

一种用于安全验证的主板以及安全验证方法、装置及介质

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种用于安全验证的主板以及安全验证方法、装置及介质。

背景技术

[02]目前，随着信息安全技术的迅速发展和人们对自身隐私数据的愈发关注，以及可信计算在解决信息安全隐患等方面的帮助，可信计算技术已经成为信息安全领域一个重要的应用和研究分支。

发明内容

[03]本说明书提供一种用于安全验证的主板以及安全验证方法、装置及介质，以部分的解决相关技术存在的上述问题。

[04]本说明书采用下述技术方案：本说明书提供一种用于安全验证的主板，所述用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，其中：所述校验单元，用于当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；接收所述通道管理单元返回的所述待校验设备的配置信息，并根据所述校验单元存储的各待校验设备的校验信息对所述配置信息进行校验，以及当确定所述待校验设备校验通过后，控制所述电子设备启动；所述通道管理单元，用于根据接收到的所述校验指令，确定所述待校验设备，并获取所述待校验设备的配置信息，以及将所述配置信息返回所述校验单元。

[05]本说明书提供一种安全验证方法，用于校验单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，包括：当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；接收所述通道管理单元返回的所述待校验设备的配置信息；根据已存储的各待校验设备的校验信息，对所述配置信息进行校验；当确定所述待校验设备校验通过后，控制所述电子设备启动。

[06]本说明书提供一种安全验证方法，用于通道管理单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，包括：当所述电子设备上电后，接收所述校验单元发送的校验指令；根据所述校验指令，确定所述待校验设备；获取所述待

校验设备的配置信息，并将所述配置信息返回所述校验单元。

[07]本说明书提供一种安全验证装置，用于校验单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，包括：发送模块，用于当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；接收模块，用于接收所述通道管理单元返回的所述待校验设备的配置信息；校验模块，用于根据已存储的各待校验设备的校验信息，对所述配置信息进行校验；启动模块，用于当确定所述待校验设备校验通过后，控制所述电子设备启动。

[08]本说明书提供一种安全验证装置，用于通道管理单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，包括：接收模块，用于当所述电子设备上电后，接收所述校验单元发送的校验指令；确定模块，用于根据所述校验指令，确定所述待校验设备；转发模块，用于获取所述待校验设备的配置信息，并将所述配置信息返回所述校验单元。

[09]本说明书提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述安全验证方法。

[10]本说明书采用的上述至少一个技术方案能够达到以下有益效果：本说明书公开了一种用于安全验证的主板以及安全验证方法、装置及介质，通过设置和通道管理单元连接的校验单元，以及和各待校验设备连接的通道管理单元，当电子设备上电后，控制校验单元向通道管理单元发送针对待校验设备的校验指令，并通过通道管理单元根据接收到的校验指令获取待校验设备的配置信息，以及将配置信息返回校验单元，再由校验单元根据已存储的校验信息对接收到的配置信息进行校验，当校验通过后，控制电子设备启动。

[11]通过通道管理单元，将待校验设备的配置信息发送至校验单元进行校验，来实现在电子设备启动过程中对于设置在电子设备内的待校验设备和/或该电子设备外接的待校验设备的安全验证，保证了信息安全。

附图说明

[12]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。在附图中：

[13]图 1 为本说明书提供的用于安全验证的主板的结构示意图；

[14]图 2A 为本说明书提供的用于安全验证的主板的结构示意图;

[15]图 2B 为本说明书提供的用于安全验证的主板的结构示意图;

[16]图 3 为本说明书提供的安全验证方法的流程示意图;

[17]图 4 为本说明书提供的安全验证方法的流程示意图;

[18]图 5 为本说明书提供的安全验证装置的结构示意图;

[19]图 6 为本说明书提供的安全验证装置的结构示意图。

具体实施方式

[20]为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书保护的范围。

[21]目前，随着计算机技术的发展，类似于网卡等能和网络中的设备进行交互，和/能对数据进行处理的外设逐渐增多，在外设中部署用于进行数据处理的芯片已经成为较为普遍的情况了。在此情况下，攻击者利用电子设备连接的外设对电子设备进行攻击以窃取信息的情况变得愈发常见。因此，在电子设备上电启动时，对连接该电子设备的外设进行安全验证已经成为信息安全领域中需要解决的问题之一。

[22]以下结合附图，详细说明本说明书各实施例提供的技术方案。本说明书实施例将基于一种用于安全验证的主板来对电子设备的外设进行安全验证。

[23]图 1 为本说明书提供的用于安全验证的主板的结构示意图。其中：该用于安全验证的主板包含校验单元和通道管理单元。

[24]从硬件上来说，本说明书提供的一个或多个实施例中，该用于安全验证的主板中的校验单元和通道管理单元，具体可为芯片、逻辑控制电路等。该校验单元为可接收配置信息，并对配置信息进行验证的 TPM 芯片，当电子设备上电后，即启动该校验单元，即，TPM 芯片，由该校验单元从通道管理单元处获取各待校验设备的配置信息，并对各配置信息进行校验。

