

(12) 发明专利申请

(10) 申请公布号 CN 102236747 A

(43) 申请公布日 2011.11.09

(21) 申请号 201010153807.0

(22) 申请日 2010.04.23

(71) 申请人 北京同方微电子有限公司

地址 100083 北京市海淀区同方科技广场 A
座 2901

申请人 清大安科(北京)科技有限公司

(72) 发明人 王庆林 徐秀波 丁义民 黄金煌
王小龙

(51) Int. Cl.

G06F 21/00 (2006.01)

G06F 9/445 (2006.01)

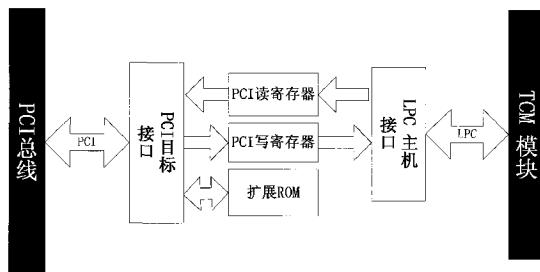
权利要求书 1 页 说明书 3 页 附图 3 页

(54) 发明名称

一种传统计算机升级为可信计算机的方法

(57) 摘要

一种传统计算机升级为可信计算机的方法，涉及信息安全技术领域。本发明的方法步骤为：
1) 将传统计算机通过主板上的PCI接口与可信计算TCM模块上的LPC接口转换电路连接访问可信计算TCM模块；2) PCI接口电路中扩展一个只读存储器ROM电路；3) 传统计算机在BIOS启动阶段运行PCI接口电路中的扩展ROM内的程序；4) 扩展ROM程序实现信任链的建立。同现有技术相比，本发明能将传统计算机升级实现可信计算，具有操作简单、节时、省力的特点。



1. 一种传统计算机升级为可信计算机的方法,其步骤为:

1) 将传统计算机通过主板上的 PCI 接口与可信计算 TCM 模块上的 LPC 接口转换电路连接访问可信计算 TCM 模块;

2) PCI 接口电路中扩展一个只读存储器 ROM 电路;

3) 传统计算机在 BIOS 启动阶段运行 PCI 接口电路中的扩展 ROM 内的程序;

4) 扩展 ROM 程序实现信任链的建立。

2. 根据权利要求 1 所述的传统计算机升级为可信计算机的方法,其特征在于,所述传统计算机主板上的 PCI 接口与可信计算 TCM 模块上的 LPC 接口转换电路之间包括 PCI 目标接口和 LPC 主机接口。

3. 根据权利要求 1 或 2 所述的传统计算机升级为可信计算机的方法,其特征在于,所述扩展 ROM 程序实现信任链建立的步骤为:

1) 传统计算机 BIOS 程序对扩展 ROM 检测正确后, BIOS 程序拷贝扩展 ROM 程序到运行空间;

2) 执行扩展 ROM 程序,扩展 ROM 程序完成信任链建立的处理;

3) 退出扩展 ROM 程序,执行 BIOS 的其他功能。

4. 根据权利要求 3 所述的传统计算机升级为可信计算机的方法,其特征在于,所述 BIOS 程序对扩展 ROM 检测方法为:

1) BIOS 启动代码,检测 PCI 设备的配置空间的扩展 ROM 基址寄存器是否存在,存在则 BIOS 将为扩展 ROM 分配一段空闲的地址空间;

2) 检测代码的前两个字节是否是 AA55;

3) 如果扩展 ROM 有效,则 BIOS 会检测代码类型,以及厂商代码和设备代码的其他信息;

4) 信息都正确后, BIOS 会将扩展 ROM 中正确的代码都拷贝到 RAM 中,这些代码就可以执行了。

5. 根据权利要求 3 所述的传统计算机升级为可信计算机的方法,其特征在于,所述扩展 ROM 程序完成信任链建立的处理方法为:

1) 启动 TCM 模块并进行初始化;

2) 将 BIOS 空间代码送给 TCM 模块进行摘要计算;

3) 将摘要计算的结果存放在 TCM 模块的 PCR 中;

4) 将摘要计算结果和存放在 TCM 模块内部非易失存储区中的正确摘要值进行比较;

