Journal of Computer Applications
计算机应用,2013,33(11):3235-3238
ISSN 1001-9081
CODEN JYIIDU
2013-11-01
http://www.joca.cn

文章编号:1001-9081(2013)11-3235-04
doi:10.11772/j.issn.1001-9081.2013.11.3235

基于身份的受控文档透明加解密方案

金 彪[1],熊金波[1*],姚志强[1],刘西蒙[2]
(1.福建师范大学 软件学院,福州 350108; 2.西安电子科技大学 通信工程学院,西安 710071)
(*通信作者电子邮箱 jinbo810@163.com)

摘 要:针对日益严峻的文档安全形势,为了更好地保护受控文档,将基于身份的加密机制与透明加密(OTFE)技术相结合,提出基于身份的受控文档透明加解密方案。采用文件系统过滤驱动技术监控程序对受控文档的操作,并使用基于身份的加密机制执行加解密操作。特别地,提出将原始密文耦合后分块存储的新算法,使得敌手不可能获取完整密文进而恢复出原始明文。从系统层面和算法层面对方案进行了详细描述,安全分析表明该方案能有效地保护受控文档。

关键词:受控文档;基于身份的加密;透明加密;文档安全;访问控制
中图分类号:TP309.2 **文献标志码**:A

Identity-based on-the-fly encryption and decryption scheme for controlled documents

JIN Biao[1], XIONG Jinbo[1*], YAO Zhiqiang[1], LIU Ximeng[2]
(1. *Faculty of Software, Fujian Normal University, Fuzhou Fujian* 350108, *China*;
2. *School of Telecommunication Engineering, Xidian University, Xi'an Shaanxi* 710071, *China*)

Abstract: To deal with the increasingly serious situation of document's security and better protect the controlled documents, in this paper, an identity-based On-The-Fly Encryption (OTFE) and decryption scheme was proposed for the controlled documents, which combined an Identity-Based Encryption (IBE) algorithm with an on-the-fly encryption technique. In the scheme, file system filter driver technology was used to monitor program's behaviors on the controlled documents; meanwhile, the IBE algorithm was used to encrypt and decrypt the controlled documents. Specifically, a new algorithm that associated the original ciphertext and divided the associated ciphertext into two parts stored in different locations was proposed. Therefore, it is impossible for an adversary to obtain the whole ciphertext and further recover the original plaintext. Finally, an elaborate description was made on the scheme from system level and algorithm level. The security analysis indicates that the proposed scheme is able to effectively protect the controlled documents.

Key words: controlled document; identity-based encryption; On-The-Fly Encryption (OTFE); document security; access control

0 引言

随着政府、企业信息化建设的推进,信息安全形势也日益严峻。如何在不影响员工正常工作的前提下,保护企业或商业隐私,确保商业信息及数据使用过程的安全,是企业亟须解决的问题。企业相关文档可划分为受控文档和非受控文档。所谓受控文档,是指文档管理部门想控制且能控制的文档;反之,非受控文档指的是文档管理部门不想控制、不能控制或不必控制的文档。如何保护受控文档的安全是本文的研究重点。

透明加密(On-The-Fly Encryption, OTFE)技术[1]是近年来针对企业文件保密需求应运而生的一种与 Windows 紧密结合的文件加密技术,工作于 Windows 底层。OTFE 通过监控应用程序对文件的操作,执行加密或者解密操作。整个加解密过程无需任何人工干预,不会被文档使用者察觉,符合不影响员工正常工作的要求。