[25]该通道管理单元可为可编程数字逻辑芯片，如，现场可编程门阵列（Field - Programmable Gate Array, FPGA）芯片、复杂可编程逻辑器件（Complex Programmable Logic Device, CPLD）芯片等。该通道管理单元可与该校验单元连接进行数据传输，且该通道管理单元还可与待校验设备连接进行数据传输。

[26]其中，该待校验设备包含有存储该电子设备的主机配置信息的目标存储器。该主机配置信息为包含 BIOS 和/或 BMC 等电子设备自身最基本的配置信息。该待校验设备可

与该电子设备外接，如，打印机、网卡等，也可为设置在该电子设备内，如，图形处理器（Graphic Processing Unit，GPU）等协处理器、用于散热的风扇等。

[27]当然，上述用于安全验证的主板，可部署在独立的电路板上，也可与该电子设备的其他电子器件部署在同一个电路板中。其他电子器件可为CPU、GPU、内存条等。该待校验设备可与该校验单元和通道管理单元设置在同一电路板上，也可与该校验单元和通道管理单元设置在不同电路板，并通过排线、I/O总线等进行连接，来实现通道管理单元和待校验设备之间的数据传输。具体该用于安全验证的主板如何设置，该用于安全验证的主板设置在该电子设备中的位置、该用于安全验证的主板具体与该电子设备中的待校验设备如何连接等可根据需要进行设置，本说明书对此不做限制。

[28]从软件上来说，本说明书提供的一个或对一个或多个实施例中，该校验单元可为在TPM芯片上运行，并对接收到的数据进行安全校验的程序。该通道管理单元可为在可编译芯片上运行，接收数据并对数据进行解析或转发等处理的程序。该用于安全验证的主板通过运行各单元的代码实现各单元的功能。并且，本说明书中不同单元的代码是相互独立的，每个单元可通过预设的数据接口和其他单元或设备进行通信或数据传输，通过相互独立的单元使得可以单独对每个单元进行代码的迭代更新以及测试。

[29]在本说明书提供的一个或多个实施例中，该用于安全验证的主板能够实现对多个待校验设备进行安全验证的基础是：该校验单元不直接与待校验设备连接来获取待校验设备的配置信息，而是与通道管理单元连接，由通道管理单元与各待校验设备连接来获取各配置信息，并将配置信息转发至该校验单元，由校验单元对配置信息进行校验。其中，该通道管理单元预留了多条通道与待校验设备连接，因此可实现在电子设备上电时对于多个待校验设备的安全验证，来保证信息安全。

[30]基于此，该校验单元可通过通道管理单元来获取各待校验设备的配置信息。

[31]具体的，在电子设备上电时后，该校验单元可被唤醒。

[32]则该校验单元可在被唤醒，即，上电后，向通道管理单元发送针对于待校验设备的校验指令。

[33]其中，该校验指令可为针对该通道管理单元所连接的所有待校验设备发送的，也可为该通道管理单元所连接的至少部分待校验设备发送的。

[34]于是，该通道管理单元在接收到该校验指令后，可根据该校验指令确定待校验设备，并从该待校验设备中，获取该待校验设备的配置信息，以及将该配置信息返回给校验单元。

[35]该校验单元可将该通道管理单元发送的至少部分待校验设备的配置信息进行接收。其中，接收的配置信息所对应的各待校验设备，与上述校验指令所针对的各待校验设备为相同设备。

[36]则在接收到配置信息后，该校验单元可根据自身预先存储的各待校验设备的校验信息对接收到的配置信息进行校验。

[37]以获取电子设备的主机配置信息为例，假设主机配置信息为 BIOS 程序，则该校验单元可向通道管理单元发送针对于目标存储器的校验指令。该通道管理单元可根据该校验指令，确定存放 BIOS 程序的目标存储器，并从该目标存储器中获取 BIOS 程序，以及将该 BIOS 程序转发至校验单元。

[38]该校验单元在接收到 BIOS 程序后，可将该 BIOS 程序进行运行，并基于运行结果和自身所存储的可信度量根是否匹配，来判断是否验证通过。

[39]当然，上述通道管理单元接收到的配置信息，可为将该目标存储器中的 BIOS 程序的运行结果，则该通道管理单元可将该运行结果发送至该校验单元中，由校验单元对该 BIOS 程序的运行结果进行校验。具体配置信息的类型与形式，以及如何对配置信息进行度量已经是目前较为成熟的技术了，本说明书对此不做限制。

