



(12) 发明专利

(10) 授权公告号 CN 102567230 B

(45) 授权公告日 2014. 11. 26

(21) 申请号 201010620416. 5

US 2010023747 A1, 2010. 01. 28, 全文 .

(22) 申请日 2010. 12. 23

审查员 吴海旋

(73) 专利权人 普天信息技术研究院有限公司

地址 100080 北京市海淀区海淀北二街 6 号

(72) 发明人 龚平 窦永金 常莹 刘金鹏

(74) 专利代理机构 北京德琦知识产权代理有限公司

公司 11018

代理人 王一斌 王琦

(51) Int. Cl.

G06F 12/14 (2006. 01)

(56) 对比文件

US 6351813 B1, 2002. 02. 26, 全文 .

CN 1395180 A, 2003. 02. 05, 全文 .

CN 1501263 A, 2004. 06. 02, 全文 .

CN 1567255 A, 2005. 01. 19, 全文 .

CN 101520854 A, 2009. 09. 02, 全文 .

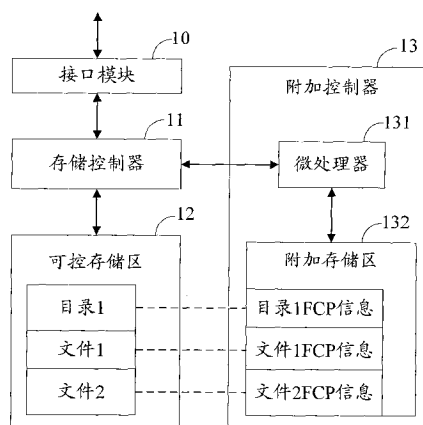
权利要求书3页 说明书8页 附图3页

(54) 发明名称

一种智能存储卡及其安全管理的方法

(57) 摘要

本发明提供了一种智能存储卡,该存储卡包含接口模块、可控存储区、存储控制器和附加控制器;附加控制器根据建立 FCP 信息指令,以名称为索引建立目录 FCP 信息和文件 FCP 信息;根据待处理文件的名称获取其 FCP 信息,解析待处理文件的 FCP 信息获得安全条件及安全算法;根据权限验证指令判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,输出安全保护后的数据至存储控制器;确定不满足安全条件,拒绝进行操作。本发明还提供了一种智能存储卡安全管理的方法。采用本发明的存储卡和方法,能够提高安全性和灵活性。



1. 一种智能存储卡,其特征在于,该存储卡包括:

接口模块,将外部输入的建立文件控制参数 FCP 信息指令输出至存储控制器;将外部输入的操作指令及权限验证指令输出至存储控制器;所述 FCP 信息至少包含文件名称、安全算法及安全条件;

可控存储区,用于保存目录及所述目录下的文件;

存储控制器,将所述建立 FCP 信息指令输出至附加控制器;将所述操作指令携带的待处理文件的名称及所述权限验证指令输出至附加控制器;根据操作指令对附加控制器输出的安全保护后的数据进行处理;

附加控制器,根据所述建立 FCP 信息指令,以名称为索引建立与所述可控存储区保存的目录一一对应的目录 FCP 信息,以名称为索引建立与所述可控存储区保存的文件一一对应的文件 FCP 信息;根据所述待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;根据权限验证指令判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,输出安全保护后的数据至所述存储控制器;确定不满足安全条件,拒绝进行操作。

2. 根据权利要求 1 所述的存储卡,其特征在于,所述 FCP 信息进一步包含一生命周期;

所述附加控制器进一步解析所述待处理文件的 FCP 信息获得生命周期,并判断是否满足生命周期的要求,确定满足之后,根据权限验证指令判断是否满足安全条件;确定不满足生命周期,拒绝进行操作。

3. 根据权利要求 2 所述的存储卡,其特征在于,所述 FCP 信息进一步包含一安全条件的逻辑组合;

所述附加控制器进一步根据所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

4. 根据权利要求 3 所述的存储卡,其特征在于,所述附加控制器包括:

微处理器,根据所述存储控制器输出的所述建立 FCP 信息指令,在附加存储区中以名称为索引保存与所述可控存储区的目录一一对应的目录 FCP 信息,在附加存储区中以名称为索引保存与所述可控存储区的文件一一对应的文件 FCP 信息;根据操作指令携带的待处理文件的名称从附加存储区中读取待处理文件的 FCP 信息,解析所述待处理文件的 FCP 信息获得生命周期、安全条件及安全算法;判断是否满足生命周期的要求,确定满足生命周期后,根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件,确定满足安全条件后,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,输出安全保护后的数据至所述存储控制器;确定不满足生命周期或不满足安全条件时,拒绝操作;

附加存储区,用于保存所述目录 FCP 信息及所述文件 FCP 信息。

5. 根据权利要求 4 所述的存储卡,其特征在于,所述附加存储区进一步用于保存安全算法所需的密钥和 / 或口令。

6. 一种智能存储卡,其特征在于,该存储卡包括:

接口模块,将外部输入的建立文件控制参数 FCP 信息的指令、权限验证指令及操作指令输出至存储控制器;所述 FCP 信息至少包含文件名称、安全条件及安全算法;

存储器,用于保存目录、所述目录下的文件、与所述目录一一对应的目录 FCP 信息及与所述目录下的文件一一对应的文件 FCP 信息;

