



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 99810571.6

[45] 授权公告日 2004 年 2 月 18 日

[11] 授权公告号 CN 1139050C

[22] 申请日 1999.8.30 [21] 申请号 99810571.6

[30] 优先权

[32] 1998. 9. 1 [33] EP [31] 98202915.9

[86] 国际申请 PCT/EP99/06340 1999.8.30

[87] 国际公布 WO00/13151 英 2000.3.9

[85] 进入国家阶段日期 2001.3.1

[71] 专利权人 耶德托存取公司

地址 荷兰霍夫多普

[72] 发明人 安德鲁·A·瓦杰斯

审查员 杨勤之

[74] 专利代理机构 中国国际贸易促进委员会专利商
标事务所

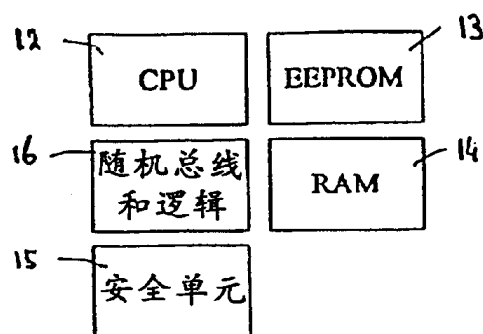
代理人 付建军

权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称 安全系统以及制造安全设备的方法

[57] 摘要

本发明公开了一种用于检验授权的安全系统，包括一些安全设备，每一个所述安全设备包括一个芯片，这个芯片中的逻辑电路具有能够提供到安全系统的授权的功能，其特征在于在至少一部分所述安全设备中，每一个安全设备的芯片具有唯一的线路图设计。



1. 一种用于检验授权的安全系统，包括多个安全设备（11），每一个所述安全设备（11）包括一个芯片，所述芯片中的逻辑电路（16）具有能够提供到安全系统的授权的功能，其特征在于，在至少几组所述安全设备中，每一个安全设备的芯片具有唯一的线路图设计。

2. 如权利要求1的安全系统，其中以FPGA的技术来实现安全设备（11）所述部分的芯片的所述逻辑电路（16），其中这个设计是可以在FPGA电路中进行编程的，编程可以在一个易失性存储器中，也可以在一个非易失性存储器中。

3. 如权利要求2的安全系统，其中每一个安全设备芯片的逻辑电路被提供在芯片的一个安全单元（15）中。

4. 如权利要求1的安全系统，其中以FPGA的技术来实现整个安全设备，其中这个设计是可以在芯片中进行编程的，编程可以在一个易失性存储器中，也可以在一个非易失性存储器中。

5. 如权利要求2，3或者4的安全系统，其中整个芯片的逻辑电路被制造为一个易失性的可编程FPGA，其中FPGA程序被保存在一个用电池供电的RAM中。

6. 如权利要求1的安全系统，其中每一个所述安全设备（11）包括一个芯片，这个芯片具有向一个安全设备（11）的所有者提供授权的功能的逻辑电路，其中在至少几组所述安全设备中，每一个安全设备的芯片具有唯一的线路图设计。

7. 如权利要求6的安全系统，其中以FPGA的技术来实现安全设备（11）所述部分的芯片的所述逻辑电路，其中这个设计是可以在FPGA电路中进行编程的，编程可以在一个易失性存储器中，也可以在一个非易失性存储器中。

8. 一种用于制造如权利要求1的安全系统中的安全设备的方法，其中使用了具有一个芯片的安全设备（11），所述芯片具有提供到安全系统的授权的功能的逻辑电路，其中在至少几组所述安全设备中，所

述安全设备的芯片是用一个唯一的线路图设计来制造的。

9. 如权利要求 8 的方法, 其中使用了 具有 FPGA 技术的逻辑电路的芯片, 所述方法包括步骤: 通过合成工具 (20) 和一个线路图设计 (22) 工具来将一个唯一的信息 (23) 编程到逻辑电路中, 其中对安全设备 (11) 的所述部分的每一个安全设备 (11), 在合成工具 (20) 和线路图设计 (22) 工具的至少一个中引入一个变化因素, 由此提供一个唯一的电路线路图设计。