[40]则在该校验单元将针对于校验指令返回的配置信息校验通过后，该校验单元可控制该电子设备启动。

[41]进一步的，该校验单元中可存储有各待校验设备的设备标识，则该待校验设备可基于存储的设备标识，向该通道管理单元发送携带有设备标识的校验指令。

[42]该通道管理单元在接收到该校验指令后，可根据该校验指令中携带的设备标识，确定该设备标识对应的待校验设备，并向该待校验设备发送获取指令。

[43]则该待校验设备在接收到该获取指令后，可将自身的配置信息发送至该通道管理单元。其中，该待校验设备还可为存放待校验设备的配置信息的非易失性存储器。具体该待校验设备的类型、如何存放配置信息，以及如何从待校验设备中获取配置信息，可根据需要进行设置，本说明书对此不做限制。

[44]针对每个待校验设备的配置信息，在接收到该配置信息后，该通道管理单元可根据该待校验设备的设备标识，将该配置信息转发至该校验单元。

[45]则该校验单元可对该配置信息进行接收，并根据该配置信息对应的设备标识，从预先存储的各配置信息分别对应的校验信息中，确定该设备标识对应的校验信息，进而基于确定出的校验信息对该设备标识进行校验。

[46]其中，该校验信息可为字符串、也可为密钥、还可为预设规则，具体该校验信息的类型和形式以及如何基于校验信息对配置信息进行校验等可根据需要进行设置，本说明书对此不做限制。

[47]更进一步的，若该电子设备本身不可信，则再去验证其他待校验设备的安全性将毫无疑问，也就是说，只有在电子设备可信的情况下，才有必要去度量其他待校验设备的安全性。

[48]基于此,该校验单元可首先对电子设备的主机配置信息进行校验,并当校验通过后,再对其他待校验设备的配置信息进行校验。

[49]具体的,该校验单元可在上电后,向通道管理单元发送针对于目标存储器的第一校验指令。

[50]则该通道管理单元可根据该第一校验单元中的设备标识,确定目标存储器,并从目标存储器中获取该电子设备的主机配置信息,并将该主机配置信息转发至校验单元。

[51]则该校验单元可在接收到该主机配置信息后,根据已存储的该电子设备对应的校验信息,对该主机配置信息进行校验。

[52]若校验不通过,则该校验单元可认为该电子设备自身不可信,于是,在此场景中,为了保证信息安全,避免危险进一步扩大,该校验单元可发送用于提示该主机存在故障的预警信息,并控制电子设备下电关机。

[53]若校验通过,则该校验通过可认为电子设备处于可信执行环境,并继续对其他待校验设备进行安全验证。于是,该校验单元可根据除该目标存储器外的其他待校验设备的设备标识,向通道管理单元发送第二校验指令。

[54]则该通道管理单元可根据该第二校验指令中的设备标识,确定该设备标识对应的待校验设备,于是,该通道管理单元可获取该待校验设备的外设配置信息,并当获取到该外设信息后,根据该第二校验指令中的设备标识,将该外设配置信息返回该校验单元。

[55]该校验单元可根据该外设配置信息中携带的设备标识,从预先存储的各待校验设备分别对应的校验信息中,确定该设备标识对应的校验信息,并基于确定出的该校验信息,对该外设配置信息进行校验。

[56]若校验不通过,则该校验单元可认为该待校验设备不可信。同样的,在此场景中,为了保证信息安全,避免危险进一步扩大,该校验单元可发送用于提示该待校验设备存在故障的预警信息,并控制该电子设备下电关机。

[57]若校验通过,则该校验单元可认为该待校验设备可信,在此场景中,该校验单元可对各其他待校验设备分别进行安全验证,直至根据各待校验设备的外设配置信息均校验通过后,则可控制该电子设备启动。

[58]上述图 1 中仅以该用于安全验证的主板对该电子设备内部设置的一个待校验设备和外接于该用于安全验证的主板的一个待校验设备为例进行说明,但实际上,设置在该电子设备内部的待校验设备以及外接于该电子设备的待校验设备均可为多个,如图 2A 所示。

[59]图 2A 为本说明书提供的用于安全验证的主板的结构示意图,图中,该电子设备内部设置有 n 个待校验设备,该电子设备外接有 $m-k+1$ 个待校验设备,于是,该通道管理单元可与设置在该电子设备内部的待校验 1 设备~待校验设备 n 连接,同样的,该通道