存储控制器,根据所述建立 FCP 信息指令,在存储器中以名称为索引建立与保存的所述目录一一对应的目录 FCP 信息,在存储器中以名称为索引建立与保存的所述文件一一对应的文件 FCP 信息;根据所述操作指令携带的待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;根据所述权限验证指令判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,根据所述操作指令对安全保护后的数据进行处理;确定不满足安全条件,拒绝进行操作。

7. 根据权利要求 6 所述的存储卡,其特征在于,所述 FCP 信息进一步包含一生命周期;所述存储控制器进一步解析所述待处理文件的 FCP 信息获取生命周期,并判断是否满足生命周期的要求,确定满足之后,根据权限验证指令判断是否满足安全条件;确定不满足生命周期,拒绝进行操作。

8. 根据权利要求 6 或 7 所述的存储卡,其特征在于,所述 FCP 信息进一步包含一安全条件的逻辑组合;

所述存储控制器进一步根据权限验证指令及所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

9. 根据权利要求 8 所述的存储卡,其特征在于,所述存储器包括:

可控存储区,用于保存目录及所述目录下的文件;

附加存储区,用于保存与所述可控存储区的所述目录一一对应的目录 FCP 信息,用于保存与所述可控存储区的所述目录下的文件一一对应的文件 FCP 信息。

10. 根据权利要求 8 所述的存储卡,其特征在于,所述存储器进一步用于保存安全算法所需的密钥和 / 或口令。

11. 一种智能存储卡安全管理的方法,其特征在于,该方法包括:

A、在附加存储区建立以名称进行索引的与可控存储区保存的目录一一对应的目录文件控制参数 FCP 信息、及以名称进行索引的与可控存储区保存的文件一一对应的文件 FCP 信息;所述 FCP 信息至少包含文件名称、安全条件及安全算法;

B、根据外部输入的操作指令携带的待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;

C、根据外部输入的权限验证指令,判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护获得安全保护后的数据,根据所述操作指令对安全保护后的数据进行处理;在确定不满足安全条件时,拒绝进行操作。

12. 根据权利要求 11 所述的方法,其特征在于,所述 FCP 信息进一步包含一生命周期;所述步骤 B 与所述步骤 C 之间进一步包括:解析所述待处理文件的 FCP 信息获得生命周期,在确定满足生命周期后,执行步骤 C,否则拒绝进行操作。

13. 根据权利要求 11 或 12 所述的方法,其特征在于,所述 FCP 信息进一步包含一安全条件的逻辑组合;

所述步骤 B 进一步包括:根据所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

14. 根据权利要求 13 所述的方法,其特征在于,步骤 A 所述与可控存储区保存的文件一一对应的文件 FCP 信息为:所述文件 FCP 信息与所述目录 FCP 信息在附加存储区中构成

的文件结构,与所述文件 FCP 信息对应的文件和所述目录 FCP 信息对应的目录在可控存储区中构成的文件结构相同。

15. 根据权利要求 13 所述的方法,其特征在于,所述安全算法至少包含加密算法和校验,或者所述安全算法至少包含解密算法和校验;

步骤 C 所述利用安全算法,对待处理文件的数据进行保护包括:

C1、利用加密算法对待处理文件包含的数据进行加密,或利用解密算法对待处理文件包含的数据进行解密;

C2、对加密后获得的数据或解密后获得的数据的完整性进行校验,将加密后的数据及校验值作为安全保护后的数据,或将解密后的数据及校验值作为安全保护后的数据。

16. 根据权利要求 13 所述的方法,其特征在于,步骤 A 所述在附加存储区建立以名称进行索引的与可控存储区保存的文件一一对应的文件 FCP 信息之前,进一步包括:为所述可控存储区中所述目录下保存的文件添加一文件名称;所述文件名称的长度为 M 字节;所述 M 为小于 256 的自然数。

一种智能存储卡及其安全管理的方法

技术领域

[0001] 本发明涉及存储技术,特别涉及一种智能存储卡及其安全管理的方法。

背景技术

[0002] 智能存储卡 (Smart Storage Card, SSC) 将传统的智能卡技术和超大容量存储器技术结合起来,利用多种通信和计算机接口,装载在移动通信终端、计算机、以及其他数码终端设备内,提供大容量存储、新型的无线增值应用、多媒体处理、信息安全、DRM 等多种功能的智能化信息,多媒体、娱乐等产品。

[0003] 由于智能存储卡内的数据多为用户或发行商的重要数据,如何实现安全的数据存储、通信及特定区域操作指令的安全将是智能存储卡必须解决的重要问题。

[0004] 公开号为 CN101520854A 的发明专利提出了包含存储介质和 USB 接口模块的智能存储卡、及实现智能存储卡与访问设备 (PC) 间安全访问的方法,存储介质的存储空间划分为机密数据区和海量存储区;机密存储区使用 ISO7816-4 标准的文件系统,其为可对文件进行权限控制的区域;USB 接口模块用于将机密数据区和海量存储区所覆盖的不同扇区与访问智能存储卡的设备 (PC 机) 的存储扇区进行映射;访问智能存储卡的设备上的机密数据操作模块通过智能存储卡的 USB 接口模块,来对智能存储卡上的机密存储区内的文件进行安全管理。由于访问智能存储卡的设备对智能存储卡进行安全管理,安全性较低;且机密数据区采用固定的文件结构,权限管理以扇区为单位,较易被物理或软件截获破解,存在较高的安全风险;该发明专利中的安全逻辑较为固定、简单,不能进行灵活设置,还有待进一步改进。

