



(12) 发明专利

(10) 授权公告号 CN 101971187 B

(45) 授权公告日 2015.02.25

(21) 申请号 200980107426.4

G07F 7/10(2006.01)

(22) 申请日 2009.03.02

G06K 19/073(2006.01)

(30) 优先权数据

102008012231.9 2008.03.03 DE

(56) 对比文件

(85) PCT国际申请进入国家阶段日

2010.09.02

WO 2007048649 A1, 2007.05.03, 说明书第
0002段, 0019-0028段、说明书附图1.

(86) PCT国际申请的申请数据

PCT/EP2009/052446 2009.03.02

US 2006124756 A1, 2006.06.15, 全文.

(87) PCT国际申请的公布数据

W02009/109543 DE 2009.09.11

CN 1983338 A, 2007.06.20, 全文.

任侠等. ARP 协议欺骗原理分析与抵御方

法. 《计算机工程》. 2003, 第 29 卷 (第 9 期),

审查员 张雯

(73) 专利权人 温科尼克斯多夫国际有限公司

地址 德国帕德博恩

(72) 发明人 A·米勒

(74) 专利代理机构 中国专利代理 (香港) 有限公司 72001

代理人 张涛 李家麟

(51) Int. Cl.

G06K 7/08(2006.01)

权利要求书2页 说明书5页 附图1页

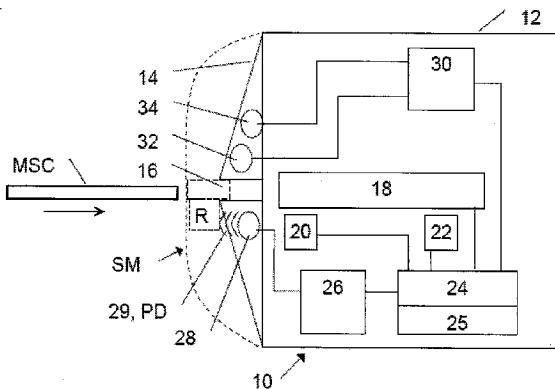
(54) 发明名称

用于防止在读卡机上窃读的保护装置和方法

(57) 摘要

在自助终端 (例如自动取款机) 上, 通过操纵以欺诈的方式安放所谓的窃读模块, 以便读取插入读卡机 (10) 中的磁条卡的数据。为了补救, 提出一种保护装置 (26, 28), 该保护装置 (26, 28) 具有用于生成电磁保护场 (29) 的保护场发生器 (26) 和与此相连接的电感 (28), 以用于妨碍侦察设备 (SM) 的功能。在此生成模拟在读出磁条卡时所出现的信号的保护信号。由此在可能存在的窃读模块中效仿磁条卡的读取。保护信号尤其是可以含有在解调时与实际卡数据混合或完全叠加于这些实际卡数据的伪数据, 使得第三者最终获得不能使用的数据。

B
CN 101971187



CN

1. 一种用于自助终端的读卡机 (10) 的保护装置 (26, 28), 用于防止借助于由第三者以欺诈意图安装在读卡机 (10) 附近的侦察设备 (SM) 来读出磁条卡 (MSC) 的数据, 其中所述保护装置具有保护场发生器 (26) 和与保护场发生器 (26) 相连接的电感 (28) 以用于生成适合于妨碍侦察设备 (SM) 的功能的电磁保护场 (29),

其特征在于,

所述保护装置 (26, 28) 生成具有保护信号的电磁保护场 (29), 该保护信号模拟在读出磁条卡时所出现的信号, 并且

所述保护场发生器 (26) 生成用伪数据 (PD) 调制的保护信号, 这些伪数据 (PD) 模拟存储在磁条卡上的数据。

2. 根据权利要求 1 的保护装置 (26, 28), 其特征在于, 所述保护场发生器 (26) 根据至少一个为在读卡机 (10) 上读出磁条卡所标准化的信号格式来生成保护信号。

3. 根据权利要求 2 的保护装置 (26, 28), 其特征在于, 所述保护场发生器 (26) 根据至少一个为在读卡机 (10) 上读出磁条卡所标准化的数据格式和 / 或数据内容来生成伪数据。