10. 如权利要求 9 的方法, 其中合成工具 (20) 被提供从一个高级语言代码 (17, 18) 编译而成的输入信息, 其中在高级语言代码的编译步骤, 合成工具和线路图设计工具的至少一个中引入一个变化因素 (17)。

安全系统以及制造安全设备的方法

技术领域

本发明涉及一种用于检验授权的安全系统，该安全系统包括一些安全设备，每一个所述安全设备包括一个芯片，这个芯片中的逻辑电路具有能够提供到安全系统的授权的功能。

背景技术

上述类型的安全系统可以用于许多应用，例如禁止未经授权就进入安全房间，例如在收费电视中的应用，在银行系统中的应用，等等。所使用的安全设备一般用包括一个芯片的所谓智能卡做成。WO 95/34054 公开了一种具有一个秘钥的安全设备，其中秘钥被存储在一个独立的、硬线连接的电路。很清楚，从被提供给许多不同个人的许多智能卡来说，这个类型的安全系统是很容易受到个人或者诈骗者的攻击。目前对一个智能卡的攻击包括一个过程，这个过程中，在一个分析阶段，对这个智能卡的芯片进行探测以发现进行攻击的一个方法。在进行攻击的这个过程中，分析这个芯片的布局设计来识别能够访问被包括在这个芯片中的数据的数据的合适探测点。其后，在一个准备阶段来计划进行攻击，并且最后在实际进行攻击的阶段，读取这个芯片中的内容。虽然第一和第二步骤通常将花费几个月，但是第三步骤将在一天内就能够完成。这意味着一旦第一次破解了一个智能卡后，就能够很容易地进行第二次攻击。很清楚，这在安全系统中是一个很严重的问题。因为，一旦一个智能卡已经被识别为已经被破解，并且已经被控制系统所关闭，但是这个个人可以在一个相对较短的时间内对另一个卡进行再一次攻击，由此进行获得隐私或者进行诈骗。

另外，在现有安全系统中被使用的智能卡一般被提供了具有相同基本硅片线路设计的一个芯片，即使这些智能卡被用于不同的应用。

如果例如，当对一特定类型的智能卡进行攻击而窃取了其银行信息时，也可以使用窃取这个银行智能卡所获得的知识来用于从相同类型的智能卡中读取安全信息，即使这个智能卡是用于一个不同的应用中，例如在一个收费电视系统中。

发明内容

本发明的目的是提供上述类型的一种安全系统，其中被一个人进行攻击的脆弱性大大减小，并且其中对这个安全设备进行再一次的攻击所需要的时间被大大增加了。

为了实现这个目的，本发明提供了上述类型的一个安全系统，其特征在于在至少一部分所述安全设备中，一个安全设备的芯片具有一个唯一的芯片线路设计。

使用这个方式，可以得到这样一个安全系统，其中至少一部分安全设备，优选是全部安全设备，被提供了一个芯片，这个芯片的安全设备的电路设计是随机的。这意味着每一个安全设备的安全功能的硬件实现都是不同的。

根据本发明的一个优选实施方式，以 FPGA 的技术来实现安全设备所述部分的芯片的所述逻辑电路，其中这个设计是可以在 FPGA 电路中进行编程的，编程可以在一个易失性存储器中，也可以在一个非易失性存储器中。

本发明进一步提供了一组安全设备来用于本发明的一个安全系统，其中每一个所述安全设备包括一个芯片，这个芯片具有向一个安全设备的所有者提供授权的功能的逻辑电路，其中在至少一部分所述安全设备中，每一个安全设备的芯片具有唯一的线路图设计。

最后，本发明提供了一种方法来制造用于本发明的安全系统中的安全设备，其中使用了具有一个芯片的安全设备，所述芯片具有提供到安全系统的授权的功能的逻辑电路，其中在至少一部分所述安全设备中，一个安全设备的芯片具有一个唯一的线路图设计。