发明内容

[0005] 有鉴于此,本发明的目的在于提供一种智能存储卡,该存储卡能够提高安全性和灵活性。

[0006] 本发明的目的在于提供一种智能存储卡安全管理的方法,该方法能够提高安全性和灵活性。

[0007] 为达到上述目的,本发明的技术方案具体是这样实现的:

[0008] 一种智能存储卡,该存储卡包括:

[0009] 接口模块,将外部输入的建立文件控制参数 FCP 信息指令输出至存储控制器;将外部输入的操作指令及权限验证指令输出至存储控制器;所述 FCP 信息至少包含文件名称、安全算法及安全条件;

[0010] 可控存储区,用于保存目录及所述目录下的文件;

[0011] 存储控制器,将所述建立 FCP 信息指令输出至附加控制器;将所述操作指令携带的待处理文件的名称及所述权限验证指令输出至附加控制器;根据操作指令对附加控制器输出的安全保护后的数据进行处理;

[0012] 附加控制器,根据所述建立 FCP 信息指令,以名称为索引建立与所述可控存储区

保存的目录一一对应的目录 FCP 信息,以名称为索引建立与所述可控存储区保存的文件一一对应的文件 FCP 信息;根据所述待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;根据权限验证指令判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,输出安全保护后的数据至所述存储控制器;确定不满足安全条件,拒绝进行操作。

[0013] 较佳地,所述 FCP 信息进一步包含一生命周期;

[0014] 所述附加控制器进一步解析所述待处理文件的 FCP 信息获得生命周期,并判断是否满足生命周期的要求,确定满足之后,根据权限验证指令判断是否满足安全条件;确定不满足生命周期,拒绝进行操作。

[0015] 较佳地,所述 FCP 信息进一步包含一安全条件的逻辑组合;

[0016] 所述附加控制器进一步根据所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

[0017] 上述存储卡中,所述附加控制器包括:

[0018] 微处理器,根据所述存储控制器输出的所述建立 FCP 信息指令,在附加存储区中以名称为索引保存与所述可控存储区的目录一一对应的目录 FCP 信息,在附加存储区中以名称为索引保存与所述可控存储区的文件一一对应的文件 FCP 信息;根据操作指令携带的待处理文件的名称从附加存储区中读取待处理文件的 FCP 信息,解析所述待处理文件的 FCP 信息获得生命周期、安全条件及安全算法;判断是否满足生命周期的要求,确定满足生命周期后,根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件,确定满足安全条件后,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,输出安全保护后的数据至所述存储控制器;确定不满足生命周期或不满足安全条件时,拒绝操作;

[0019] 附加存储区,用于保存所述目录 FCP 信息及所述文件 FCP 信息。

[0020] 较佳地,所述附加存储区进一步用于保存安全算法所需的密钥和 / 或口令。

[0021] 一种智能存储卡,该存储卡包括:

[0022] 接口模块,将外部输入的建立文件控制参数 FCP 信息的指令、权限验证指令及操作指令输出至存储控制器;所述 FCP 信息至少包含文件名称、安全条件及安全算法;

[0023] 存储器,用于保存目录、所述目录下的文件、与所述目录一一对应的目录 FCP 信息及与所述目录下的文件一一对应的文件 FCP 信息;

[0024] 存储控制器,根据所述建立 FCP 信息指令,在存储器中以名称为索引建立与保存的所述目录一一对应的目录 FCP 信息,在存储器中以名称为索引建立与保存的所述文件一一对应的文件 FCP 信息;根据所述操作指令携带的待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;根据所述权限验证指令判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护,获得安全保护后的数据,根据所述操作指令对安全保护后的数据进行处理;确定不满足安全条件,拒绝进行操作。

[0025] 较佳地,所述 FCP 信息进一步包含一生命周期;

[0026] 所述存储控制器进一步解析所述待处理文件的 FCP 信息获取生命周期,并判断是否满足生命周期的要求,确定满足之后,根据权限验证指令判断是否满足安全条件;确定不

满足生命周期,拒绝进行操作。

[0027] 较佳地,所述 FCP 信息进一步包含一安全条件的逻辑组合;

[0028] 所述存储控制器进一步根据权限验证指令及所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

[0029] 上述存储卡中,所述存储器包括:

[0030] 可控存储区,用于保存目录及所述目录下的文件;

[0031] 附加存储区,用于保存与所述可控存储区的所述目录一一对应的目录 FCP 信息,用于保存与所述可控存储区的所述目录下的文件一一对应的文件 FCP 信息。

[0032] 较佳地,所述存储器进一步用于保存安全算法所需的密钥和 / 或口令。

[0033] 一种智能存储卡安全管理的方法,该方法包括:

[0034] A、在附加存储区建立以名称进行索引的与可控存储区保存的目录一一对应的目录文件控制参数 FCP 信息、及以名称进行索引的与可控存储区保存的文件一一对应的文件 FCP 信息;所述 FCP 信息至少包含文件名称、安全条件及安全算法;