4. 根据权利要求 3 的保护装置 (26, 28), 其特征在于, 所述伪数据 (PD) 是 $f/2f$ 编码的虚构的卡数据。

5. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护场发生器 (26) 生成具有保护信号频率的保护信号, 所述保护信号频率与在磁条卡正常插入和 / 或退出读卡器时所出现的数据速率或数据速度相匹配。

6. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述伪数据 (PD) 具有同步数据。

7. 根据权利要求 6 的保护装置 (26, 28), 其特征在于, 所述同步数据是前置零和 / 或开始符号或结束符号的形式。

8. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述伪数据 (PD) 是连续的数据流。

9. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护装置 (26, 28) 生成具有如下伪数据 (PD) 的经调制的保护信号: 所述伪数据为至少两个至少部分地叠加的数据流的形式。

10. 根据权利要求 9 的保护装置 (26, 28), 其特征在于, 所述保护装置 (26, 28) 是保护场发生器 (26)。

11. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 在读卡机 (10) 上的电感 (28) 布置在磁条卡 (MSC) 的插入区域 (16) 附近, 并且所述电感 (28) 发射配备有经调制的保护信号的保护场 (29)。

12. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护装置 (26, 28) 生成具有足以影响侦察设备 (SM) 的读取传感器 (R) 的微小发射功率的电磁保护场 (29)。

13. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护装置包括用于生成保护场的电感 (28), 并且所述电感 (28) 集成在读卡机 (10) 的盖板 (14) 中。

14. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述读卡机 (10) 包括至少一个磁道读取头 (20, 22), 并且所述保护装置 (26, 28) 由读卡机 (10) 的用于控制读卡机的卡传送装置 (18) 的控制单元 (24) 控制, 使得至少在读卡机 (10) 中读取磁条卡 (MSC)

的时间段期间将电磁保护场 (29) 改变为使得读卡机 (10) 中的磁条卡 (MSC) 的读取不受保护场 (29) 妨碍。

15. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护场 (29) 的场强在读取过程期间降低或关断。

16. 根据权利要求 1 至 4 之一的保护装置 (26, 28), 其特征在于, 所述保护装置 (26, 28) 还包括适合于确定侦察设备的存在的传感系统 (30, 32, 34)。

17. 一种自助终端, 具有读卡机 (10) 并且具有用于读卡机 (10) 的用于防止借助于由第三者以欺诈意图安装在读卡机 (10) 附近的侦察设备 (SM) 来读出磁条卡 (MSC) 的数据的保护装置 (26, 28), 其中所述保护装置具有保护场发生器 (26) 和与保护场发生器 (26) 相连接的电感 (28) 以用于生成适合于妨碍侦察设备 (SM) 的功能的电磁保护场 (29),

其特征在于,

所述保护装置 (26, 28) 生成具有保护信号的电磁保护场 (29), 该保护信号模拟在读出磁条卡时所出现的信号, 并且

所述保护场发生器 (26) 生成用伪数据 (PD) 调制的保护信号, 这些伪数据 (PD) 模拟存储在磁条卡上的数据。

18. 根据权利要求 17 的自助终端, 其特征在于, 所述自助终端被构造为自动取款机、银行结单打印机和 / 或信息终端。

19. 一种通过防止借助于由第三者以欺诈意图安装在读卡机 (10) 附近的侦察设备 (SM) 读出磁条卡 (MSC) 的数据来保护配备有读卡机 (10) 的自助终端的方法, 其中通过设置在保护装置中的保护场发生器 (26) 和与保护场发生器 (26) 相连接的电感 (28) 生成适合于妨碍侦察设备 (SM) 的功能的电磁保护场,

