有符合条件时，才能正确解密并获得相应的明文。

防护系统主要工作流程如图 2 所示。系统包含 5 个实体，分别为：移动存储介质(M)、用户(U)、接入终端主机(C)、接入认证服务器(AS)以及授权服务器(PS)。其中接入认证服务器负责接入认证，接入终端主机负责进行健康检测，授权服务器负责权限的分配。

系统分层防护的主要工作流程如下。

步骤 1　移动存储介质要求与终端主机连接，终端主机读取移动存储介质中的数字证书(1a)并接受用户输入用户名和密码(1b)。

步骤 2　接入终端将数字证书、用户信息以及自身信息提交给认证服务器。

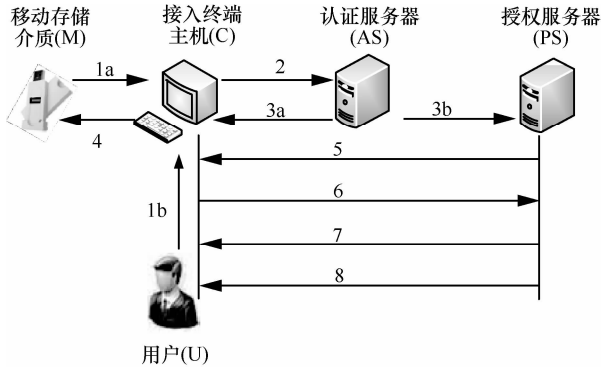

图 2　系统框架及流程

步骤 3　认证服务器根据收到的信息，进行接入认证，并将认证结果返回给接入终端主机(3a)，同时若认证成功，认证服务器向授权服务器转发属性证书请求(3b)。

步骤 4　接入终端主机根据收到的认证结果，执行对移动存储介质的接入控制。

步骤 5　授权服务器收到属性证书请求后，下发健康状态检测器。

步骤 6　接入主机收到下发健康检测器后进行相应检测，并将检测结果送给权限服务器。

步骤 7　权限服务器根据健康状态检测结果赋予介质相应的权限集。

步骤 8　当移动存储介质进行具体文件的存取时，进行加解密操作。

3.2.1　接入认证

针对目前移动存储介质接入认证机制均存在的安全性问题，作者提出了一种基于用户与存储介质绑定的双因子认证方法，该方法既考虑用户信息，也认证物理特性，能很好地做到用户和移动存储介质的绑定。相关技术细节已在文献[16]中介绍，本文不再赘述。

3.2.2　健康状态检测及权限分配

健康状态检测由授权服务器下发的健康状态检测器对移动存储介质和接入终端主机的健康状态进行检测。

定义 8　健康指数。

健康状态用量化的健康指数 $H(x)$表达。$H(\mathrm{M})$表示移动存储介质 M 的健康指数，为

$$H(\mathrm{M})=\begin{cases}0, \text{M中未检出恶意代码}\\ 1, \text{M中检出恶意代码}\end{cases}$$

$H(\mathrm{C})$表示接入终端主机 C 的健康指数为

$$H(\mathrm{C})=1\,000h_1(\mathrm{C})+100h_2(\mathrm{C})+h_3(\mathrm{C})+h_4(\mathrm{C})$$

其中，$h_1(\mathrm{C})$表示木马指数，$h_2(\mathrm{C})$表示病毒指数，$h_3(\mathrm{C})$表示未打补丁指数，$h_4(\mathrm{C})$表示自启项指数，且 $h_i(\mathrm{C})\in[0,0.1,0.2,\cdots,1], i\in[1,4]$ 表示各类的危害程度，危害越大取值越大。

定义 9　移动存储介质权限集。

当移动存储介质中检测出恶意代码，该移动存储介质将无法使用，否则，根据接入主机的健康状态赋予移动存储介质相应的读(R)、写(W)权限。移动存储介质权限集用 ACC(M)表示为

$$ACC(\mathrm{M})=\begin{cases}\mathrm{R}, H(\mathrm{M})=0, H(\mathrm{C})<100\\ \mathrm{RW}, H(\mathrm{M})=0, H(\mathrm{C})<10\\ \mathrm{DENY}, H(\mathrm{M})=1\end{cases}$$