[0035] B、根据外部输入的操作指令携带的待处理文件的名称获取其 FCP 信息,解析所述待处理文件的 FCP 信息获得安全条件及安全算法;

[0036] C、根据外部输入的权限验证指令,判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护获得安全保护后的数据,根据所述操作指令对安全保护后的数据进行处理;在确定不满足安全条件时,拒绝进行操作。

[0037] 较佳地,所述 FCP 信息进一步包含一生命周期;

[0038] 所述步骤 B 与所述步骤 C 之间进一步包括:解析所述待处理文件的 FCP 信息获得生命周期,在确定满足生命周期后,执行步骤 C,否则拒绝进行操作。

[0039] 较佳地,所述 FCP 信息进一步包含一安全条件的逻辑组合;

[0040] 所述步骤 B 进一步包括:根据所述 FCP 信息包含的安全条件的逻辑组合判断是否满足安全条件。

[0041] 上述方法中,步骤 A 所述与可控存储区保存的文件一一对应的文件 FCP 信息为:所述文件 FCP 信息与所述目录 FCP 信息在附加存储区中构成的文件结构,与所述文件 FCP 信息对应的文件和所述目录 FCP 信息对应的目录在可控存储区中构成的文件结构相同。

[0042] 上述方法中,所述安全算法至少包含加密算法和校验,或者所述安全算法至少包含解密算法和校验;

[0043] 步骤 C 所述利用安全算法,对待处理文件的数据进行保护包括:

[0044] C1、利用加密算法对待处理文件包含的数据进行加密,或利用解密算法对待处理文件包含的数据进行解密;

[0045] C2、对加密后获得的数据或解密后获得的数据的完整性进行校验,将加密后的数据及校验值作为安全保护后的数据,或将解密后的数据及校验值作为安全保护后的数据。

[0046] 较佳地,步骤 A 所述在附加存储区建立以名称进行索引的与可控存储区保存的文件一一对应的文件 FCP 信息之前,进一步包括:为所述可控存储区中所述目录下保存的文件添加一文件名称;所述文件名称的长度为 M 字节;所述 M 为小于 256 的自然数。

[0047] 由上述的技术方案可见,本发明提供了一种智能存储卡及其安全管理的方法,智能存储卡根据建立 FCP 信息及设置的 FCP 信息,在智能存储卡内建立目录 FCP 信息及文件

FCP 信息,智能存储卡在建立 FCP 信息时,根据目录及文件在可控存储区内保存时形成的文件结构,在附加存储区内建立相同文件结构的目录 FCP 信息及文件 FCP 信息;根据待处理的文件获取其 FCP 信息,根据安全条件及其逻辑组合,确定满足安全条件时,利用安全算法对待处理的数据进行保护,获得安全保护后的数据,根据操作指令对安全保护后的数据进行处理。采用本发明的存储卡及方法,对可控存储区内的文件进行操作时,对其操作指令进行安全控制,通过安全条件及其逻辑组合实现对数据的安全保护,提高了安全性和灵活性。

附图说明

[0048] 图 1 为本发明智能存储卡第一实施例的结构示意图。

[0049] 图 2 为本发明智能存储卡第二实施例的结构示意图。

[0050] 图 3 为本发明智能存储卡安全管理的方法的流程图。

具体实施方式

[0051] 为使本发明的目的、技术方案、及优点更加清楚明白,以下参照附图并举实施例,对本发明进一步详细说明。

[0052] 本发明的智能存储卡及智能存储卡安全管理的方法不再以扇区为单位进行安全管理,而是以文件为单位进行管理,且由智能存储卡内的存储控制器或附加控制器实现对可控存储区内保存的文件进行安全管理,提高了安全性;可根据用户对于某一文件的具体需求,对该文件的 FCP 信息包含的安全条件和安全算法进行设置,提高了灵活性。

[0053] 本发明的 FCP 信息是参照 IS07816-4 标准中所描述的结构进行定义的,但本发明的 FCP 信息还进一步对 IS07816-4 标准进行了扩展,在 FCP 信息中增加了可设置成任意字节长度的文件名称,进一步便于实现以文件为单位进行安全管理。

[0054] 图 1 为本发明智能存储卡第一实施例的结构示意图。现结合图 1,对本发明智能存储卡的第一实施例进行说明,具体如下:

[0055] 本发明智能存储卡包括:接口模块 10、存储控制器 11、可控存储区 12 和附加控制器 13。其中,接口模块 10 一端连接存储控制器 11,另一端连接访问智能存储卡的外部设备;存储控制器 11 连接可控存储区 12 和附加控制器 13。

[0056] 接口模块 10 提供存储控制器 11 与访问智能存储卡的外部设备之间的通讯通道。接口模块 10 将外部输入的建立文件控制参数 (FCP) 信息指令输出至存储控制器 11。其中,建立 FCP 信息指令携带有待建立 FCP 信息的目录名称及设置的 FCP 信息,或携带有待建立 FCP 信息的文件名称及设置的 FCP 信息;所述设置的 FCP 信息至少包括文件名称和安全属性;所述安全属性至少包括安全条件和安全算法;所述安全属性可设置为紧凑模式、扩展模式、参考扩展模式或上述多种模式的组合。为了提高安全性,所述安全属性还可进一步包括一生命周期和 / 或安全条件的逻辑组合。