其特征在于,

生成具有保护信号的电磁保护场 (29), 该保护信号模拟在读出磁条卡时所出现的信号, 并且

所述保护场发生器 (26) 生成用伪数据 (PD) 调制的保护信号, 这些伪数据 (PD) 模拟存储在磁条卡上的数据。

20. 根据权利要求 19 的方法, 其中所述自助终端是自动取款机、银行结单打印机和 / 或信息终端。

用于防止在读卡机上窃读的保护装置和方法

[0001] 本发明涉及一种根据权利要求 1 的前序部分的用于读卡机的保护装置。此外，本发明涉及一种装备有该保护装置的自助终端 - 尤其是自动取款机、银行结单打印机或信息终端，以及涉及一种应用于该自助终端的用于防止借助于由第三者以欺诈意图安装在读卡机附近的侦察装置来读出磁条卡的数据的方法。

[0002] 常规的自助终端 - 也简称为 SB 终端 - 在功能上常常可以作为自动取款机或银行结单打印机而遇到。为了操作，使用者或客户需要一种银行卡，该银行卡通常相当于可由读卡机读取的磁条卡，在该磁条卡上存储有包括个人的客户数据和账户数据的卡数据。可惜，在 SB 终端上有越来越多的操纵由第三者进行，以便以欺诈的方式获得卡数据。为此，在各 SB 终端上尽可能不显眼地安装专门的侦察装置，该侦察装置主要含有一个小小的外来读卡器，该外来读卡器尽可能直接安放在 SB 终端或实际读卡机的实际插入口之前。如果客户现在将他的银行卡插入 SB 终端的读卡机中，则该银行卡的磁道也由该外来的读卡器读取，由此第三者取得卡数据、尤其是客户数据和账户数据，并且使得能够制造该银行卡的非法复制品。如果除此之外，第三者成功侦察到属于银行卡的密码（所谓的 P I N），则该第三者可以用伪造的银行卡和所侦察到的 P I N 不费力地在自动取款机上提取所属账户的钱。

[0003] 用于侦察卡数据或客户信息的所述欺诈行为，在专业界也称为“窃读”或卡滥用。防止该行为或至少使该行为困难的一种可能性在于，生成一种适合于妨碍位于侦察装置中的磁卡读取头的读取功能的电磁保护场。为此，必须恰好在通常安装有侦察装置的地方、也就是直接在“真正的”或实际读卡机的插入口之前生成该保护场，或使该保护场起作用。此外，保护场必须足够强，以便确保有效地妨碍或阻断侦察装置的读取功能，并且不再能通过窃读磁条卡来读取数据。

[0004] 但是，准确地定向或定位这样的保护场以及调节该保护场的场强使得不会无意地也随同妨碍了 SB 终端的实际读卡机的读取功能，不是那么简单。例如在许多读卡机中，所谓的磁道预识别头直接位于插入口后面，借助该磁道预识别头可以确定是否已正确翻转地插入磁条卡。因此，该磁道预识别头通常位于保护场起作用的区域附近。因此可能容易发生的是，磁道预识别头在读取时受到保护场妨碍。但是，除此之外，更深地布置在读卡机内部的读取头也可能受到保护场无意地妨碍或干扰。所以在实践中，结果常常证明为困难的是：在一方面保护场的最佳定向以及足够场强与另一方面读卡机的可靠的无干扰的运行之间建立良好的平衡。

[0005] 为了克服该问题，在 DE 102005043317B3 中提出一种可以有利地在自助终端 - 尤其是自动取款机、银行结单打印机和 / 或信息终端 - 中使用的保护装置。该保护装置具有用于生成交变场形式的电磁保护场的保护场发生器和与该保护场发生器相连接的电感，该电磁保护场适合于妨碍侦察装置或窃读装置的功能，其中该保护装置被由读卡机的用于控制读卡机的卡传送装置的控制单元控制为使得保护场至少在实际读卡机中读取磁条卡的时间区间内被减小或关断，使得在实际读卡机中读取磁条卡不受保护场妨碍。因此仅仅暂时地或恰好在由实际的和“真正的”读卡器读取磁条卡时或期间，才停用保护场发生器。只要没有卡位于读卡机中，就接通保护场，并且该保护场以足够的场强起到防止潜在窃读的