附图说明

通过参考附图，将进一步详细描述本发明，其中在附图中，示意性地显示了系统的一个实施方式和本发明的一个方法。

图 1 示意性地显示了包括本发明的一个安全系统的一个实施方式的一个收费电视系统。

图 2 示意性地显示了在图 1 系统中，被用作安全设备的一个智能卡的内部结构。

图 3 显示了本发明的这个方法的一个实施方式的一个图。

具体实施方式

图 1 通过示例仅仅显示了一个广播系统，其中 3 个广播设备 1-3 被连接到一个复用器单元 4。复用器单元 4 包括用于对广播设备 1-3 所提供的广播信号进行扰码，编码和压缩的装置，这样所获得的数字数据流被复用到一个数字传送系统中。在所显示的这个实施方式中，在进行传输前，用调制器 5 来对这个数字数据流进行调制。包括复用器单元 4 和调制器 5 的这个设备的操作员负责将这个信号传送到公众的接收设备，在图 1 所显示的示例中，是一个电视设备 6。一个或者多个广播设备 1-3 可以是根据收费电视的概念而工作的私人广播设备，收费电视隐含了订阅的过程。这意味着希望观看由一特定广播设备所广播的节目的人必须订阅这样的广播节目，并且付适当的费用。

如示意图所显示的，这个信号的传输可以通过一个或者多个电信信道来传送，包括一个卫星链路 7，陆地链路 8 或者一个电缆系统 9。

访问广播设备 1-3 所提供的任何一个广播信号需要一个解码器 10，解码器 10 通常包括没有显示的、以一个固有的方式与智能卡 11 进行合作的一个有条件的访问模块。智能卡 11 是在图 1 所显示的广播系统中实现的一个安全系统的一个安全设备，这个安全设备用于禁止没有订购这个广播的个人对收费电视进行非授权的访问。每一个用户被提供了一个智能卡 11，每一个智能卡 11 具有一个唯一的密钥和/或者地址。例如，这个安全系统可以用本质上已知的一个方式、使用 ECM

或者 EMM 来向授权用户提供对收费电视信号的访问，这个授权用户具有能够提供对安全系统进行授权访问的装置的一个智能卡 11。

如上面所解释的，这样一个安全系统能够被个人以拷贝一个原始智能卡，由此提供数量很大的盗版智能卡的方式来进行攻击。为了大大增加对一个智能卡进行再一次攻击所需要的时间，所描述的安全系统具有安全设备或者智能卡 11，每一个智能卡包括其逻辑电路具有以一个传统的方式提供到系统的授权访问的功能的一个芯片。这个逻辑电路可能包括电路来保存一个唯一的密钥，和/或者提供授权所需要的算法和逻辑，例如，对在一个安全系统中（例如 eurocrypt）所使用的密钥层结构进行解密 的算法。

图 2 以一个示意图的方式显示了一个智能卡 11 的内部结构，智能卡 11 的这个芯片包括一个中央处理单元 12，一个 EEPROM 电路 13，一个 RAM 电路 14，一个安全单元 15 和随机总线 and 逻辑电路 16。在所描述的实施方式中，仅在安全单元 15 中提供了唯一的电路线路设计图，其中例如，具有一个加密引擎和用于保存一个密钥的、易失性存储部件。关于一个智能卡的这个结构的进一步解释，可以参考相同申请人的欧洲专利申请 97202854.2。

根据一个优选实施方式，这个安全单元的实现使用的是 FPGA 技术（现场可编程门阵列）。安全单元 5 的 FPGA 电路被根据图 3 的图、以一个通常的方式来对智能卡进行个性化定制。为了使智能卡 11 个性化，唯一的信息被保存在这个安全单元中，这个唯一的信息包括一个唯一的密钥，在安全系统中所使用的一个密钥解密算法或者类似的。通常，按照如下的方法来对 FPGA 进行编程。首先，用一个高级语言，例如 C 或者 VHDL 来写用于个性化的唯一信息。首先编译高级语言。其后，这个信息被输入到一个合成工具以产生高级语言代码的一个逻辑实现。这个逻辑实现一般包括逻辑电路，例如与门，或门，D 寄存器等，这些门被组合在一起产生正确的加密功能。其后，逻辑实现被输入到一个构成一个特定 FPGA 的实际程序的一个布线程序。这个文件将规定哪一个单元在 FPGA 内被互联，并且每一个单元是如何