5) 比较结果正确则正常启动,否则提示用户出现异常。

一种传统计算机升级为可信计算机的方法

技术领域

[0001] 本发明涉及信息安全技术领域,特别是一种传统计算机升级为可信计算机的方法。

背景技术

[0002] 近几年来,可信计算已经成为信息安全领域的一个热点,中国的可信计算现在已经越来越受到国家密码管理部门的重视,并已经上升为国家标准,众多的对安全保密要求比较高的场所对可信计算的需求越来越多。

[0003] 在原来的可信计算模块的设计中,基本都是采用低引脚数目 LPC 总线接口, LPC 总线接口是周边元件扩展 PCI 总线接口的一个子集,并满足 TIS 规范 (TPM Interface Specification)。TIS 规范是 TCG(Trust Compute Group) 提出的针对 TPM 的一种通讯规范,在我们国内的 TCM 规范中沿用了此规范。

[0004] 但是,传统计算机的主板上普遍没有预留 LPC 接口,无法连接只具备标准 LPC 接口的可信计算 TCM 模块。而如果将现有传统计算机的主板全部更换成具备 LPC 接口的主板,将耗费大量的资金、人力和时间。

发明内容

[0005] 针对上述现有技术中存在的不足,本发明的目的是提供一种传统计算机升级为可信计算机的方法。它能将传统计算机升级实现可信计算,具有操作简单、节时、省力的特点。

[0006] 为了达到上述发明目的,本发明的技术方案以如下方式实现:

[0007] 一种传统计算机升级为可信计算机的方法,其步骤为:

[0008] 1) 将传统计算机通过主板上的 PCI 接口与可信计算 TCM 模块上的 LPC 接口转换电路连接访问可信计算 TCM 模块;

[0009] 2) PCI 接口电路中扩展一个只读存储器 ROM 电路;

[0010] 3) 传统计算机在 BIOS 启动阶段运行 PCI 接口电路中的扩展 ROM 内的程序;

[0011] 4) 扩展 ROM 程序实现信任链的建立。

[0012] 在上述方法中,所述传统计算机主板上的 PCI 接口与可信计算 TCM 模块上的 LPC 接口转换电路之间包括 PCI 目标接口和 LPC 主机接口。

[0013] 在上述方法中,所述扩展 ROM 程序实现信任链建立的步骤为:

[0014] 1) 传统计算机 BIOS 程序对扩展 ROM 检测正确后, BIOS 程序拷贝扩展 ROM 程序到运行空间;

[0015] 2) 执行扩展 ROM 程序, 扩展 ROM 程序完成信任链建立的处理;

[0016] 3) 退出扩展 ROM 程序, 执行 BIOS 的其他功能。

[0017] 在上述方法中,所述 BIOS 程序对扩展 ROM 检测方法为:

[0018] 1) BIOS 启动代码, 检测 PCI 设备的配置空间的扩展 ROM 基址寄存器是否存在, 存在则 BIOS 将为扩展 ROM 分配一段空闲的地址空间;

- [0019] 2) 检测代码的前两个字节是否是 AA55；
- [0020] 3) 如果扩展 ROM 有效，则 BIOS 会检测代码类型，以及厂商代码和设备代码的其他信息；
- [0021] 4) 信息都正确后，BIOS 会将扩展 ROM 中正确的代码都拷贝到 RAM 中，这些代码就可以执行了。
- [0022] 在上述方法中，所述扩展 ROM 程序完成信任链建立的处理方法为：
- [0023] 1) 启动 TCM 模块并进行初始化；
- [0024] 2) 将 BIOS 空间代码送给 TCM 模块进行摘要计算；
- [0025] 3) 将摘要计算的结果存放在 TCM 模块的 PCR 中；
- [0026] 4) 将摘要计算结果和存放在 TCM 模块内部非易失存储区中的正确摘要值进行比较；
- [0027] 5) 比较结果正确则正常启动，否则提示用户出现异常。
- [0028] 本发明由于采用了上述方法，通过在传统计算机主板上插入一块 PCI 卡，使传统计算机实现可信计算的全部功能。本发明方法操作简单、成本低廉，借助可信计算的完备的安全机制，为传统计算机提供可靠的安全保障。
- [0029] 下面结合附图和具体实施方式对本发明作进一步说明。