3.2.3　情境访问控制流程

下面以用户 U 利用移动存储介质 M 在接入终端主机 C 上存取文件 File 为例，描述信息存取访问控制技术的实现细节。

首先，介绍在存取控制中用到的存储介质权限表、用户安全级别表、主机安全级别表以及文件属性表。这 4 类表格均存储在授权服务器上，存储介质权限表在对介质进行健康检测后的权限分配阶段产生，表中包括“移动存储介质唯一性标识”、“权限”和“时间戳”3 项内容。“权限”根据健康状态检测结果动态给出，“时间戳”用于记录最新权限赋予的时间。

在用户注册阶段，系统会为每个用户在用户安全级别表中生成一条记录，格式为：{用户 *id*，安全级别，时间戳}，其中安全级别取值如表 2 所示。系统根据用户行为可随时调整该用户的安全级别，调整时间以时间戳方式记录。

系统在初始化阶段会根据主机所在部门等因素，为每台主机在主机安全级别表中生成一条记录，格式为：{主机 Mac，安全级别，时间戳}，其中安全级别取值如表 2 所示。系统可根据健康状态检测的结果，调整主机的安全级别，调整时间以时间戳方式记录。

当每个文件被创建或修改时，系统会在文件属性表中为此文件建立一条记录，格式为：{文件名，创建者或最终修改者 *id*，时间戳}。

1) 存入文件

步骤 1　C 向 PS 发送操作请求，请求协议格式为：Write|Id(M)|File|Mac(C)。其中 Write 表示操作类型为向移动存储介质 M 中存入文件，Id(M)表示移动存储介质唯一性标识，File 表示需存入的文件名，Mac(C)表示接入终端主机 C 的网卡硬件地址。

步骤 2　PS 收到操作请求后，利用 Id(M)查看移动存储介质权限表中 Id(M)所对应的权限，如无此权限，返回 DENY；若有此权限，则查看相应文件属性表和用户安全级别表得到相应文件的 A_u 属性值，查看主机安全级别表得到相应主机的 A_l 属性值，然后根据系统时间得到相应的 A_t 属性值。返回当前访问情境 $Context=\{(a_u,a_l,a_t)\,|\,a_u\in A_u\wedge a_l\in A_l\wedge a_t\in A_t\}$。

步骤 3　C 收到访问情境后，首先产生相应的访问策略 $W=\{(w_1,w_2,w_3)\,|\,w_1=a_u,w_2=a_l,w_3=a_t)\}$，用对称密钥 Key 对文件加密得 $\mathrm{E_{Key}}$(File)，然后采用隐含格结构的 ABE 算法对对称密钥 Key 进行加密：*WK*=Encrypt(*PK*,*EK*,*Key*,*W*)。

步骤 4　C 将 *WK* 与 E_{Key}(File)作为一个密文整体写入 M 中。

2) 读取文件

步骤 1　C 向 PS 发送操作请求，请求协议格式为：Read|Id(M)|Id(U)|Mac(C)。

步骤 2　PS 收到操作请求后，利用 Id(M)查看移动存储介质权限表中相应 Id(M)所对应权限，如无此权限，返回 DENY；若有此权限，则 PS 根据相应用户安全级别表得到试图读取文件的用户 A_u 属性值，查看主机安全级别表得到相应主机的 A_l 属性值，根据系统时间得到相应的 A_t 属性值。由此产生试图读取该文件的用户属性 $L=\{(l_1,l_2,l_3)\,|\,l_1=a_u, l_2=a_l, l_3=a_t)\}$，然后采用隐含格结构的 ABE 算法产生解密私钥 *SK*=KeyGen(*MK*,*L*)，并将其返回给 C。