作用。该解决方案虽然确保不由反窃读措施来妨碍或干扰实际的读卡过程,但是为了实现保护场的暂时关断,该解决方案与一定的成本相联系。

[0006] 因此,发明所基于的任务在于,说明一种开始时所述方式的用于生成电磁保护场的改善了的保护装置。尤其是应生成一种尽可能可以保持永久接通的保护场。此外,将提出一种装备有这种保护装置的自助终端,以及一种用于生成这种保护场的方法。

[0007] 该任务通过具有权利要求 1 所述特征的保护装置来解决。该任务还通过具有并列独立权利要求所述特征的自助终端以及方法来解决。

[0008] 因此,这里所提出的保护装置的特点在于,保护装置借助于保护场发生器生成电磁保护场,该电磁保护场具有模拟在读出磁条卡时所出现的信号的保护信号。

[0009] 因此通过保护场在可能存在的侦察装置(窃读模块)中感应出专门的保护信号,以便在那里仿效磁条卡的读出。因此,窃读读卡器读出伪磁条卡,或者至少在侦查出真正的磁条卡时明显地受到迷惑。用成功的侦察过程蒙骗第三者或窃读者,使得他首先对保护措施没有任何察觉。保护信号可以对应于至少一个为磁条卡的读出所标准化的信号格式。保护信号尤其是可以含有在解调时与实际卡数据混合或完全叠加于这些实际卡数据(capture effect, 遮蔽效应)的伪数据,使得第三者最终获得不能使用的数据。但是,该第三者可能只有当他想使用利用这些数据制备的磁条卡时才觉察到这点。

[0010] 有利的扩展方案在从属权利要求中说明。

[0011] 因此有利的是,保护场发生器生成用伪数据调制的模拟存储在磁条卡上的数据的保护信号。与此相关地有利的是,保护信号发生器根据至少一种为在读卡机上读出磁条卡所标准化的数据格式和 / 或数据内容来生成伪数据。例如可以生成 f/2f 编码的虚构的卡数据。

[0012] 还有利的是,保护场发生器生成用伪数据调制的具有如下保护信号频率的保护信号:所述保护信号频率与在磁条卡正常插入和 / 或退出读卡器时所出现的数据速率或数据速度相匹配。伪数据也可以具有尤其是前置零和 / 或开始符号或结束符号形式的同步数据。

[0013] 伪数据优选是连续的数据流。

[0014] 保护装置、尤其是保护场发生器也可以生成具有如下伪数据的经调制的保护信号:所述伪数据为至少两个至少部分地叠加的数据流的形式。

[0015] 现在,在以下的描述中参照附图借助实施例来描述本发明。

[0016] 以下的描述说明在这里所提出的防止例如对自助终端或 SB 终端的读卡机窃读的保护措施,其中根据本发明设置的保护装置防止可以借助于安装在读卡机附近的侦察装置读出所插入的磁条卡的真实的卡数据。

[0017] 唯一的图以示意图示出用于 SB 终端、在所示实施例中用于银行结单打印机或自动取款机的读卡机 10 的构造。读卡机 10 具有带有前端面盖板 14 的壳体 12,该前端面盖板 14 优选是塑料盖板。在盖板 14 中构造有槽口 16 形式的插入区域,通过该槽口 16 可以将磁条卡 - 在这里是银行卡 MSC- 插入读卡机 10 中。

[0018] 传送装置 18 直接连接在插入口 16 后面。传送装置 18 一般包括用于传送银行卡的滚柱或辊子以及驱动电机和多个用于确定银行卡在传送装置 18 中的位置的传感器。在该图的简化示图中没有示出这些细节。传送装置 18 还具有在插入银行卡之后由活门驱动

装置（未示出）所关闭的活门（未示出）。

[0019] 沿着磁条卡或银行卡 MSC 在传送装置 18 内的传送路径布置有用于读取银行卡的磁条的读取装置，其中在图 1 中示出第一读取磁头 20 和第二读取磁头 22。传送装置 18 和读取头 20 和 22 与控制单元 24 相连接，该控制单元 24 又经过接口 25 与计算机或 PC（未示出）相连接。