附图说明

- [0030] 图 1 为本发明的连接示意图；
- [0031] 图 2 为本发明方法中 BIOS 程序对扩展 ROM 检测方法流程图；
- [0032] 图 3 为本发明方法中扩展 ROM 程序完成信任链建立的处理方法流程图；
- [0033] 图 4 为本发明中 PCI 目标接口使用信号示意图；
- [0034] 图 5 为本发明中 PCI 配置空间读时序图；
- [0035] 图 6 为本发明中 PCI 配置空间写时序图；
- [0036] 图 7 为本发明中 LPC 总线时序图。

具体实施方式

- [0037] 参看图 1 至图 3，本发明传统计算机升级为可信计算机的方法步骤为：
- [0038] 1) 将传统计算机通过主板上的 PCI 接口与可信计算 TCM 模块上的 LPC 接口转换电路连接访问可信计算 TCM 模块，PCI 接口与 LPC 接口转换电路之间包括 PCI 目标接口和 LPC 主机接口。
- [0039] 2) PCI 接口电路中扩展一个只读存储器 ROM 电路。
- [0040] 3) 传统计算机在 BIOS 启动阶段运行 PCI 接口电路中的扩展 ROM 内的程序。
- [0041] 4) 扩展 ROM 程序实现信任链的建立，其方法为：
- [0042] A) 传统计算机 BIOS 程序对扩展 ROM 检测正确后，BIOS 程序拷贝扩展 ROM 程序到运行空间；BIOS 程序对扩展 ROM 检测方法为：
- [0043] a) BIOS 启动代码，检测 PCI 设备的配置空间的扩展 ROM 基址寄存器是否存在，存在则 BIOS 将为扩展 ROM 分配一段空闲的地址空间；
- [0044] b) 检测代码的前两个字节是否是 AA55；

[0045] c) 如果扩展 ROM 有效，则 BIOS 会检测代码类型，以及厂商代码和设备代码的其他信息；

[0046] d) 信息都正确后，BIOS 会将扩展 ROM 中正确的代码都拷贝到 RAM 中，这些代码就可以执行了。

[0047] B) 执行扩展 ROM 程序，扩展 ROM 程序完成信任链建立的处理方法为：

[0048] a) 启动 TCM 模块并进行初始化；

[0049] b) 将 BIOS 空间代码送给 TCM 模块进行摘要计算；

[0050] c) 将摘要计算的结果存放在 TCM 模块的 PCR 中；

[0051] d) 将摘要计算结果和存放在 TCM 模块内部非易失存储区中的正确摘要值进行比较；

[0052] e) 比较结果正确则正常启动，否则提示用户出现异常。

[0053] C) 退出扩展 ROM 程序，执行 BIOS 的其他功能。

[0054] 本发明中的 PCI 目标接口接收来自 PCI 主设备的命令，完成对 PCI 读写寄存器的访问以及扩展 ROM 的访问，扩展 ROM 中存放用于信任链建立的代码。PCI 目标接口通过 PCI 写寄存器向 LPC 主机接口发送指令，完成对 LPC 接口的 TCM 模块的访问。PCI 读、写寄存器地址分配于配置空间，扩展 ROM 地址分配于记忆 memory 空间。

[0055] 参看图 4，本发明中为处理数据、寻址、接口控制、仲裁以及系统功能，PCI 目标接口只需要做为目标设备使用。

[0056] 在本发明的可信计算平台上，通过对 PCI 目标接口和 LPC 主机接口的自动检测，将自动加载不同的驱动，不需要根据不同的系统分别安装不同的驱动。在同时安装了 LPC 主机接口的 TCM 模块和 PCI 目标接口的 TCM 模块的场合，将优先选择 LPC 主机接口的 TCM。

[0057] 参看图 5，在 FRAME# 信号由高变低有效后的第一个时钟上升沿，地址总线信号 AD 被采样，由 C/BE# 决定选择的是 PCI 设备的配置空间，IDSEL# 是用于选取被配置的 PCI 设备。当 PCI 主设备端准备好接收数据时，IRDY# 变有效（本设计 IRDY# 始终准备好接收数据），如果 PCI 设备端也准备好发送数据，则 TRDY# 信号被 PCI 设备端拉低，变为有效。只有在 IRDY# 和 TRDY# 都有效时，同时 DEVSEL# 也有效时，数据传输才开始进行。在传输到最后一个字节时，FRAME# 信号无效，但是 IRDY# 信号继续保持有效，此时 TRDY# 有效时，则传输最后一个字节。