透明加密的实现技术主要有加密文件系统(Encrypting File System, EFS)[2]、钩子(Hook)加密技术[3]、磁盘加密系统[4]和文件系统过滤驱动[5-7]。这些技术的工作原理不尽相同:加密文件系统和文件系统过滤驱动技术均工作在系统的内核层,利用文件驱动监控程序对文件的操作;钩子加密技术工作在系统的应用层,使用 Windows 的钩子技术监控程序对文件的操作;磁盘加解密系统则直接对磁盘数据进行加解密,忽视文件等存储数据的逻辑概念。文献[1]基于安全操作系统 SecLinux 设计实现了透明加解密文件系统,整个系统由文件服务器、客户端和文件密码服务器三部分组成;文献[2]在第 12 章对 Windows 所支持的文件系统作了详细的介绍和比较;文献[3]对常用的 Hook 技术进行分析,举例说明不同 Hook 技术的不同应用场合;文献[4]提出了一种数据加密的硬件解决方案,指出磁盘加密系统应该具备数据加解密、密码算法可更换/升级以及可存放密钥/证书/其他必须数据等功能;文献[5-7]提出了一种基于文件系统过滤器的加密方法,数据加解密操作在操作系统内核态执行,整个过程对用户透明。为了增强加密系统的安全性,文献[6]使用智能卡作

收稿日期:2013-05-24;**修回日期**:2013-07-22。 **基金项目**:国家自然科学基金资助项目(61370078);福建省自然科学基金资助项目(2011J01339);福建省教育厅科研基金资助项目(JA12078,JB12022)。

作者简介:金彪(1985-),男,安徽六安人,硕士,主要研究方向:文档安全; 熊金波(1981-),男,湖南益阳人,讲师,博士研究生,CCF 会员,主要研究方向:内容安全、隐私保护; 姚志强(1967-),男,福建莆田人,教授,博士研究生,CCF 高级会员,主要研究方向:信息安全; 刘西蒙(1988-),男,陕西西安人,博士研究生,主要研究方向:密码学。

为加解密密钥的存储器。这些研究成果表明,文件系统过滤驱动技术能够在满足操作透明性的同时,保证高效的执行效率,更适用于监控程序对文件的操作行为。

然而,上述文献的研究工作均存在不足之处,主要体现在:1)加解密过程与身份认证相独立(用户的身份认证和访问控制等在用户态完成),虽然操作方便,但是在发生文档泄密时无法查找泄密源(因为密文中未包含用户信息);2)当加密文档不慎外传后,敌手将得到完整的密文,他们可以通过密码分析等传统攻击手段破解获得明文;3)密钥管理不方便,且存在安全隐患(例如文献[1]将所有文件密码的统一存放在一台服务器上)。

基于身份的加密(Identity-Based Encryption, IBE)[8]机制因可从加解密密钥中验证用户信息以及密钥管理方便等优点,是上述问题的有效解决途径。本文将基于身份的加密技术与透明加密技术相结合,提出基于身份的受控文档透明加解密方案,能够保护企业网络中的受控文档存储与访问安全。最后对方案的可行性和安全性进行了论证。

1 相关基础

1.1 透明加密基础

通过监控程序对文件的操作,自动执行文件加解密的实现技术主要包括加密文件系统、钩子加密技术、磁盘加密系统和文件系统过滤驱动。表1对4种实现技术的工作原理作了简单介绍,并对它们的优缺点进行分析。

表1 4种实现技术介绍与比较

实现技术	工作原理	优缺点分析
钩子加密技术	1)基于钩子技术:利用Windows的钩子技术,监控应用程序对文件的打开、保存等操作,执行加解密操作; 2)工作与操作系统应用层	1)与应用程序密切相关,随监控应用程序的启动而启动,一旦应用程序名更改,则无法挂钩;2)运行在Windows应用层,易被发现,安全性较差
加密文件系统	1)基于文件系统驱动技术:文件系统驱动是把文件作为一种设备来处理的一种虚拟驱动,文件驱动监控程序对文件读写操作,对需要保护的数据就进行加密或者解密工作; 2)工作在操作系统的内核层,对上层应用透明	1)与应用程序无关; 2)工作在操作系统的内核层,运行速度更快,加解密操作更稳定; 3)必须与NTFS结合使用,不支持其他文件系统格式如FAT32,通用性差; 4)涉及到Windows底层的诸多处理,开发难度很大
文件系统过滤驱动	同加密文件系统工作原理的1)和2)	同加密文件系统优缺点分析中的1)、2)、4); 此外,与操作系统的内核联系紧密,特别是内存和高速缓存管理器,使系统对磁盘的访问更有效率
磁盘加解密系统	不考虑文件等存储数据的逻辑概念,直接对磁盘数据进行加解密	难以实现对指定的文件或目录进行加密隐藏以及权限控制等操作