[0020] 在一种实施方式中，根据本发明的保护装置集成到读卡机中，其中利用该保护装置有效地防止借助于由第三者直接布置在插入口 16 之前的侦察装置 SM（在图中由虚线表示）非法地读出银行卡 MSC 的数据。保护装置包括与控制单元 24 相连接的保护场发生器 26，在该保护场发生器 26 上连接有保护场电感 28。

[0021] 该电感 28 位于插入区域或插入口 16 附近，并且向外部发射由保护场发生器 26 所生成的并且配备有经调制的保护信号的保护场 29。电磁保护场 29 被生成为使得该电磁保护场 29 具有利用伪数据 PD 所调制的保护信号，这些伪数据 PD 模拟在读出磁条卡时所使用的数据。因此，可能安放在插入口 16 附近的侦察装置 SM 的读取传感器接收具有这些伪数据 PD 的保护信号，由此又妨碍侦察装置 SM 并且尤其是设置在其中的解调级（未示出）。可以利用足以影响侦察装置 SM 的读取传感器 R 的较微小的发射功率来生成电磁保护场 29。

[0022] 因此在保护装置的运行中，由保护场发生器 26 和与其相连接的电感 28 生成这种特别适合于妨碍侦察装置 SM 的功能的电磁保护场 29，其方式是电磁保护场 29 含有作为伪磁卡信号所生成的保护信号，该保护信号尤其是具有模拟在读出磁条卡时所使用的数据的伪数据 PD。用于生成和发射保护场 29 的电感 28 例如可以集成到读卡机的盖板 14 中，其中盖板优选由塑料制成。这里所生成的具有伪数据的保护场 29 是电磁交变场。可以尤其是以连续数据流的形式永久地生成保护场 29。

[0023] 但是保护场 29 不必强制性地永久存在，而是也可以暂时关断。例如可以规定，只有当没有磁条卡位于实际的读卡机 10 中时，才存在电磁保护场 29。因此，总是只有当有必要激活保护机制时、即当使用者将他的卡 MSC 插入卡槽口 16 时，才激活保护机制。

[0024] 这里所示出的保护装置也还可以含有金属检测器 30，该金属检测器 30 同样与控制单元 24 相连接，并且在该金属检测器 30 上连接有第一电感 32 和第二电感 34。保护场电感 28、第一电感 32 和第二电感 34 优选被构造为线圈，并优选浇注到读卡机 10 的塑料盖板 14 中，并因此集成到该塑料盖板 14 中。借助于线圈 32 和 34，金属检测器 30 可以确定，是否已安装诸如所示出的窃读模块 SM 的外来读取装置。然后，与金属检测器 30 相连接的控制单元 24 可以根据所确定的状态来控制保护场发生器 26，并且因此使保护场 29 的生成与状态有关。

[0025] 例如，金属检测器 30 通过第一电感 32 在插入口 16 的区域中生成初级电磁场。该初级电磁场会与在外来读取装置或窃读模块中必然地含有的金属部件共同作用，并且在这些金属部件中生成涡流。通过初级电磁场与外来读取装置的金属部件的相互作用，生成由金属检测器 30 通过第二电感 34 所检测到的次级电磁场。以此方式可以利用金属检测器 30 确定，是否已安装外来的读取装置，例如在预先规定的持续时间内金属检测器 30 已检测到外来的金属物体时。由于金属检测和保护场的生成，客户的磁卡受到防止侦察侵犯的双重保护。

[0026] 当银行卡 MSC 插入到插入口 16 中时，借助于传感器获取该银行卡 MSC，并且由传送

装置 18 将该银行卡 MSC 传送到读卡机 12 中并且向读卡机 12 的读取装置的实的读取头 22 传送,使得可以读出银行卡 MSC 的磁条。但是在银行卡 MSC 完全被传送装置 18 获取并送入到读卡机 12 中之前,就已经可以利用也称为磁道预识别头的前面的读取头 20 确定,磁条是否处于正确的位置上,即是否已将磁条卡 MSC 以正确的取向插入到插入口 16 中。