管理单元可与设置在该电子设备外部的待校验设备 k~待校验设备 m 连接。于是，该校验单元可通过通道管理单元，对该通道管理单元连接的各待校验设备进行校验。

[60]另外，在本说明书中，还可能出现通过物理接口和通道管理单元进行连接的待校验设备。以待校验设备为网卡、物理接口为满足（Open Core Protocol，OCP）标准的 OCP 接口为例，则该网卡中至少设置有接口单元和外设存储器，该接口单元用于通过物理接口和该通道管理单元连接进行数据传输，该外设存储器用于存储该待校验设备的外设配置信息。

[61]于是，该通道管理单元在获取该待校验设备的外设配置信息时，需要通过该待校验设备的接口单元，将该外设配置信息进行获取。

[62]更进一步的，针对每个接口单元，该接口单元中传输的数据类型等为预先定义好的，若攻击者利用该接口单元，在电子设备启动过程中或启动后，从该电子设备中获取敏感信息，或注入不可信数据，则同样无法保证该信息安全。

[63]基于此，在对待校验设备的外设配置信息进行校验之前，还需对待校验设备的接口单元进行安全验证。

[64]具体的，该校验单元在对主机配置信息校验通过后，可向该通道管理单元发送针对该待校验设备的接口单元的第三校验指令。

[65]则该通道管理单元在接收到该第三校验指令后，可根据该第三校验指令中的设备标识，确定该待校验设备中的接口单元，并从该接口单元中，获取该接口单元的接口配置信息，以及将该接口配置信息转发至该校验单元中。

[66]其中，该接口单元中可设置有存储该接口单元对应的接口配置信息的存储器，则该接口单元可获取该存储器中存储的接口配置信息，并将该接口配置信息转发至校验单元。存储该接口单元的接口配置信息的存储器可与该接口单元连接，且该接口配置信息可为该接口对应的执行标准，即，该接口单元中各管脚传输的数据类型，各管脚传输数据的时间等。

[67]该校验单元可根据自身存储的对于接口单元的校验信息，对该接口配置信息进行验证，并在对该接口配置信息验证通过后，向该通道管理单元发送针对于该待校验设备的外设存储器的第二校验指令。

[68]则该通道管理单元可根据该第二校验指令，通过该接口单元，从该待校验设备的外设存储器中获取外设配置信息，并将该外设配置信息返回至校验单元，由该校验单元对该外设配置信息进行验证。如图 2B 所示。

[69]图 2B 为本说明书提供的用于安全验证的主板的结构示意图，图中，需要对包含该电子设备内设的待校验设备 a、该电子设备外接的待校验设备 b，以及存储该电子设备的主机配置信息的目标存储器进行安全度量，即，进行校验。该通道管理单元和该接口

单元通过预设的物理接口连接。该电子设备内设的待校验设备和目标存储器与该通道管理单元部署在用于安全验证的主板中，通过串行总线进行连接。

[70]在该电子设备上电后，该校验单元可向该通道管理单元发送第一校验指令，该通道管理单元可根据该第一校验指令，从该目标存储器中获取该电子设备的主机配置信息，并将该主机配置信息发送至校验单元中进行验证。

[71]当主机配置信息验证通过后，若需对通过预设的物理接口连接的待校验设备 b 进行校验，则该校验单元需针对该待校验设备 b 的接口单元，发送第三校验指令。该通道管理单元可根据该第三校验指令，从该接口单元中获取该接口单元的接口配置信息，并将该接口配置信息发送至校验单元中进行验证。当验证通过后，该校验单元可针对该待校验设备 b 的外设存储器，向该通道管理单元发送第二校验指令。则该通道管理单元可根据该第二校验指令，通过该接口单元从该外设存储器中获取该待校验设备的外设配置信息，并将该外设配置信息返回校验单元进行校验。

[72]当主机配置信息验证通过后，若需对通过预设的物理接口连接的待校验设备 a 进行校验，则该校验单元可直接向该通道管理单元发送针对该待校验设备 a 的第二校验指令。由该通道管理单元根据该第二校验指令获取该待校验设备 a 的外设配置信息，并将该外设配置信息发送至该校验单元，由该校验单元对该外设配置信息进行验证。

[73]当然，上述图 2B 中的外设存储器还可视为是与通道管理单元通过预设的接口单元连接的待校验设备。即，该接口单元并非在该待校验设备内，而是该待校验设备通过外设的接口单元与该通道管理单元连接。具体该待校验设备如何定义以及如何与该接口单元进行连接，可根据需要进行设置，本说明书对此不做限制。

[74]另外，位于任一芯片，该芯片在生产后，其各管脚对应的数据传输标准已经预定义。其中，针对每个管脚，该管脚的数据传输标准至少包含有该管脚传输信号的时段。而在该通道管理单元使用可编程逻辑芯片的情况下，若该可编程逻辑芯片在该电子设备启动后仍需进行数据处理，则该通道管理单元需在不影响各管脚原有传输信号的情况下，将配置信息进行传输。