传统加解密系统运行在操作系统的用户态,如常用的WinRAR、Word、Excel文档,访问文件时用户须手动输入密码或显示进行加解密操作,这种方式使用极其不便,并且数据在使用过程存在明文落地(明文内容存储在磁盘上),这样很容易造成机密信息的失密和泄露,此外该方式无法对机密信息的使用进行权限控制以及对数据使用行为的跟踪记录[8]。为了达到"透明"效果,即整个加解密过程无需文档使用者人工干预且不易被其察觉,必须采用透明加密技术,在系统内核态自动执行加解密操作。

透明加密技术具有强制加密(所有指定类型或属于某一(些)安全级别的文档都将被强制加密)、使用方便(加解密过程无需用户干预,不影响用户原有的操作习惯)、于内无碍(加密文档在内部仍可正常共享和使用)和对外受阻(文档离开限定范围后,将因为无法解密而自动失效)四个重要特性。图1为透明加密技术的具体流程。

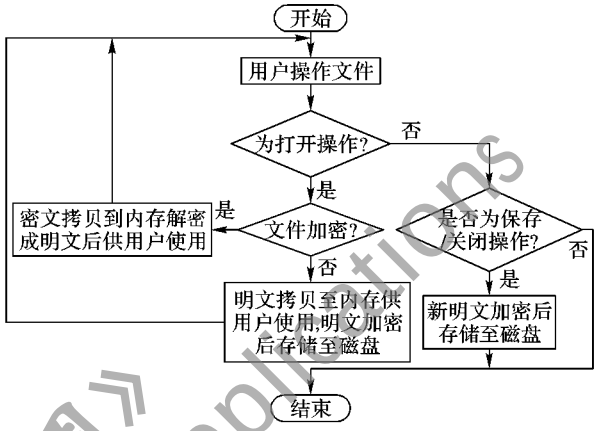

图1 透明加密流程

鉴于上述分析,本文在设计受控文档透明加解密方案时,使用文件系统过滤驱动技术来监控程序对受控文档的操作。

1.2 IBE基础

IBE是一类典型的公钥密码方案,与公钥基础设施(Public Key Infrastructure, PKI)的公/私钥对随机产生不同,IBE的公/私钥对是基于身份信息计算出来的。目前已有不同类型的IBE方案,如由Boneh等[9]提出第一个实用且可证明安全的基于Weil Pairing的IBE方案,此后,由RFC(Request For Comments)于2007年发布正式的IBE标准[10]而备受学术界和产业界关注。

在IBE方案[9]587-588,[10]34-35中,用于计算用户公钥的是用户独特的身份标识符,包含公开知道的身份信息,如通常将Email地址、手机号码等作为IBE身份标识符。用户的私钥则由可信第三方的密钥产生中心(Key Generation Center, KGC)利用用户公钥等信息计算得到。值得注意的是,在计算用户公钥时,除利用用户独特的身份标志外,通常还结合KGC产生的完全公开的IBE系统参数(明文空间、密文空间、密码函数等)。IBE系统参数可以指定不同的IBE算法、密文空间长度和密钥强度。

文献[11]证明了基于身份的密码学(Identity-Based Cryptography, IBC)在中断容错网络(Disruption-Tolerant Networking, DTN)中的适用性;文献[12]提出了一种适用于传感器的轻量级IBE(IBE-Lite),在此基础上开发适用于身体传感器网络(Body Sensor Network, BSN)的协议。

2 方案设计

为了方便方案描述,如图2所示本文将用户划分成可信用户和不可信用户。局域网内已有用户为可信用户,新用户进入局域网后需经过管理员审核方可成为可信用户,可信用户离开局域网即变成不可信用户。