[0027] 由于磁条的读取和银行卡通过传送装置 18 的运动互相紧密地联系并互相同步,所以由同一个控制单元 24 来控制传送装置 18 和读取头 20 和 22。现在可以利用在传送和读取控制的过程中由控制单元 24 明确地确定或考虑读取头 20 和 22 读取磁条的开始和结束的这个事实,以便使对保护场 29 的时间上的控制与读卡机 10 的读取过程同步。为此,由也控制传送装置 18 和读取装置的读取头 20 和 22 的同一个控制单元 24 来控制保护场发生器 26,而且保护场发生器 26 被控制为使得在读卡机 10 中读取银行卡期间,保护场 29 的场强降低或完全关断并在读取结束之后重新建立。由于在读卡机 10 中读取银行卡期间通过这些附加措施关断或减弱保护场 29,可以用简单和可靠的方式排除保护场 29 对在实际的读卡机 10 中进行读取的妨碍。

[0028] 总之,提出用于保护配备有读卡机的自助终端的一种保护装置、一种装备有该保护装置的 SB 终端和一种方法,以用于防止借助于侦察装置(窃读模块)读出磁条卡的数据。为此生成适合于妨碍侦察装置的功能的电磁保护场。保护场像干扰场那样对窃读模块起反作用,通过该保护场发出保护信号或干扰信号,这些保护信号或干扰信号基本上相当于在读取头中记录或扫描磁条卡时所产生的信号。由此干扰分析算法,并使通过外来人员的分析明显变难。尤其是在窃读模块中感应出专门的干扰信号,以便在卡插入或退出读卡机 10 时或在卡穿过通过式读取头(Durchzugs leser)时干扰在窃读模块处的读取头,使得不能再分析所读取的卡数据或只获得不能使用的伪数据。保护信号或干扰信号的信号形式优选以类似于典型的卡数据信号的形式呈现。这些保护信号或干扰信号可以含有例如 $f/2f$ 编码的数据。保护信号的信号频率优选相当于在基于卡传送的正常的卡读取过程中所出现的数据速率或有用数据速度。

[0029] 可以以具有前置零和开始符号或结束符号的形式生成伪数据或干扰数据。由此,窃读模块在接收该数据流时被指示,开始解释、记录或向外部的窃听设备进行传输,并且窃读模块优选同步到该干扰数据流上。与实际卡数据的数据流的同步失败。必要时,真正的卡数据与伪数据混合成不能继续利用的数据量。如果连续生成干扰数据流,则窃读者得不到可以读取不受干扰的起始条件的机会。因此必要时导致真正的卡数据和干扰数据的信号混合或数据混合。为了使对所记录的数据流的解调或解释进一步变得困难,可以生成和叠加另一干扰数据流。

[0030] 替代于集成到读卡机 10 中,根据本发明的具有保护场发生器 26 和电感 28 的保护装置 26,28 也可以独立于该读卡机 10 布置在 SB 终端上。因此以有利的方式设置,将具有保护场发生器 26 和电感 28 的保护装置布置在插入口 16 后面的 SB 终端的壁板的背面上。另外与此相对应地,还可以将具有电感 32,34 的金属检测器 30 布置在该区域中。

[0031] 附图标记列表

[0032] 10 读卡机

[0033] 12 壳体

[0034] 14 塑料盖板

- [0035] 16 插入区域或插入口
- [0036] 18 传送装置
- [0037] 20 读取磁头（前面的读取头）
- [0038] 22 读取磁头（后面的读取头）
- [0039] 24 控制单元
- [0040] 25 通向计算机（PC）的接口
- [0041] 26 保护场发生器
- [0042] 28 保护场电感
- [0043] 29 保护场（所生成的电磁场）
- [0044] 30 金属检测器
- [0045] 32 第一电感
- [0046] 34 第二电感
- [0047] SM 偷察装置（窃读模块）
- [0048] R 读取设备（窃听设备）
- [0049] PD 伪数据（通过保护场发出）
- [0050] MSC 磁条卡