[0057] 接口模块 10 将外部输入的操作指令及权限验证指令输出至存储控制器 11。其中,操作指令包括读数据指令或写数据指令;操作指令还进一步携带有待处理的文件的名称;待处理文件的名称可为待处理的目录的名称或待处理数据所属的文件的名称。权限验证指令还携带有此次操作的验证参数。

[0058] 可控存储区 12 用于保存多个目录及所述每一目录下的多个文件。可控存储区 12

保存的目录及文件是需要进行安全保护的内容。比如：目录 1 包含文件 1 和文件 2，目录 2 包含文件 3 和文件 4。

[0059] 存储控制器 11 将建立 FCP 信息指令输出至附加控制器 13。存储控制器 11 将操作指令携带的待处理文件的名称及权限验证指令输出至附加控制器 13。存储控制器 11 根据操作指令对附加控制器 13 输出的安全保护后的数据进行处理，向接口模块 10 反馈处理结果及处理后的数据。本实施例中，存储控制器 11 不对可控存储区 12 保存的文件或目录进行安全管理，仅根据操作指令对附加控制器 13 输出的安全保护后的数据执行读取或写入操作。

[0060] 附加控制器 13 根据建立 FCP 信息指令，以名称为索引建立与可控存储区 12 保存的目录一一对应的目录 FCP 信息，以名称为索引建立与可控存储区 12 保存的文件一一对应的文件 FCP 信息；具体地，附加控制器 13 可通过与存储控制器 11 的通讯，通过存储控制器 11 获取可控存储区 12 的文件结构，及可控存储区 12 保存的目录及目录下的文件。上述一一对应的关系体现在由文件和目录组成的文件结构上，即文件 FCP 信息和目录 FCP 信息在附加控制器 13 中形成的文件结构，与文件 FCP 信息对应的文件和目录 FCP 信息对应的目录在可控存储区 12 中形成的文件结构相同。

[0061] 附加控制器 13 根据待处理的文件的名称，从已建立的 FCP 信息中查找待处理的文件的 FCP 信息；解析待处理文件的 FCP 信息获得生命周期、安全条件、安全条件的逻辑组合及安全算法；判断是否满足生命周期，如果满足生命周期，根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件，在确定满足安全条件时，利用安全算法对待处理文件包含的数据进行保护获得安全保护后的数据，输出安全保护后的数据至存储控制器 11；在确定不满足生命周期或安全条件时，拒绝此次操作。生命周期为一有效期，判断是否满足生命周期也就是判断对待处理文件的操作是否处于有效期内，如果是，则进行安全条件的判断，否则，拒绝此次操作。附加控制器 13 还进一步保存用于进行安全算法的密钥和 / 或口令。比如：解析文件 1 的 FCP 信息获得安全条件为 PIN 码，安全算法为加密算法和校验，则判断权限验证指令携带的验证参数是否与 PIN 码相同，如果相同，则满足安全条件，利用保存的密钥对待处理的数据进行加密运算，对加密运算后的数据进行完整性校验，输出安全保护后的数据或校验值至存储控制器 11；确定权限验证指令携带的验证参数与 PIN 码不相同，则确定不满足安全条件，拒绝此次操作。

[0062] 其中，附加控制器 13 包括微处理器 131 和附加存储区 132。微处理器 131 连接存储控制器 11 和附加存储区 132。

[0063] 附加存储区 132 用于保存目录 FCP 信息及文件 FCP 信息。附加存储区 132 进一步用于保存安全算法所需的密钥和 / 或口令。

[0064] 微处理器 131 根据存储控制器 11 输出的建立 FCP 信息指令，在附加存储区 132 中以名称为索引保存与可控存储区 12 的目录一一对应的目录 FCP 信息，在附加存储区 132 中以名称为索引保存与可控存储区 12 的文件一一对应的文件 FCP 信息；根据操作指令携带的待处理文件的名称，从附加存储区 132 中读取待处理文件的 FCP 信息，解析待处理文件的 FCP 信息获得生命周期、安全条件、安全条件的逻辑组合及安全算法；判断是否满足生命周期的要求，确定满足生命周期后，根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件，在确定满足安全条件后，利用安全算法对待处理文件包含的数据进行保护获得

安全保护后的数据,输出安全保护后的数据至存储控制器 11;确定不满足生命周期或不满足安全条件时,拒绝操作。

[0065] 图 2 为本发明智能存储卡第二实施例的结构示意图。现结合图 2,对本发明智能存储卡的第二实施例进行说明,具体如下:

[0066] 本发明智能存储卡第二实施例与第一实施例相比,缺少了用于进行文件安全管理的附加控制器,第二实施例中的存储控制器实现第一实施例中附加控制器的功能,该实施例的智能存储降低了硬件成本。

[0067] 本发明智能存储卡包括接口模块 20、存储控制器 21 和存储器 22。接口模块 20 一端连接存储控制器 21,另一端连接访问智能存储卡的外部设备;存储控制器 21 连接存储器 22。

[0068] 本实施例的接口模块 20 与第一实施例的接口模块 10 相同,在此不再对接口模块 20 进行说明。

[0069] 存储器 22 用于保存目录、目录下的文件、与所述目录一一对应的目录 FCP 信息及与所述目录下的文件一一对应的文件 FCP 信息。存储器 22 还进一步保存用于进行安全算法的密钥和 / 或口令。目录 FCP 信息及文件 FCP 信息的内容与实施例一的内容相同,在此不再赘述。