2.1 方案假设前提

假设前提如下:

1) KGC 以及下文即将提到的 KPCS(Keep Part of Ciphertext Server)仅能够被局域网内计算机访问。为了降低受控文档被泄密的风险,KGC 与 KPCS 不提供对外访问服务。

2)KGC 以及 KPCS 由专业的可信人员负责管理。KGC 与 KPCS 是整个方案的核心,除了保证 KGC 与 KPCS 本身正常运作之外,还必须保证存储在 KGC 与 KPCS 上数据的安全。为此,企业必须指派专业管理员管理和维护 KGC 与 KPCS。

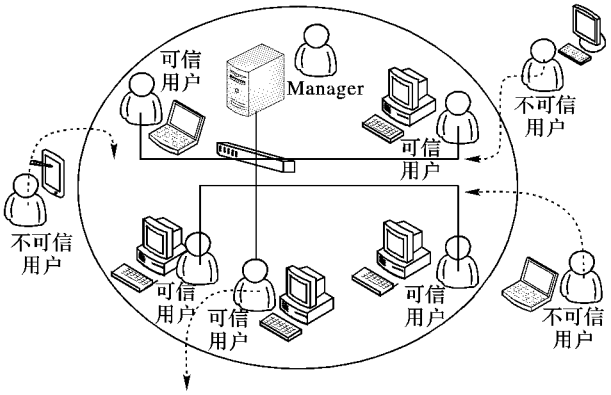

图2　用户划分

2.2　受控文档加解密方案描述

本节将从系统级和算法级两个层面对方案进行描述。

2.2.1　系统级描述

图3为本方案的系统模型。其中 KGC 中存储的内容包括局域网内可信计算机的 ID 列表 *PIDList*、主私钥 x 和主公钥 $y = g^x$,使用 EAC(Extracting After Coupling)算法处理原始密文。

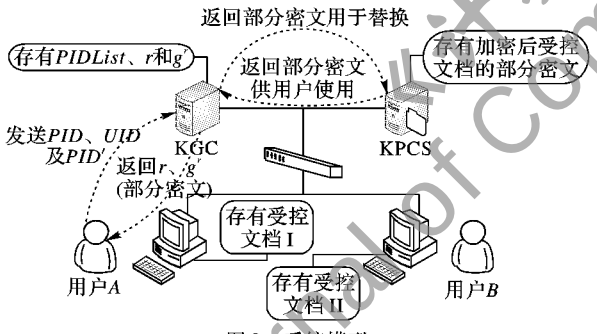

图3　系统模型

受控文档加解密方案具体描述如下。

步骤1　企业管理者(或相关授权人员)将所有受控文档依据访问操作权限分发到相应可信用户的计算机。

步骤2　可信用户(经企业管理者审核认证通过)计算机相关程序对受控文档进行预处理。预处理操作包括:1)获取 *PID*(计算机 ID)和 *UID*(用户 ID);2)组合 *PID* 和 *UID* 成唯一 ID,参与求解 r 和 g^r,求得 IBE 加密密钥 *key*;3)用 *key* 对受控文档进行加密;4)使用 EAC 算法处理原始密文 *Ct* 得到 *Ct'*,将部分密文 Ct'_{p1} 存放至 KPCS,其余密文 Ct'_{p2} 仍存储在可信用户计算机;5)将 *PID* 和 *UID* 追加到 Ct'_{p2} 头部。经过上述处理后的受控文档的组成形式可用图4表示。

PID+*UID*	Ct'_{p2}(本机存储)	Ct'_{p1}(KPCS存储)

图4　受控文档组成

步骤3　利用文件系统过滤驱动技术监控用户操作文件的行为,重点关注两种情形:Case1 和 Case2。

Case1　用户 *A* 试图打开受控文档,计算机发送指令(组成部分(*PID_A*,*UID_A*,*PID'*))至KGC。其中,*PID_A* 和 *UID_A* 从计算机直接自动获取,*PID'* 从受控文档中自动获取。KGC 判断 *PID_A* 是否存在于 *PIDList* 中,存在即表示 *A* 为可信用户,执行步骤4;否则提示 *A* 无权操作该文件,流程结束。