[75]具体的，该通道管理单元可针对每个管脚，根据该管脚的数据传输标准，来确定出该管脚的空闲时段。于是，该通道管理单元可在该空闲时段内将配置信息进行传输。其中，该空闲时段为预先定义该管脚进行数据传输的时段。

[76]进一步的，在本说明书中，可采用时分复用的方式，复用该通道管理单元对应的各管脚，来将配置数据进行传输。以该通道管理单元为符合开方计算项目（Open Compute Project, OCP）标准的芯片为例，如表 1 所示：

管脚	原有信号	复用信号	I/O
OCP_A1	DATA_N	SPI_CS	I
OCP_A2	CLK	SPI1_MISO	0
OCP_A3	SLOT_ID1	CLK	I
.....			

表 1

[77]表 1 为本说明书提供的通道管理单元的信号复用示意表。其中，OCP_A1、OCP_A2、OCP_A3、...为该通道管理单元的不同管脚，原有信号为基于各管脚预先定义的数据传输标准进行数据传输时，所传输的信号类型，其中，DATA_IN 为输入信号，CLK 为时钟信号、SLOT_ID1 为上述物理接口的接口序号。其中，一个通道管理设备可通过多个物理接口，与多个待校验设备连接。复用信号为该通道管理单元在该管脚的空闲时段传输的信号的类型。其中，SPI_CS 为选片信号，用于并控制该通道管理单元选通待校验设备。I/O 为该管脚具体用于接收数据还是用于发送数据。

[78]当然，针对每个管脚，该管脚的原有信号以及复用信号所符合的标准或定义方式，以及具体定义的类型可根据需要进行设置，本说明书对此不做限制。

[79]进一步的，在本说明书中，通道管理单元和待校验设备之间的通道在该电子设备上电后会产生随机信号，为了避免该随机信号对该通道管理单元所传输的配置信息的干扰。通道管理单元还可在确定待校验设备后，选通自身与该校验设备连接的通道，并从该通道获取待校验设备的配置信息。

[80]当然，该通道管理单元还可在确定待校验设备后，选通自身与该校验设备连接的通道，并为该待校验设备进行供电，以唤醒该待校验设备，从在该待校验设备唤醒后，从该通道获取待校验设备的配置信息。以此来避免上述随机信号的影响，以及节省资源。

[81]另外，目前校验单元在将主机配置信息校验通过后，即会对电子设备中部署的操作系统等进行校验，并当校验通过后，启动该操作系统。而本说明书中的校验单元在将主机配置信息校验通过后，还需要对其他待校验设备的安全进行验证。

[82]因此，在对主机配置信息校验通过后，该校验单元可向该电子设备的控制单元发送挂起指令，断开和存储该主机配置信息的非易失性存储单元的连接，从而延迟电子设备启动，并根据待校验设备的设备标识向通道管理单元发送校验信息，从而根据校验结果判断该电子设备和待校验设备均处于可信环境中。

[83]于是，在该校验单元将各待校验设备的外设配置信息校验通过后，该校验单元可确定该电子设备和待校验设备均处于可信环境，则该校验单元可控制该电子设备继续启动，于是，该校验单元可向该电子设备的控制单元发送执行指令，将存储该主机配置信息的

非易失性存储单元进行连接，从而继续该电子设备的启动程序。

[84]进一步的，该电子设备中可包含和/或连接有多个待校验设备，而每个待校验设备的优先级不完全相同，如，网卡因为可对电子设备中的数据进行处理的原因，可优先对网卡进行校验，而打印机因为只能执行将数据进行打印等操作，可暂缓对打印机的校验。且若网卡校验失败时，该校验单元可认为该电子设备的网络环境不可信，控制电子设备下电关机，若打印机校验失败，则该校验单元可认为打印机不可信，继续启动电子设备并发送用于提示该打印机存在异常的预警信息。

[85]于是，当主机配置信息校验通过后，该校验单元可按照预设的各待校验设备的优先级，依次针对每个待校验设备，向该通道管理单元发送针对该待校验设备的第二校验指令，并接收针对该第二校验指令返回的配置信息。

[86]则当根据接收到的配置信息确定该待校验设备处于可信环境时，则该校验单元可根据下一个待校验设备的设备标识，向该通道管理单元发送校验指令，直至完成对各待校验设备的验证为止。