被编程的。然后，依据所使用的特定 FPGA 技术，实际的程序文件在加电后被载入到 FPGA 电路中，或者熔丝烧结在 FPGA 电路中。

一般，一个合成工具可以对相同的功能产生很多变化。在现有应用中，这个合成工具被设计成产生具有最小数目门的逻辑，这显示具有最佳的功率效率，具有最佳的速度性能或者上面两个的折衷。

根据本发明，一个变化因素 19，例如一个随机数，被引入到合成工具 20 中，以使合成工具 20 所提供的线路图设计可以随芯片而变化。如图 3 的图所示意性显示的，一个变化因素 19，例如一个随机数被输入到合成工具 20，并且这产生了对该变化因素产生一组唯一的逻辑的合成工具。一个新的变化因素被用于对安全系统的每一个智能卡 11 进行个性化。使用这个方法，这个安全系统的智能卡 11 的安全单元 15 具有一个唯一的逻辑电路线路图。

类似地，一个变化因素 21 可以被输入到线路图设计工具 22 中，这产生对逻辑电路的线路图设计的进一步随机化。

另外，也可以在编译步骤中引入一个变化因素，以使到合成工具 20 的输入也是一个可变的输入。所有可能的变化均可以被分别使用或者混合使用。

使用本发明的这个方法，个性化的步骤将一个唯一的密钥，密钥的逻辑实现和/或者解密功能引入到智能卡 11 中，而这将产生对每一个智能卡 11 是唯一的逻辑电路的线路图。使用这个方法，对一个安全系统的每一次攻击所需要的时间被大大增加了，以使个人不能够使用在对一第一智能卡进行攻击的一个分析阶段和一个准备阶段中所获得的信息来对另一个智能卡进行攻击。

作为一个替代的方法，不是仅在安全单元中使用 FPGA 技术，而是可以使用 FPGA 技术来制造智能卡的更多部分或者整个芯片，然后可以使用上述的方法来进行随机化。

在一个优选实施方式中，使用了一个易失性 FPGA，其中这个 FPGA 程序被保存在智能卡 11 的 RAM 14 中，它被一个电池所供电，正如安全单元 15 中的密钥的挥发性保存一样。在智能卡中包括本身已

知的保护陷阱将导致如果一个人没有成功地克服这个芯片的活力保护策略 (thew protection strategy), 芯片将导致 RAM 存储器中内容的丢失和安全单元 15 中挥发性存储器中内容的丢失。由此, FPGA 电路中的程序就丢失。使用这个方法, 通过攻击一个卡, 也不能够收集关于攻击另一个卡的任何信息。

尽管通过参考一个收费电视系统, 在上面描述了本发明, 但是, 本发明的安全系统可以在使用安全设备 11 的任何安全系统中所使用, 以对安全设备 11 的所有者提供授权, 例如用于保护房间, 建筑物, 或者类似的不被非授权进入的安全系统, 银行卡等等。另外, 尽管优选向每一个智能卡 11 提供一个唯一的线路图设计, 也能够向一组卡提供一个唯一的线路图设计。