Case2　用户 *A* 试图关闭或者保存文档(意味着 *A* 为可信用户;否则他无法打开文件),计算机发送指令(组成部分(*PID_A*,*UID_A*,*PID'*))至KGC。KGC 将 r、和 g^r 返回给 *A*,*A* 用户计算机上监控程序将分别计算 *SIE*(Shared Information in Encryption)和 *AES*(*SIE*),得到 IBE 加密密钥,将文档加密成密文后,使用 EAC 算法抽取部分密文 Ct'_{p1} 经 KGC 存放到 KPCS,并替换 KPCS 中原有的 Ct'_{p1},其余密文 Ct'_{p2} 本机存储。

步骤4　KGC 分析指令,判断 *PID_A* 和 *PID'* 是否相同:*PID_A* ≡ *PID'*(用户 *A* 为文档的原始拥有者),KGC 将 r、g^r 以及 KPCS 中该文档的 Ct'_{p1} 返回给 *A*,*A* 用户计算机上监控程序将分别计算 *SID*(Shared Information in Decryption)和 *AES*(*SID*),得到 IBE 解密密钥 *key*,将内存中的密文 Ct'_{p2} 以及 Ct'_{p1} 组成完整密文 *Ct'*,利用 EAC 算法求得原始密文 *Ct* 后解密成明文;*PID_A* ≠ *PID'*(用户 *A* 不是文档的原始拥有者,不妨假设文档来自用户 *B*),此时 KGC 依据 *B* 用户的 *PID_B* 和 *UID_B* 计算并返回 r、g 以及 KPCS 中该文档的 Ct'_{p1} 给 *A*,*A* 用户计算机上监控程序将分别计算 *SID* 和 *AES*(*SID*),得到解密密钥 *key*。

2.2.2　算法级描述

为了能在受控文档泄密时查找出泄密当事人并加大敌手破解密文的难度,本文引入 IBE 机制并提出了密文处理算法 EAC。

1)IBE 机制。

给定安全参数 κ,系统初始化算法 setup(k) 产生耦合密文分量个数 v、每个分量的 bit 数为 u、每次提取 u 中的 *et* bit、对称密钥算法 *SE*(如 AES)、具有大素数阶 q 的 2 个有限域群 G_1(G_1 的生成元为 g)和 G_2、一个双线性配对函数 $e: G_1 \times G_1 \rightarrow G_2$、一个 Hash 函数 $H: \{0,1\}^* \rightarrow G_1$ 和一个密钥推导函数 *KDF*(Key Derivation Function):$G_3 \rightarrow \{0,1\}^l$,其中 l 是加密算法 *SE* 中对称密钥的长度,则系统参数 $params = (v,u,et,g,e,SE,H,KDF)$。KGC 初始化产生主密钥 $x(x \in \mathbf{Z}_q)$ 和主公钥 $(g, y = g^x) \in G_1^2$,其中:x 由 KGC 秘密保存,$(g, y = g^x)$ 公开。

加密过程可描述为:用户 *A* 将自己的 ID 发送给数据 *data* 拥有者 *B*,*B* 计算得到临时(伪)私钥 r,进而计算得到临时(伪)公钥 $z = g^r$(r 由 *B* 保存,$z = g^r$ 公布给用户 *A*)。*B* 计算 *SIE*,$SIE = KDF(e(H(ID)^r, y))$,并将 *SIE* 作为对称密钥算法 AES 的输入,$AES(SIE) \rightarrow key$。最后 *B* 利用 *key* 对数据 *data* 加密成 *data'* 后发送给 *A*。