[87]更进一步的，在校验单元对待校验设备的外设配置信息进行验证时，还可能出现由于外设配置信息由于待校验设备的状态影响，导致验证失败的情况出现。

[88]因此，针对每个待校验设备，该校验单元可根据该待校验设备的设备标识，向通道管理单元发送复位指令。

[89]则该通道管理单元可将该复位指令转发至待校验设备。

[90]待校验设备根据该复位指令恢复初始状态，并在恢复初始状态后，将自身的外设配置信息发送至该通道管理单元。

[91]该通道管理单元可根据该复位指令，将该外设配置信息发送至该校验单元中，由该校验单元对该待校验设备进行安全验证。

[92]其中，该复位指令也可该校验单元根据外设配置信息校验不通过时，由该校验单元根据该待校验设备的设备标识发送的。该复位指令的具体发送时机可根据需要进行设置，本说明书对此不做限制。

[93]如图 1 所述的用于安全验证的主板，通过设置和通道管理单元连接的校验单元，以及和各待校验设备连接的通道管理单元，当电子设备上电后，控制校验单元向通道管理单元发送针对待校验设备的校验指令，并通过通道管理单元根据接收到的校验指令确定待校验设备，获取待校验设备的配置信息，以及将配置信息返回校验单元，再由校验单元根据已存储校验信息对接收到的配置信息进行校验，当校验通过后，控制电子设备启动。用于安全验证的主板通过通道管理单元，来实现将待校验设备的配置信息发送至校验单元进行校验，来实现在电子设备启动过程中对于设置在电子设备内的待校验设备和/或该电子设备外接的待校验设备的安全验证，保证了信息安全。

[94]另外,为了保证资源的利用率,该校验单元和该通道管理单元还可将采用时分复用,和/或频分复用的形式,在数据传输通道中传输数据。

[95]具体的,该校验单元和该通道管理单元在第一数据传输通道中传输第一数据,来实现数据传输。

[96]于是,该校验单元可确定与该通道管理单元进行数据传输时所用的第一传输通道,并确定该第一传输通道对应的时频资源。

[97]然后,该校验单元可确定与该通道管理单元进行数据传输时的第一数据,并根据第一数据,将该第一传输通道的时频资源进行分割。

[98]最后,该校验单元可根据分割后的时频资源,将各第一数据进行传输。

[99]其中,在根据第一数据将时频资源进行分割时,可根据该第一数据中包含的数据量将时频资源进行分割,或根据第一数据中包含的数据种类将时频资源进行分割,具体如何基于时分复用,和/或频分复用的形式来传输数据,已经是目前较为成熟的技术了,本说明书对此不做限制。

[100]当然,该通道管理单元和各待校验设备还采用时分复用,和/或频分复用的形式,在数据传输通道中传输数据。

[101]具体的,通道管理单元和各待校验设备在第二数据传输通道中传输第二数据,来实现数据传输。

[102]于是,针对每个待校验设备,该设备管理单元可确定与该待校验设备进行数据传输时所用的第二传输通道,并确定该第二传输通道对应的时频资源。

[103]然后,该设备管理单元可确定与该待校验设备进行数据传输时的第二数据,并根据第二数据,将该第二传输通道的时频资源进行分割。

[104]最后,该校验单元可根据分割后的时频资源,将各第二数据进行传输。

[105]同样的,在根据第二数据将时频资源进行分割时,可根据该第二数据中包含的数据量将时频资源进行分割,或根据第二数据中包含的数据种类将时频资源进行分割,具体如何基于时分复用,和/或频分复用的形式来传输数据,已经是目前较为成熟的技术了,本说明书对此不做限制。

[106]上述采用时分复用/频分复用的方式来进行数据传输,以在较少的时间内,将主机配置信息和各待校验设备的外设配置信息传输至该校验单元中,在较短时间内完成对该主机自身以及该主机内待校验设备的验证。保证业务执行的效率,避免电子设备启动时需要太长时间导致用户满意度下降,资源利用率变低等情况的出现。

[107]基于同样思路,本说明书还提供一种安全验证方法的流程示意图,具体如图3所示。

[108]图3为本说明书提供的安全验证方法的流程示意图,用于校验单元进行安全验证,

用于安全验证的主板部署在电子设备中,所述电子设备内设有待校验设备和/或外接有待校验设备,所述用于安全验证的主板包含校验单元和通道管理单元,所述校验单元和所述通道管理单元连接,所述通道管理单元和各待校验设备连接。

[109]S100: 当所述电子设备上电后,向所述通道管理单元发送针对待校验设备的校验指令。

[110]S102: 接收所述通道管理单元返回的所述待校验设备的配置信息。

[111]S104: 根据已存储的各待校验设备的校验信息,对所述配置信息进行校验。

[112]S106: 当确定所述待校验设备校验通过后,控制所述电子设备启动。

[113]在本说明书中的一个或多个实施例中,该安全验证方法可由上述用于安全验证的主板中的校验单元执行,具体流程可参见上述对于用于安全验证的主板中对于校验单元的描述,本说明书对此不再赘述。