步骤 3　C 收到解密私钥后，首先读取密文首部，获得对称密钥密文 *WK*，然后用私钥对其解密得 Key= Decrypt(*WK*,*SK*)。最后用解密后的对称密钥对文件密文解密 $\mathrm{D_{Key}}(\mathrm{E_{Key}}(\mathrm{File}))$。

3.3　方案分析

本文所提出的方案能很好地实现移动存储介质信息存取的访问控制，具有良好的安全性、灵活性及效率。

1) 安全性

移动存储介质在使用过程当中，遭受的攻击主要有冒用攻击、摆渡攻击以及滥用攻击[16]。下面针对这 3 类攻击，分析本文所提出方案的安全性。

① 冒用攻击。冒用攻击主要手段有：改变用户和伪造移动存储介质。所谓改变用户是指对于一个属于用户 UA 的移动存储介质 M，被用户 UB 获得后，用户 UB 试图得到合法的使用权限；伪造移动存储介质是指用户用未注册过的移动存储介质取代合法注册过的移动存储介质，以期能得到合法的使用权限。

为了抵抗此类攻击，本文所给方案在移动存储介质接入前采用了双因子认证技术，即综合了移动存储介质唯一性标识和用户信息。只有当一个合法用户将一个合法的移动存储介质接入系统，才能获得合法性认证，否则，移动存储介质将无法接入系统。限于篇幅，本文不再对双因子认证技术展开说明，文献[16]中有详细阐述。

② 摆渡攻击。摆渡攻击一般通过摆渡木马将可信系统内部的敏感文件隐蔽写入移动存储设备中，一旦该移动存储设备再接入到连接互联网的计算机上，木马就会将这些敏感文件自动发送到指定计算机中。

为了抵抗此类攻击，本文所给方案在移动存储介质接入中，采用了动态授权技术，即先对移动存储介质进行健康状态的检测，然后根据此时移动存储介质的健康指数，分配相应的权限。根据 3.2.2 节中的描述，当移动存储介质中存在摆渡木马时，移动存储介质的健康指数 H(M)必等于 1，根据权限分配方案，此时移动存储介质权限集 ACC(M)=*DENY*，说明此时的移动存储介质不能进行任何读写操作，因此，摆渡木马便无法将敏感文件写入移动存储设备中，从而抵抗摆渡攻击。

③ 滥用攻击。本文所谓滥用攻击是指一个合法的用户将一个合法的移动存储介质接入系统后，在不合法的情境中进行了文件的读取，从而导致敏感信息的泄露。

为了抵抗此类攻击，本文所给方案在移动存储介质接入后，根据它所处的安全情境不同，利用隐含格结构的 ABE 算法对文件进行加解密，从而有效防止了信息从高密级的使用环境流向低密级的使用环境而造成信息的泄露。

为了清晰地介绍本文提出方案的安全性及应用效果，下面以一个简化的实例加以说明。

在正常工作时间，当用户 U 在主机 C(Mac=44-45-53-54-00-00)上接入移动存储介质 M(*id*=43278)后，假设接入认证通过，且权限分配为 RW，此时用户 U 需将主机中名为 abc.doc 的文件拷贝至 M 中。此时用户安全级别、主机安全级别以及文件属性如表 3~表 5 所示。

表 3 用户安全级别

用户 id	安全级别	时间戳
908	2	1377151510
123	2	1376962830
…	…	…

表 4 文件属性

文件名	用户 id	时间戳
abc.doc	123	1378174815
…	…	…

表 5 主机安全级别

MAC	安全级别	时间戳
F0-DE-F1-5F-18-5A	1	1373851233
44-45-53-54-00-00	2	1373934790
…	…	…

C 向 PS 发出操作请求：Write|43278|abc.doc|44-45-53-54-00-00。PS 根据上述各表的情况得出当前情境取值：*Context*=(2,2,2)并将此结果返回给 C，C 用密钥 Key 对文件 abc.doc 进行 AES 加密，然后利用访问策略 W=(2,2,2)对 Key 进行加密得 WK，最后将 WK 和密文作为整体存入 M 中。