[0070] 存储控制器 21 根据建立 FCP 信息指令,从存储器 22 中获取其保存的目录及目录下的文件,根据 FCP 信息指令携带的设置的 FCP 信息,在存储器中以名称为索引建立与保存的所述目录一一对应的目录 FCP 信息、及与保存的所述文件一一对应的文件 FCP 信息,换句话说,文件 FCP 信息和目录 FCP 信息在存储器 22 形成的文件结构与文件 FCP 信息对应的文件和目录 FCP 信息对应的目录在存储器 22 形成的文件结构相同。

[0071] 存储控制器 21 根据操作指令携带的待处理的文件的名称,从已建立的 FCP 信息中查找待处理的文件的 FCP 信息;解析所述 FCP 信息获得对于待处理文件的生命周期、安全条件、安全算法及安全条件的逻辑组合。存储控制器 21 判断是否满足生命周期,在确定满足生命周期之后,根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件,在确定满足安全条件时,利用安全算法对待处理文件包含的数据进行保护获得安全保护后的数据,按照操作指令对安全保护后的数据进行处理;在确定不满足生命周期或不满足安全条件时,拒绝此次操作。

[0072] 存储控制器 21 进一步向接口模块 20 反馈处理结果及处理后的数据;所述处理结果为拒绝操作的结果或完成操作的结果;所述处理后的数据为安全保护后的数据或完整性校验值。

[0073] 其中,存储器 22 包括:可控存储区 221 和附加存储区 222。

[0074] 可控存储区 221 用于保存多个目录及每一目录下的多个文件。可控存储区 221 中保存的目录和文件是用以进行安全保护的文件。

[0075] 附加存储区 222 用于保存目录 FCP 信息及文件 FCP 信息。

[0076] 附加存储区 222 保存的目录 FCP 信息及文件 FCP 信息形成的文件结构与可控存储区 221 保存的目录及目录下的文件形成的文件结构相同。

[0077] 图 3 为本发明智能存储卡安全管理的方法的流程图。现结合图 3,对本发明智能存储卡安全管理的方法进行说明,具体如下:

[0078] 步骤 301 :建立以名称进行索引的 FCP 信息 ;

[0079] 该步骤包括 :步骤 3011,根据可控存储区保存的目录添加目录名称,根据可控存储区保存的文件添加文件名称 ;步骤 3012,根据建立 FCP 信息指令携带的设置的 FCP 信息及目录名称,在附加存储区中建立以目录名称进行索引的与可控存储区中的目录一一对应的目录 FCP 信息 ;步骤 3013,根据建立 FCP 信息指令携带的设置的 FCP 信息及文件名称,在附加存储区中建立以文件名称进行索引的与可控存储区中的文件一一对应的文件 FCP 信息。

[0080] 步骤 3011 中,根据可控存储区保存的文件添加文件名称的长度和具体内容可根据用户的需求进行设置,不再局限于 ISO7816-4 中规定的固定字节长度的名称,可将文件名称设置为 M 个字节 ;所述 M 为小于 256 的自然数。

[0081] 该步骤中,附加存储区保存的目录 FCP 信息及文件 FCP 信息形成的文件结构与可控存储区保存的目录及文件形成的文件结构相同,在此不再赘述。

[0082] 步骤 302 :获取待处理文件的 FCP 信息 ;

[0083] 根据操作指令中携带的待处理文件的名称,从附加存储区中保存的 FCP 信息查找待处理文件的 FCP 信息。

[0084] 步骤 303 :解析 FCP 信息获得安全条件、安全条件的逻辑组合及安全算法 ;

[0085] 智能存储卡内负责对文件进行安全管理的控制器,比如存储控制器或附加控制器,对待处理文件的 FCP 信息进行解析,获得与待处理文件相关的安全条件、安全条件的逻辑及安全算法。

[0086] 步骤 304 :判断是否满足安全条件,如果是,执行步骤 305,否则执行步骤 307 ;

[0087] 该步骤中,若未设置安全条件的逻辑组合,则直接根据权限验证指令判断是否满足安全条件 ;若设置了安全条件的逻辑组合,则根据权限验证指令及安全条件的逻辑组合判断是否满足安全条件。

[0088] 本发明所述的安全条件还进一步携带有用以判定是否满足安全条件的参数,比如 :安全条件可为 PIN 码验证、身份验证、外部认证、内部认证、多重认证等等,则根据输入的 PIN 码、身份验证码、外部认证码、内部认证码、多重认证码等等来确定是否与安全条件携带的参数相同,如果是,则确定满足安全条件,否则确定不满足安全条件。

[0089] 步骤 305 :利用安全算法对待处理文件进行保护 ;

[0090] 所述安全算法至少包含加密算法和校验,或者所述安全算法至少包含解密算法和校验。

[0091] 以安全算法包括加密算法和校验为例,该步骤包括 :利用加密算法及保存的密钥,对待处理文件进行加密 ;对加密后获得的数据进行数据完整性校验,将加密后的数据及校验值作为安全保护后的数据。