[114]基于同样思路,本说明书还提供一种安全验证方法的流程示意图,具体如图 4 所示。

[115]图 4 为本说明书提供的安全验证方法的流程示意图,所述方法通道管理单元进行安全验证,用于安全验证的主板部署在电子设备中,所述电子设备内设有待校验设备和/或外接有待校验设备,所述用于安全验证的主板包含校验单元和通道管理单元,所述校验单元和所述通道管理单元连接,所述通道管理单元和各待校验设备连接。

[116]S200: 当所述电子设备上电后,接收所述校验单元发送的校验指令。

[117]S202: 根据所述校验指令,确定所述待校验设备。

[118]S204: 获取所述待校验设备的配置信息,并将所述配置信息返回所述校验单元。

[119]在本说明书中的一个或多个实施例中,该安全验证方法可由上述用于安全验证的主板中的通道管理单元执行,具体流程可参见上述对于用于安全验证的主板中对于通道管理单元的描述,本说明书对此不再赘述。

[120]基于同样思路,本说明书还提供一种安全验证装置的结构图,具体如图 5 所示。

[121]图 5 为本说明书提供的安全验证装置的结构示意图,其中,所述装置用于校验单元进行安全验证,用于安全验证的主板部署在电子设备中,所述电子设备内设有待校验设备和/或外接有待校验设备,所述用于安全验证的主板包含校验单元和通道管理单元,所述校验单元和所述通道管理单元连接,所述通道管理单元和各待校验设备连接,所述装置包括以下模块。

[122]发送模块 300,用于当所述电子设备上电后,向所述通道管理单元发送针对待校验设备的校验指令。

[123]接收模块 302,用于接收所述通道管理单元返回的所述待校验设备的配置信息。

[124]校验模块 304，用于根据已存储的各待校验设备的校验信息，对所述配置信息进行校验。

[125]启动模块 306，用于当确定所述待校验设备校验通过后，控制所述电子设备启动。

[126]基于同样思路，本说明书还提供一种安全验证装置的结构图，具体如图 6 所示。

[127]图 6 为本说明书提供的安全验证装置的结构示意图，其中，所述装置用于通道管理单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，所述装置包括以下模块。

[128]接收模块 400，用于当所述电子设备上电后，接收所述校验单元发送的校验指令。

[129]确定模块 402，用于根据所述校验指令，确定所述待校验设备。

[130]转发模块 404，用于获取所述待校验设备的配置信息，并将所述配置信息返回所述校验单元。

[131]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDL、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[132]控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机

可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit, ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器: ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320, 存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至,可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[133]上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[134]为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[135]本领域内的技术人员应明白,本说明书的实施例可提供为方法、系统、或计算机程序产品。因此,本说明书可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[136]本说明书是参照根据本说明书实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[137]这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[138]这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或

其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[139]在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[140]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[141]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[142]还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[143]本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[144]本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[145]本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法

实施例的部分说明即可。

[146]以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种用于安全验证的主板，所述用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，其中：

所述校验单元，用于当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；接收所述通道管理单元返回的所述待校验设备的配置信息，并根据所述校验单元存储的各待校验设备的校验信息对所述配置信息进行校验，以及当确定所述待校验设备校验通过后，控制所述电子设备启动；

所述通道管理单元，用于根据接收到的所述校验指令，确定所述待校验设备，并获取所述待校验设备的配置信息，以及将所述配置信息返回所述校验单元。

2、如权利要求 1 所述的用于安全验证的主板，所述电子设备内设的待校验设备至少包含存储所述电子设备的主机配置信息的目标存储器；

所述校验单元，用于当所述电子设备上电后，向所述通道管理单元发送携带有所述目标存储器的设备标识的第一校验指令；接收所述通道管理单元返回的主机配置信息，并校验，以及当确定所述主机配置信息校验通过后，根据除所述目标存储器外的其他待校验设备的设备标识，向所述通道管理单元发送第二校验指令；直至完成对所述各待校验设备的验证为止；

所述通道管理单元，用于根据所述第一校验指令携带的设备标识，确定所述目标存储器，并从所述目标存储器中获取所述主机配置信息，以及将所述主机配置信息返回所述校验单元；根据所述第二校验指令携带的设备标识，确定所述设备标识对应的待校验设备，并从所述待校验设备中获取外设配置信息，将所述外设配置信息根据所述第二校验指令返回所述校验单元。