此后，当用户 U(*id*=908)将存有该秘密信息的 M 在另一正常工作时间接入终端主机 C(Mac=F0-DE-F1-5F-18-5A)时(假设接入认证通过，且权限分配为 *RW*)，若要读取此密文信息，必须发送操作请求：Read|43278|908| F0-DE-F1-5F-18-5A 至 PS，PS 根据上述表格，可得当前用户的属性 L=(2,1,2)，由此计算出解密私钥 SK，并返回给 U。但由于 L 中的第 2 项小于 W 中的第 2 项，根据隐含格结构的 ABE 算法可知，此时的用户属性 L 是不满足访问策略 W 的，因此用户 U 利用此私钥将无法正确解密得到 Key，从而也无法还原明文 abc.doc。这样就确保了不会因信息从高密级的使用环境流向低密级使用环境而造成信息的泄露。

2) 灵活性

由于本文的方案采用基于用户安全级别、使用时间、使用环境等情境属性进行加解密，因此对文

件的存取能做到细粒度的控制，这比目前普遍采用的一个用户拥有一个对称密钥，只要是该用户进行存取时都采用统一密钥的方法控制粒度更细。

再者，移动存储介质的一个重要功能是信息交换，在目前已有的方案中，为了控制移动存储介质使用的环境，通常采用后台绑定的方式，即在系统初始化阶段为每个移动存储介质建立允许使用该介质的主机 MAC 地址表，一旦策略发生变化，必须人工修改此表。而本文提出的情境访问控制方法，可在无需修改访问控制策略的基础上，访问控制随着用户所处实时情境进行适应性变化，以动态控制用户是否可以读取相应安全级别的信息，这样，在保证安全性的同时又具有很高的灵活性。

3) 效率

本文提出的隐含格结构的 ABE 算法，在保持传统隐藏访问策略 ABE 算法优点的同时，能有效简化访问控制策略的制定，并在一定程度上减少加密时的指数运算(如表 1 所示)。基于新算法给出的方案在确保安全性的同时，也充分考虑到了效率问题，因此采用了混合加密体制，用对称密钥对文件进行加密以保证加密的高效性；同时用隐含格结构的 ABE 算法对对称加密密钥进行加密，以保证加密密钥的安全性。

表 6 给出了目前已有移动存储设备安全解决方案中通常采用的单纯对称加密的效率与本文方案混合加密效率的比较。实验环境为：接入终端主机为联想 PC 机，含 1 个 Intel Core2 Duo E7500 2.93 GHz CPU，2 GB 内存。实验中对称加密算法采用 256 bit AES 密钥，实验代码基于.NET 基础类库在 system.security.cryptography 命名空间下实现的加密服务提供类进行了封装。从表 6 中可以看出，本文方案尽管增加了利用隐含格结构的 ABE 算法对对称加密密钥进行加密的过程，但对效率的影响并不算太大，相较于安全性和灵活性的提高，这点代价是值得的。

表 6　单纯对称加密和本方案混合加密的效率比较(单位: s)

文件大小/KB	单纯对称加密		混合加密	
	加密	解密	加密	解密
1,830	0.297	0.266	0.398	0.462
22,960	2.765	2.375	2.866	2.573
1113,822	13.312	11.391	13.414	11.590
322,373	38.172	32.515	38.271	32.711

4　结束语

通过移动存储介质泄露敏感信息是当前一个非常突出的问题。本文研究了如何增强可信终端对移动存储设备的安全控制能力，以有效避免移动存储介质中的敏感信息泄露问题。

本文的工作主要包括 2 个方面：在隐含密文策略的属性加密方法(CP-ABE)的基础上，提出了基于格结构的属性策略描述方法；将移动存储介质的使用情境用格结构属性的形式表达。从而利用 ABE 算法的特点实现了细粒度、动态的访问控制。