[0058] 参看图 6，配置空间写的时序和读的时序基本相同，只是在 PCI 主设备准备发送数据时将 IRDY# 有效，然后等待 PCI 从设备端将 TRDY# 置为有效，同时使得 DEVSEL# 有效，开始数据写操作。

[0059] 参看图 7，LPC 总线主控端将 LFRAME# 信号拉低并保持大于 1 个时钟周期的时间，使得 LAD 信号发出 Start，表示一帧数据传输的开始。然后 LFRAME# 信号拉高无效，帧数据传输开始，第一个字节传输的是操作类型和读写方式，本设计采用了 I/O 读和 I/O 写两种方式。每次传输一个字节，接下来传输 I/O 的地址。TAR 表示在读取数据时数据传输方向的改变，使得外部总线处于三态，后面的 Sync 表示插入等待周期。因为在数据传输方向变化时由于 LPC 从设备可能并没有将数据准备好，所以通过插入等待周期等待对方准备数据，然后开始数据的传输。在写周期内，则 TAR 不需改变传输方向，Sync 为 0，表示不需插入等待。

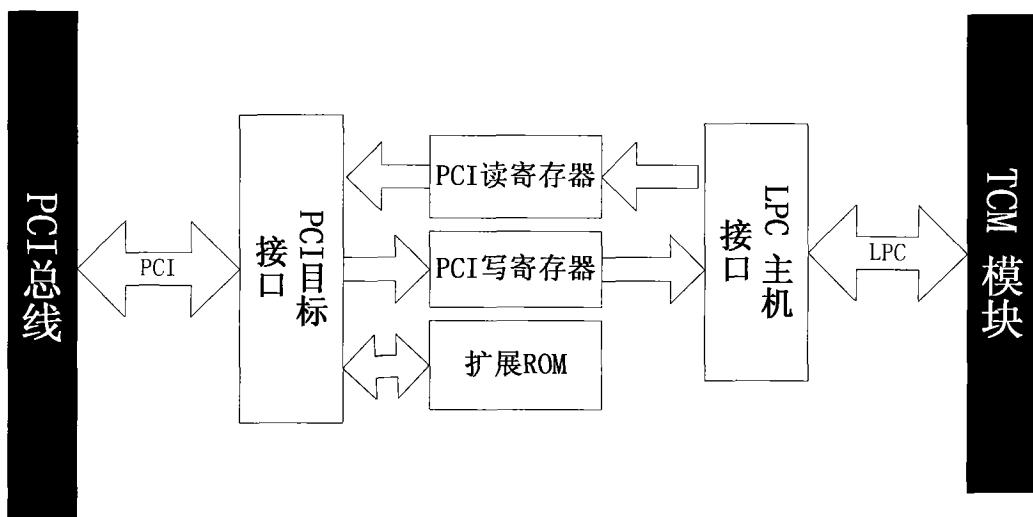


图 1