由上述加密过程可知,*A* 将得到 $z = g^r$ 和 *data'*,解密过程可描述为:*A* 将自己的 ID 发送给 KGC,KGC 认证 *A* 后返回 $KID(KID = H(ID)^x \in G_1)$ 给 *A*。*A* 利用 *KID* 和 $z = g^r$ 利用式(1)计算 *SID*,并将 *SID* 作为 *AES* 输入,$AES(SID) \rightarrow key$。分析 *SID* 可知,*SID* 与加密过程中得到的 *SIE* 相等,因此 *A* 计算得到的 *key* 与 *B* 加密 *data* 所用的 *key* 相同,可解密 *data'* 得到 *data*。

$$SID = KDF(e(KID,z)) = KDF(e(H(ID)^x, g^r)) = KDF(e(H(ID)^r, g^x)) = KDF(e(H(ID)^r, y)) \quad (1)$$

2)EAC 算法。

EAC 算法由三个子算法构成:Convert($params$,Ct) → Ct'、$Extract(params,Ct')\rightarrow(Ct'_{p1},Ct'_{p2})$ 和 Recover($params$,Ct') →Ct。

①Convert($params$,Ct) → Ct'。

给定原始密文 Ct 和系统参数 $params$,算法首先将 Ct 等分成大小为 u bit 的块,若最后一块不足 u bit 则补 0[13]。假设共有 v 块,则 $Ct=(Ct_1,\cdots,Ct_i,\cdots,Ct_v)$,然后,算法按式(2)耦合各密文块:

$$\begin{cases} Ct_1' = Ct_1 \oplus H(Ct_2,\cdots,Ct_i,\cdots,Ct_v) \\ Ct_2' = Ct_2 \oplus H(Ct_1',Ct_3\cdots,Ct_i,\cdots,Ct_v) \\ \vdots \\ Ct_i' = Ct_i \oplus H(Ct_1',\cdots,Ct_{i-1}',Ct_{i+1},\cdots,Ct_v) \\ \vdots \\ Ct_v' = Ct_v \oplus H(Ct_1',\cdots,Ct_i',\cdots,Ct_{v-1}') \end{cases} \tag{2}$$

最后,耦合后的密文即为 $Ct'=(Ct_1',\cdots,Ct_i',\cdots,Ct_v')$。

②Extract($params$,Ct') → (Ct'_{p1},Ct'_{p2})。

Ct' 由 v 个 u bit 块构成,依据参数 et 将 Ct' 中每个块都划分成 Ct'_{p1} 和 Ct'_{p2} 两部分。其中,Ct'_{p1} 由[1,et] 构成,Ct'_{p2} 由[et + 1,u] 构成。为了节省服务器存储资源,设定 $1 < et < u/2$。

③Recover($params$,Ct') → Ct。

给定耦合密文 Ct' 和系统参数 $params$,算法利用式(3)可以恢复出原始密文 Ct,执行如下:

$$\begin{cases} Ct_v = Ct_v' \oplus H(Ct_1',\cdots,Ct_i',\cdots,Ct_{v-1}') \\ Ct_{v-1} = Ct_{v-1}' \oplus H(Ct_1',\cdots,Ct_i',\cdots,Ct_{v-2}',Ct_v') \\ \vdots \\ Ct_i = Ct_i' \oplus H(Ct_1',\cdots,Ct_{i-1}',Ct_{i+1},\cdots,Ct_v) \\ \vdots \\ Ct_1 = Ct_1' \oplus H(Ct_2,\cdots,Ct_i,\cdots,Ct_v) \end{cases} \tag{3}$$

3 安全性分析

本方案实施过程无需任何特殊设备,只需要局域网内计算机与服务器(KGC 和 KPCS)可相互通信即可。更重要的是,本方案的安全性较文献[2-7]有明显增强,如表 2 所示。原因主要有:1)后者的工作重点在于加解密过程的透明,没有考虑密文本身的安全;2)本方案引入 IBE 机制,除可在发生文档泄密时查找泄密当事者之外,IBE 本身的安全性也已被文献[9]所证明;3)采用本方案,当受控文档因某些原因离开限定使用环境后,它将因无法得到自动解密服务(无法访问 KGC)而无法被解密,进而达到文档保密效果;4)采用本方案,即便受控文档离开限定使用环境后,由于密文不完整(部分密文存储在 KPCS 中),仍可以抵抗密码分析等攻击。