通常的 CP-ABE 机制相比基于身份的密码机制，能够灵活地表示访问控制策略，适用于分布式环境中的信息共享。本文针对其访问策略的描述冗长且可理解性差等缺陷，提出了基于格的多级信息流控制模型来制定访问策略，在保持已有隐藏访问策略 ABE 算法优点的同时，能有效简化访问控制策略的制定，更符合多级安全中敏感信息的共享，能够实现细粒度的访问控制。

目前移动存储设备中敏感信息的访问控制主要采用数据加密的方法，这种静态访问控制方式不能适应移动存储设备在泛在应用环境中的数据安全防护，因为共享用户安全级不确定，连接的主机安全级不确定。本文提出的情境访问控制基于所提出的隐含格结构 ABE 算法，选取移动存储设备和用户的使用情境作为属性构建访问策略。当移动存储介质接入认证成功之后，访问控制可以随着用户所处实时情境(用户的安全级别、接入主机的安全级别以及接入时间等)进行适应性变化，以动态控制用户的访问权限，在保证安全性的同时又具有很高的灵活性。

本文设计的移动存储介质安全管理方案包括接入前的认证和接入后的情境访问控制，能够实现多层次的安全防护。该方案将外接移动存储设备、终端用户、可信内网整体纳入安全管理和控制中，从以往的单点安全控制拓展到整个可信域及边界的安全控制。本文提出的新方法同样适用于泛在应用环境下敏感信息的访问控制。

参考文献：

[1] IEEE Computer Society. IEEE Standard for Authentication in Host Attachments of Transient Storage Devices[S]. 2010.

[2] HALSEY M. Beginning Windows 8[M]. Berkeley, CA: Apress, 2012.

[3] TETMEYER A, SAIEDIAN H. Security threats and mitigating risk for USB devices[J]. IEEE Technology and Society Magazine, 2010, 29(4): 44-49.

[4] PHAM D V, SYED A, HALGAMUGE M N. Universal serial bus based software attacks and protection solutions[J]. Digital Investigation, 2011, 7(3):172-184.

[5] GFI White Paper. Pod Slurping-an Easy Technique for Stealing Data[R]. 2011.

[6] BERGHEL H. WikiLeaks and the matter of private manning[J]. Computer, 2012, 45(3):70-73.

[7] LANDAU S. Making sense from snowden: what's significant in the NSA surveillance revelations[J]. IEEE Security & Privacy, 2013, 11(4): 54-63.

[8] 吴世忠, 石超英. 一种智能卡和U盘复合设备及其与计算机通信的方法[P]. 中国专利 200710000328.3, 2007.
WU S Z, SHI C Y. Smart Card and USB Combined Equipment and Method for Communication with Computer[P]. Chinese Patent 200710000328.3, 2007.

[9] 马俊, 王志英, 任江春等. TRSF: 一种移动存储设备主动防护框架[J]. 电子学报, 2012, 40(2): 376-383.
MA J, WANG Z Y, REN J C, *et al*. TRSF: a positive protection framework for removable storage devices[J]. Acta Electronic Sinica, 2012, 40 (2): 376-383.

[10] 张功萱, 沈创业, 王平立等. 移动存储信息的信任链动态跟踪技术研究[J]. 计算机研究与发展, 2011, 48(S1): 37-42.
ZHANG G X, SHEN C Y, WANG P L, *et al*. The research of dynamic track technology for removable storage information's trusted chain[J]. Journal of Computer Research and Development, 2011, 48(S1):37-42.

[11] DeviceLock. Endpoint DLP suite[EB/OL]. http://www.devicelock.com/dl/features.html, 2013.

[12] VRV SpecSEC[EB/OL]. http://web.vrv.com.cn/products.html, 2013.

[13] 中兴通信股份有限公司. 一种实现接入认证的方法、装置及一种移动终端[P]. 中国专利 200910133730.8, 2009.
ZTE CORPORATION. Method to Implement Access Authentication, Equipment and a Mobile Terminal[P]. Chinese Patent 200910133730.8, 2009.