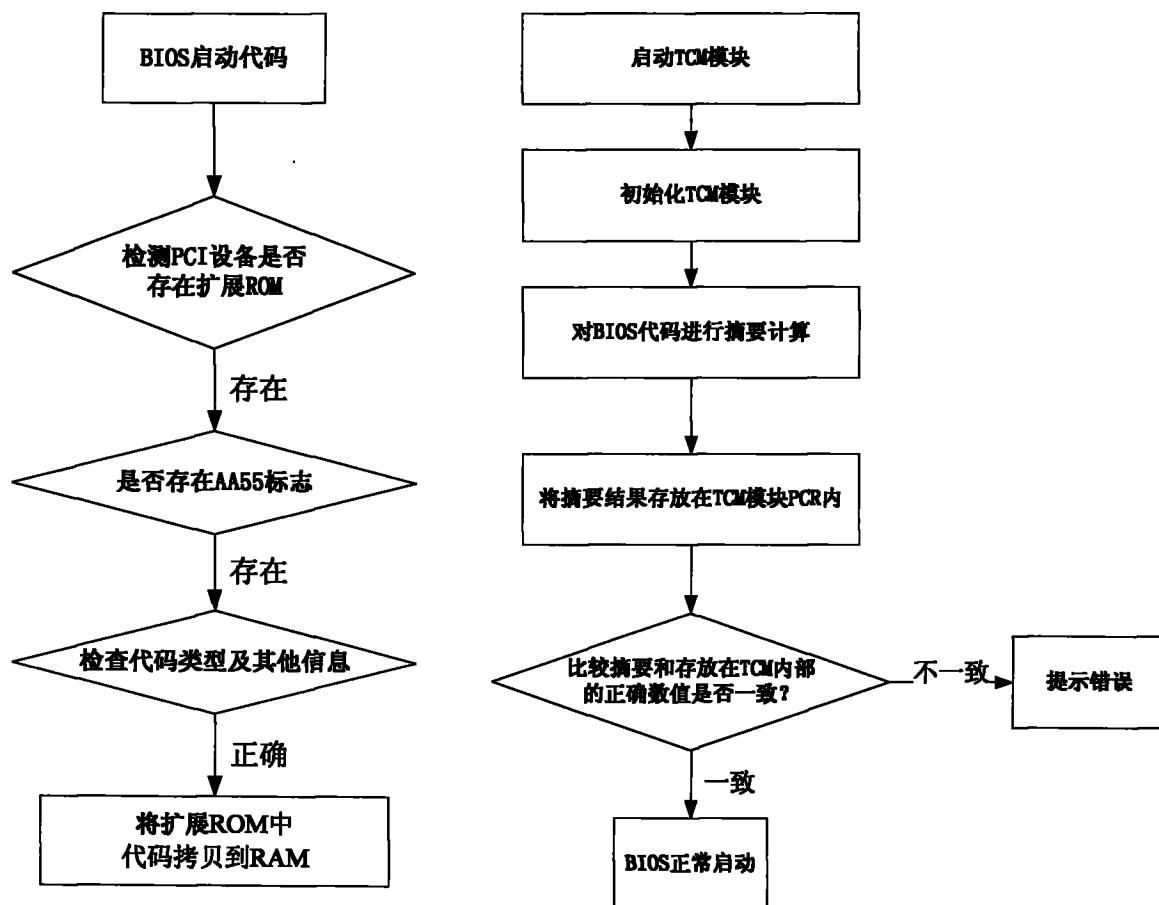


图 2

图 3

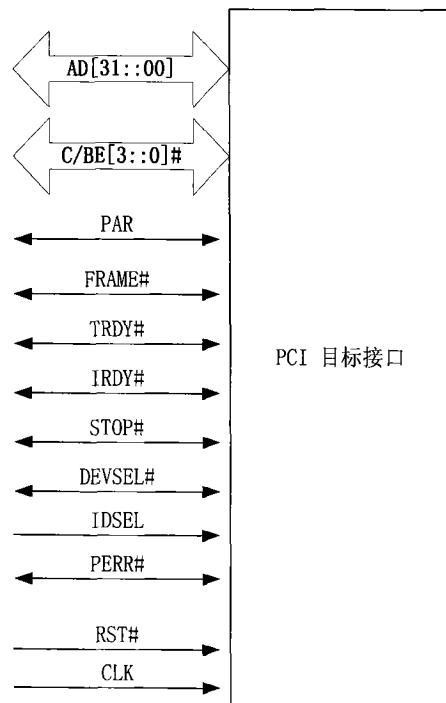


图 4

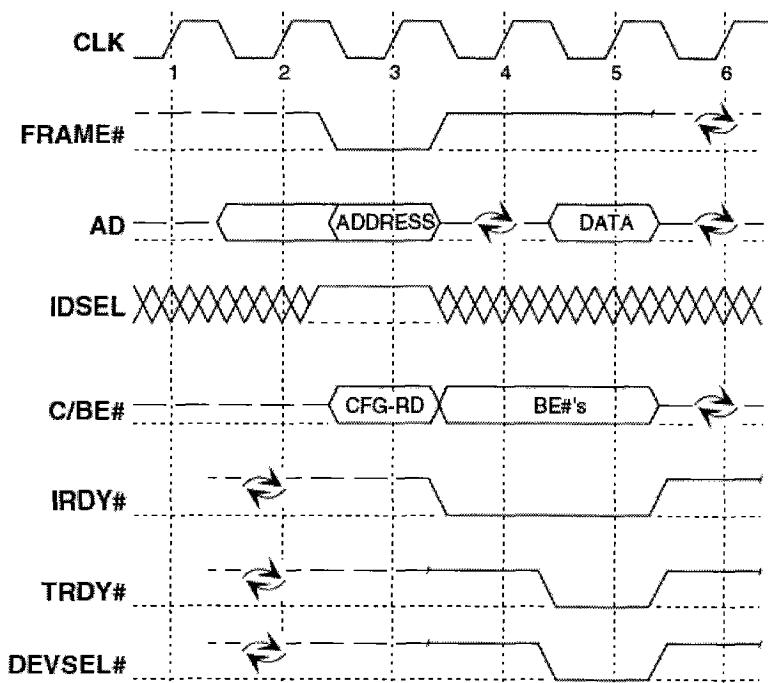


图 5

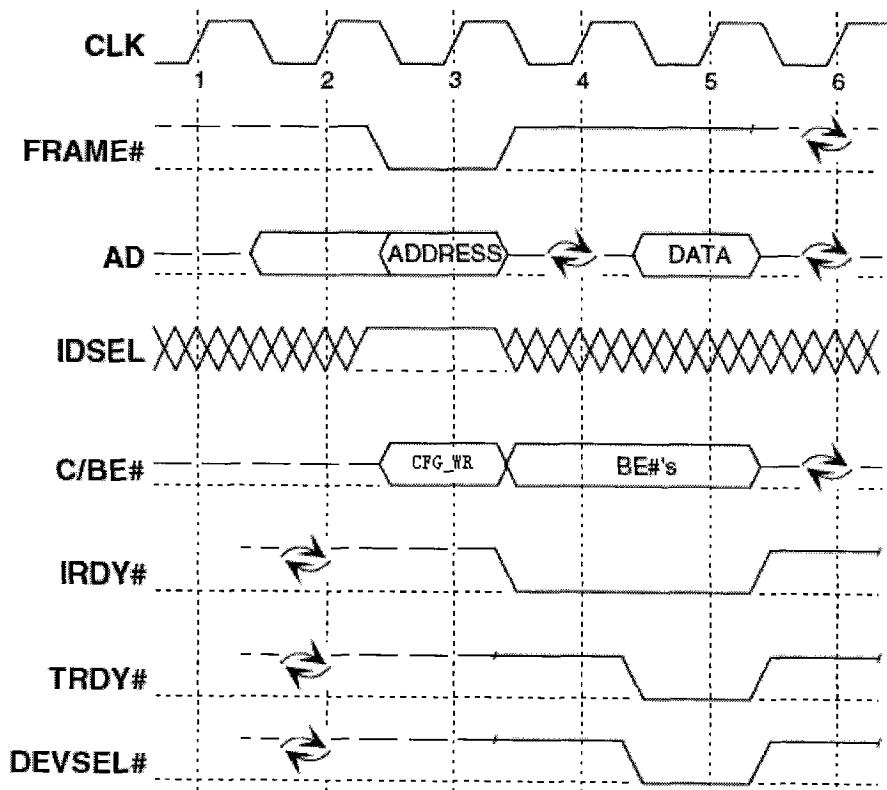


图 6

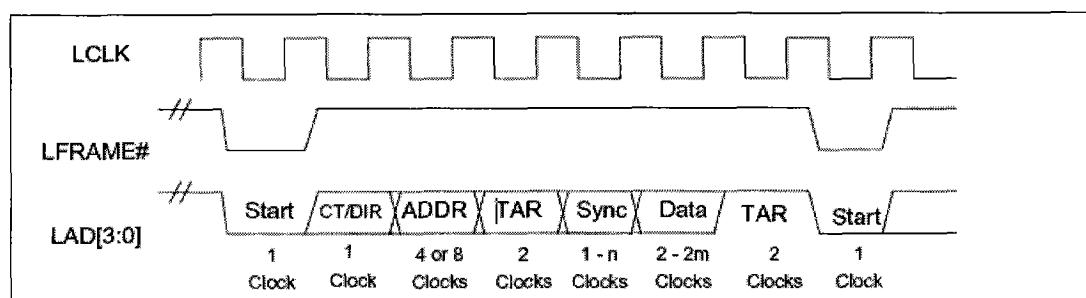


图 7