[0092] 以安全算法包括解密算法和校验为例,该步骤包括 :利用解密算法及保存的密钥,对待处理文件进行解密 ;对解密后获得的数据进行数据完整性校验,将解密后的数据及校验值作为安全保护后的数据。

[0093] 步骤 306 :根据操作指令对安全保护后的数据进行处理 ;

[0094] 所述操作指令包括读取指令或写入指令 ;根据接收到的操作指令,对步骤 305 获得的安全保护后的数据进行读取或写入操作。

[0095] 步骤 307 :结束。

[0096] 为了进一步提高安全性,FCP 信息进一步包括生命周期;生命周期是用以判定对某一文件的操作是否有效的参数。

[0097] 在步骤 303 和步骤 304 之间进一步包括:根据待处理文件的 FCP 信息包含的生命周期,判断是否满足生命周期,如果是,执行步骤 304,否则执行步骤 307。

[0098] 本发明的上述较佳实施例中,不再由访问智能存储卡的外部设备对智能存储卡内的数据进行安全管理,而是由智能存储卡根据预先设置的 FCP 信息,对可控存储区中保存的文件进行安全管理,不易被物理或软件破解,提高了安全性;本发明的智能存储卡及安全管理方法,不再以扇区作为权限管理的基本单位,而是由不同文件系统下的文件作为安全管理的基本单元,比如:FAT(File Allocation Table) 文件系统下的文件、NTFS(New Technology File System) 文件系统下的文件或 EXT(Extended File System) 文件系统下的文件,但并不局限于上述三种文件系统下的文件。本发明的智能存储卡及安全管理方法可根据用户对特定文件的安全性要求设置 FCP 信息,提高了灵活性;为了便于以文件为基本单位进行安全管理,本发明附加存储区内保存的目录 FCP 信息和文件 FCP 信息形成的文件结构与可控存储区内保存的目录及文件形成的文件结构相同。

[0099] 以上所述仅为本发明的较佳实施例而已,并不用于限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明保护的范围之内。