3、如权利要求 2 所述的用于安全验证的主板，所述待校验设备至少包含接口单元和外设存储器；所述接口单元和所述通道管理单元通过预设的物理接口连接；

所述通道管理单元，用于通过所述接口单元，从所述外设存储器中获取所述待校验设备的外设配置信息。

4、如权利要求 3 所述的用于安全验证的主板，所述校验单元，用于向所述通道管理单元发送针对所述待校验设备的接口单元的第三校验指令；接收所述通道管理单元返回的接口配置信息，并校验，以及根据所述接口配置信息确定校验通过后，向所述通道管理单元发送针对所述待校验设备的外设存储器的第二校验指令；

所述通道管理单元，用于根据所述第三校验指令，确定所述接口单元，并获取所述接口单元的接口配置信息，以及将所述接口配置信息返回至校验单元；根据所述第二校验指令，通过所述接口单元，从所述外设存储器中获取所述外设配置信息，以及将所述外设配置信息返回至校验单元。

5、如权利要求 1 所述的用于安全验证的主板，所述通道管理单元为预先定义各管

脚的数据传输标准的芯片；

所述通道管理单元，用于针对至少部分管脚，根据该管脚的数据传输标准，确定该管脚的空闲时段，并在所述空闲时段内传输所述配置信息，其中，所述空闲时段为未预先定义所述管脚进行数据传输的时段。

6、如权利要求 2 所述的用于安全验证的主板，除所述目标存储器外的其他各待校验设备的优先级不完全相同；

所述校验单元，用于当所述主机配置信息校验通过后，按照预设的所述除所述目标存储器外的其他各待校验设备的优先级，依次针对每个待校验设备，根据该待校验设备的设备标识，向所述通道管理单元发送第二校验指令，直至完成对所述各待校验设备的验证为止。

7、如权利要求 1 所述的用于安全验证的主板，所述校验单元，用于当根据接收到的配置信息确定校验失败时，确定所述电子设备不可信，并控制所述电子设备下电关机。

8、如权利要求 1 所述的用于安全验证的主板，所述电子设备中还部署有控制单元，所述控制单元和所述通道管理单元连接；

所述校验单元，用于当所述电子设备上电后，向所述通道管理单元发送用于暂停启动所述电子设备的挂起指令；当确定所述待校验设备校验通过后，向所述通道管理单元发送用于继续启动所述电子设备的启动指令；

所述通道管理单元，用于根据接收到的所述挂起指令，连通所述电子设备中的控制单元，并将所述挂起指令发送至所述控制单元，以暂停启动所述控制单元中预先部署的操作系统；将接收到的所述启动指令发送至所述控制单元，以启动所述控制单元中的所述操作系统。

9、如权利要求 1 所述的用于安全验证的主板，所述校验单元，用于向所述通道管理单元发送携带有设备标识的复位指令；

所述通道管理单元，用于根据所述设备标识，将所述复位指令转发至所述设备标识对应的待校验设备，以使所述待校验设备根据所述复位指令恢复初始状态，并获取恢复初始状态后的待校验设备的配置信息，以及将所述配置信息返回至所述校验单元。

10、如权利要求 1 所述的用于安全验证的主板，所述通道管理单元，用于确定所述待校验设备后，选通与所述待校验设备连接的通道，并通过所述通道获取所述待校验设备的配置信息。

11、一种安全验证方法，用于校验单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，所述方法包括：

当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；

接收所述通道管理单元返回的所述待校验设备的配置信息；

根据已存储的各待校验设备的校验信息，对所述配置信息进行校验；

当确定所述待校验设备校验通过后，控制所述电子设备启动。

12、一种安全验证方法，用于通道管理单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，所述方法包括：

当所述电子设备上电后，接收所述校验单元发送的校验指令；

根据所述校验指令，确定所述待校验设备；

获取所述待校验设备的配置信息，并将所述配置信息返回所述校验单元。

13、一种安全验证装置，用于校验单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，所述装置包括：

发送模块，用于当所述电子设备上电后，向所述通道管理单元发送针对待校验设备的校验指令；

接收模块，用于接收所述通道管理单元返回的所述待校验设备的配置信息；

校验模块，用于根据已存储的各待校验设备的校验信息，对所述配置信息进行校验；

启动模块，用于当确定所述待校验设备校验通过后，控制所述电子设备启动。

14、一种安全验证装置，用于通道管理单元进行安全验证，用于安全验证的主板部署在电子设备中，所述电子设备内设有待校验设备和/或外接有待校验设备，所述用于安全验证的主板包含校验单元和通道管理单元，所述校验单元和所述通道管理单元连接，所述通道管理单元和各待校验设备连接，所述装置包括：

接收模块，用于当所述电子设备上电后，接收所述校验单元发送的校验指令；

确定模块，用于根据所述校验指令，确定所述待校验设备；

转发模块，用于获取所述待校验设备的配置信息，并将所述配置信息返回所述校验单元。

15、一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 11 或权利要求 12 所述的方法。