表 2 方案比较

方案	侧重点	加密算法本身安全性	文档泄密后能否查找当事人	文档泄密后能否抵抗密码分析攻击
文献[2-7]	加密过程透明	未保证	不能(加密过程不涉及身份认证)	不能(可以获得完整密文)
本文方案	加密过程透明以及加密算法	IBE 本身安全已被证明	能(加密密钥中包含身份信息)	能(无法获得完整密文)

4 结语

为了有效地保护企业的受控文档,本文提出了一种融合 OTFE 和 IBE 的受控文档透明加解密方案,提出 EAC 算法实现密文耦合后的分块存储以增加敌手通过密文分析等攻击手段破解密文的难度。分析表明,该方案具有可行性和有效性,即使在文档不慎离开使用环境的情况下,也能有效地防止文档信息泄密。方案中对同一计算机上的所有受控文档均以相同密钥进行加密和解密操作,后续研究将引入多级安全的思想[14-15],依据受控文档各内容敏感程度的不同对其划分安全等级,不同安全等级的文档内容使用不同的密钥进行加解密,并授予不同安全等级的用户访问和处理,实现对受控文档的细粒度访问控制。

参考文献:

[1] 魏丕会,卿斯汉,刘海峰. 基于安全操作系统的透明加密文件系统的设计[J]. 计算机科学,2003,30(7):134-137.

[2] RUSSINOVICH M E, SOLOMON D A. Microsoft Windows Internals: Microsoft Windows Server 2003, Windows XP, and Windows 2000 [M]. Washington, DC: Microsoft Press, 2005: 775-785.

[3] 邱建雄. Hook 技术及其在软件开发中的应用[J]. 国防科技大学学报,2002,24(1):77-80.

[4] 游林儒,毕岩明,毕淑娥. 硬盘加密系统在信息安全中的应用[J]. 计算机应用,2002,22(8):43-45.

[5] 邵昱,萧蕴诗. 基于文件系统过滤驱动器的加密软件设计[J]. 计算机应用,2005,25(5):79-83.

[6] 郑磊,马兆丰,顾明. 基于文件系统过滤驱动的安全增强型加密系统技术研究[J]. 小型微型计算机系统,2007,28(7):1181-1184.

[7] 张汉宁,房鼎益,陈晓江,等. 基于透明加解密的数字内容安全防护系统[J]. 西北大学学报,2010,40(3):67-71.

[8] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// CRYPTO'84: Proceedings of CRYPTO 84 on Advances in Cryptology. Berlin: Springer-Verlag, 1985: 47-53.

[9] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[10] BOYEN X, MARTIN L. Identity-Based Cryptography Standard (IBCS) #1: supersingular curve implementations of the BF and BB1 cryptosystems, RFC 5091 [EB/OL]. [2013-04-20]. http://tools.ietf.org/html/rfc5091.

[11] ASOKAN N, KOSTIAINEN K, GINZBOORG P, *et al*. Applicability of identity-based cryptography for disruption-tolerant networking [C]// Proceedings of the 1st International MobiSys Workshop on Mobile Opportunistic Networking. New York: ACM Press, 2007: 52-56.

[12] TAN C C, WANG H, ZHONG S, *et al*. Body sensor network security: an identity-based cryptography approach [C]// Proceedings of the First ACM Conference on Wireless Network Security. New York: ACM Press, 2008: 148-153.

[13] WANG G J, YUE F S, LIU Q. A secure self-destructing scheme for electronic data [J]. Journal of Computer and System Sciences, 2013, 79(2): 279-290.

[14] 熊金波,姚志强,马建峰,等. 视频数据库多级访问控制[J]. 通信学报,2012,33(8):147-154.

[15] 熊金波,姚志强,马建峰,等. 基于行为的结构化文档多级访问控制[J]. 计算机研究与发展,2013,50(7):1399-1408.