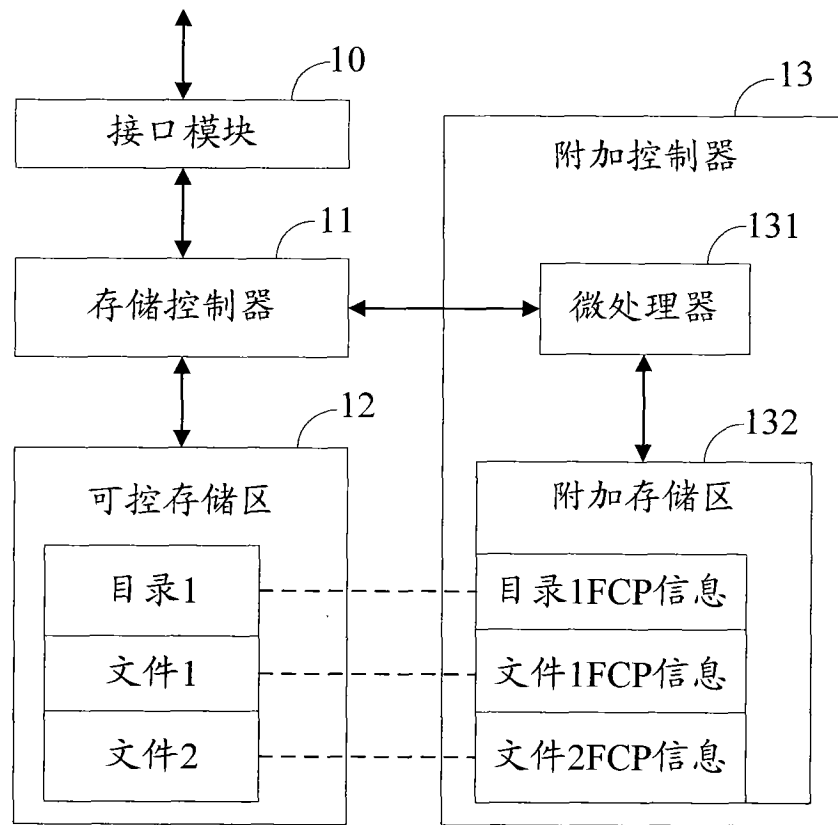


图 1

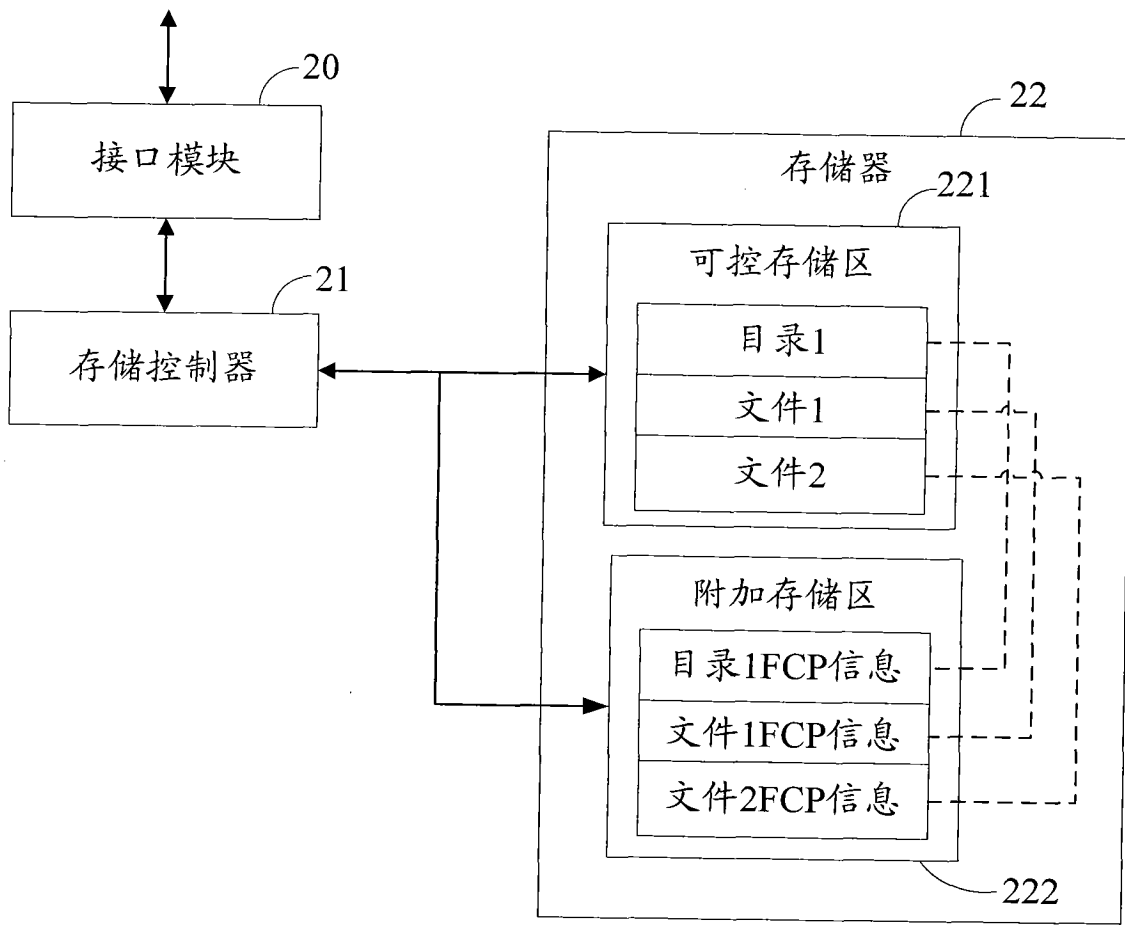


图 2

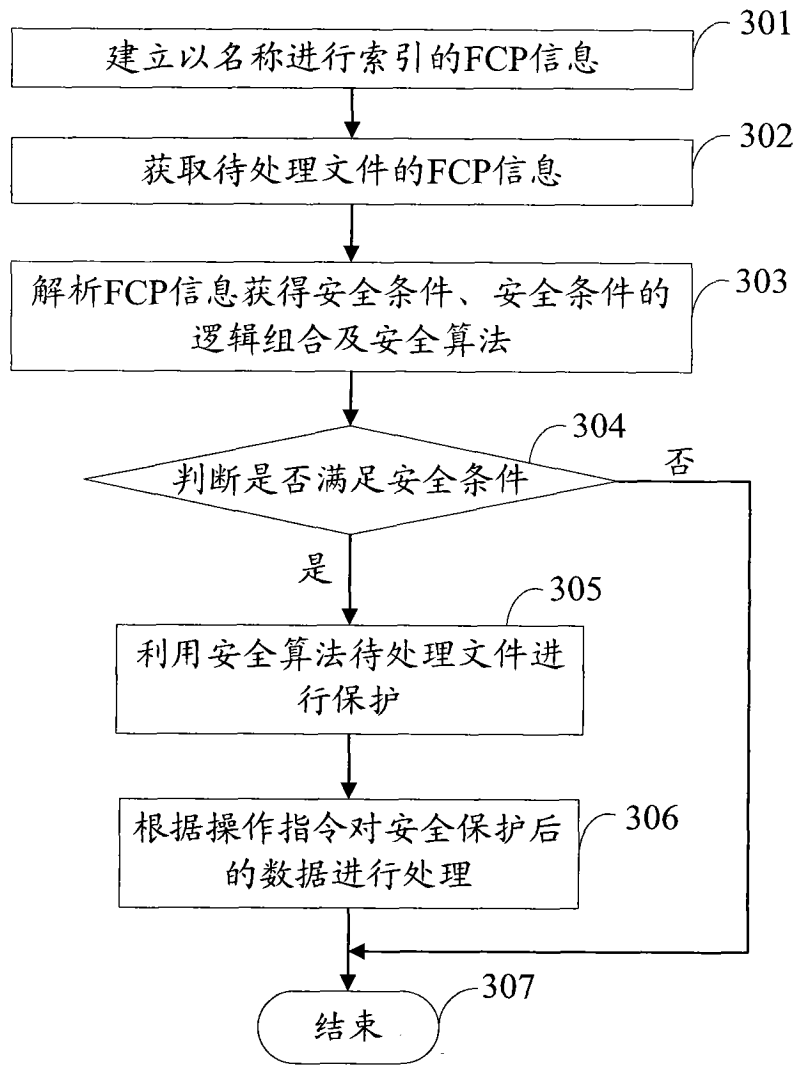


图 3