[14] 廖洪其, 凌捷, 郝彦军等. USB 移动存储设备的惟一性识别方法研究[J]. 计算机工程与设计, 2010, 31(12):2778-2780.
LIAO H Q, LING J, HE Y J, *et al*. The research of unique identification for USB removable storage devices[J]. Computer Engineering and Design, 2010, 31(12): 2778-2780.

[15] YANG F Y, WU T D, CHIU S H. A secure control protocol for USB mass storage devices[J]. IEEE Transactions on Consumer Electronics, 2010, 56(4):2339-2343.

[16] CHEN B, QIN C F, YU L. A secure access authentication scheme for removable storage media[J]. Journal of Information & Computational Science, 2012, 9(15): 4353-4363.

[17] LEE K, YIM K, SPAFFORD E H. Reverse-safe authentication protocol for secure USB memories[J]. Security and Communication Networks, 2012, 5(8):834-845.

[18] 孙国梓, 陈丹伟, 吴登荣等. 一种安全移动存储系统的研究与实现[J]. 计算机工程, 2009, 35(11):116-119.
SUN G Z, CHEN D W, WU D R, *et al*. The research and implementation of secure removable storage system[J]. Computer Engineering, 2009, 35(11):116-119.

[19] 伟利迅半导体有限公司. 基于同步用户和主机认证的加密可移动存储设备[P]. 中国专利 201110184775.5, 2011.
SuperSpeed Semiconductors Co Ltd. The Encryption of Removable Storage Devices Based on Synchronization of User and Master Authentication[P]. Chinese Patent 201110184775.5, 2011.

[20] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005)[C]. Aarhus, Berlin, GER, 2005. 457-473.

[21] 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*. Attributes radical encryption mechanism[J]. Journal of Software, 2011, 22(6): 1299-1315.

[22] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-Based encryption for fine-grained access control of encrypted data[A]. 2006 ACM Conf on Computer and Communications Security (CCS'06)[C]. Alexandria, New York, USA, 2006. 89-98.

[23] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy attribute-based encryption[A]. 2007 IEEE Symposium on Security and Privacy (SP'07)[C]. Berkeley, California, USA, 2007. 321-334.

[24] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[A]. 6th International Conference on Applied Cryptography and Network Security (ACNS'08)[C]. New York, Berlin, GER, 2008. 111-129.

[25] LAI J, DENG R H, LI Y. Fully secure cipertext-policy hiding CP-ABE[A]. 7th International Conference on Information Security Practice and Experience (ISPEC 2011)[C]. Guangzhou, Berlin, GER, 2011. 24-39.

[26] LI J, REN K, ZHU B, *et al*. Privacy-aware attribute-based encryption with user accountability[A]. 12th International Conference on Information Security (ISC'09)[C]. Pisa, Berlin, GER, 2009. 347-362.

[27] 于泠, 陈波, 肖军模. 多策略的工作流管理系统访问控制模型[J]. 系统工程理论与实践, 2009, 29(2): 151-158.
YU L, CHEN B, XIAO J M. The access control model of multiple strategies workflow management system[J]. Systems Engineering-theory & Practice, 2009, 29(2): 151-158.

[28] BONEH D, FRANKLIN M. Identity-Based encryption from the Weil pairing[A]. 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2001)[C]. Santa Barbara , Berlin, GER, 2001. 213-229.

作者简介：

陈波（1972-），男，江苏南通人，博士，南京师范大学副教授，主要研究方向为移动安全、密码技术及应用、网络与信息安全。

于泠（1971-），女，江苏金坛人，博士，南京师范大学副教授，主要研究方向为网络与信息安全、密码技术及应用。

强小辉（1990-），男，江苏扬州人，南京师范大学硕士生，主要研究方向为移动安全。

王岩（1966-），男，黑龙江哈尔滨人，博士，澳大利亚麦考瑞大学副教授，主要研究方向为可信计算、安全电子商务。