所以, 本发明不局限于上面所描述的实施方式, 它们可以在权利要求书的范围内进行很多变化。

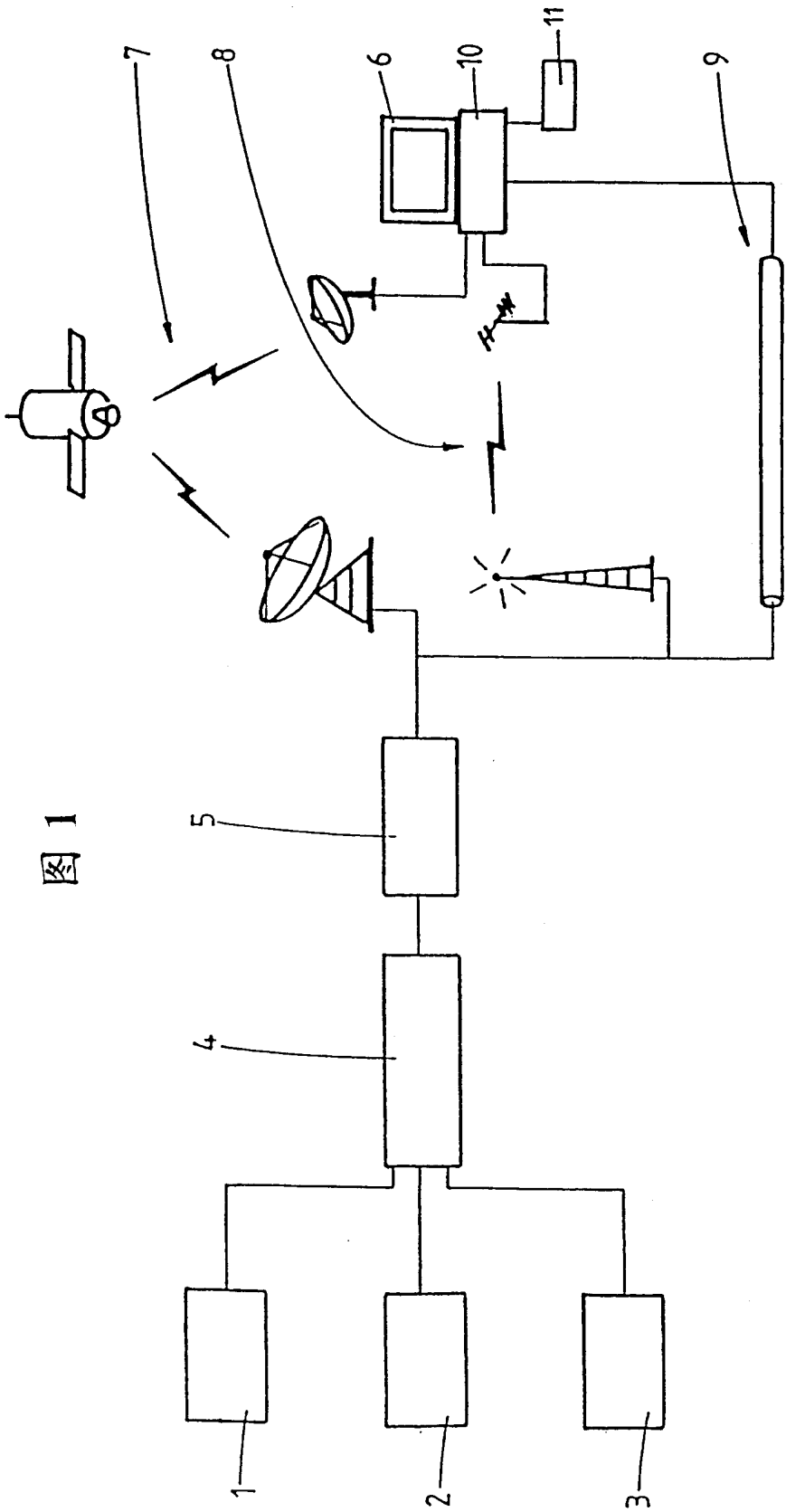


图 1

图 2

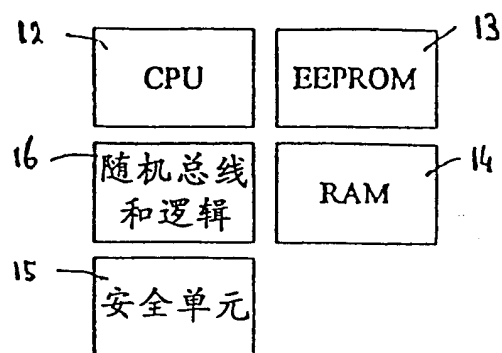


图 3

