

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06K 19/073 (2006.01)

G06K 17/00 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200610169065.4

[43] 公开日 2007 年 7 月 11 日

[11] 公开号 CN 1996350A

[22] 申请日 2006. 12. 20

[21] 申请号 200610169065.4

[71] 申请人 杭州华为三康技术有限公司

地址 310053 浙江省杭州市高新技术产业开发
区之江科技工业园六和路东华为
3Com 公司

[72] 发明人 秦 娟 苏 勇 余 涛 鲁玉春

[74] 专利代理机构 隆天国际知识产权代理有限公司
代理人 郭晓东

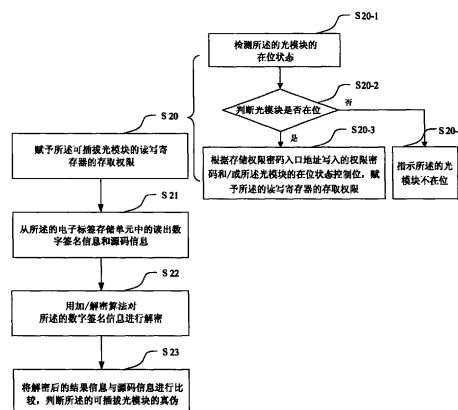
权利要求书 3 页 说明书 10 页 附图 5 页

[54] 发明名称

光模块的电子标签、制作和识别方法及识别装置

[57] 摘要

本发明提供一种可插拔光模块的电子标签、电子标签的制作方法、设备主机识别光模块的电子标签方法及其应用的识别装置。所述的电子标签包括的电子标签存储单元，位于可插拔光模块的读写寄存器中，其包含防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息。设备主机识别光模块的电子标签方法包括：从所述的电子标签存储单元中的读出数字签名信息和源码信息；用加/解密算法对所述的数字签名信息进行解密；将解密后的结果信息与源码信息进行比较，判断所述的可插拔光模块的真伪。本发明利用设备主机对光模块的读写区域的存取权限(密码保护)，通过向光模块内部读写区域写入厂家特定信息，来实现光模块的防伪。



1、一种电子标签的制作方法，所述的电子标签位于可插拔光模块中，其特征在于，包括：

步骤 11：将所述的可插拔光模块的读写寄存器划分出源码区域和数字签名区域；

步骤 12：在所述的源码区域存储可插拔光模块的防伪源码信息；

步骤 13：在所述的数字签名区域存储用以识别所述源码信息的数字签名信息。

2、根据权利要求 1 所述的电子标签的制作方法，其特征在于，所述的数字签名信息为经加/解密算法加密后的防伪源码信息。

3、根据权利要求 1 所述的电子标签的制作方法，其特征在于，所述的源码信息为固定信息和/或可变信息。

4、根据权利要求 3 所述的电子标签的制作方法，所述的可变信息为光模块的生产序列号和/或调试日期。

5、根据权利要求 1 所述的电子标签的制作方法，其特征在于，还包括：步骤 10：使用权限密码，赋予所述的读写寄存器的存取权限。

6、根据权利要求 5 所述的电子标签的制作方法，其特征在于，所述权限密码的入口地址为 A2H 的 120-127 字节。

7、根据权利要求 1 所述的电子标签的制作方法，其特征在于，所述的可插拔光模块的读写寄存器为地址 A2H 处的 128-247 字节。

8、根据权利要求 1 所述的电子标签的制作方法，其特征在于，所述的可插拔光模块为 ESFP、GBIC、XFP 以及 XENPAK。

9、一种电子标签的生成装置，所述的装置包括：

生成单元，用以产生所述电子标签中的防伪源码信息，以及经加/解密算法对所述的源码信息进行加密后的数字签名信息；

写入单元，用以将生成的源码信息和数字签名信息存入所述电子标签的读写寄存器中。

10、一种根据权利要求 1-8 任意一项所述方法制作的可插拔光模块的电子标签，其特征在于，包括：

电子标签存储单元，位于所述的可插拔光模块的读写寄存器中，其包含防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息。

11、根据权利要求 10 所述的可插拔光模块的电子标签，其特征在于，还包括：

权限密码存储单元，位于所述的可插拔光模块的寄存器中，其中，所述的权限密码用以赋予所述的读写寄存器的存取权限。

12、一种根据权利要求 10—11 任意一项所述的电子标签的识别方法，用以识别所述的可插拔光模块的真伪，其中，所述的电子标签的存储单元，位于所述的可插拔光模块的读写寄存器中，其包含防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息；其特征在于，包括：

步骤 21：从所述的电子标签存储单元中读出数字签名信息和源码信息；

步骤 22：用加/解密算法对所述的数字签名信息进行解密；

步骤 23：将解密后的结果信息与源码信息进行比较，判断所述的可插拔光模块的真伪。

13、根据权利要求 12 所述的电子标签的识别方法，其特征在于，所述的方法还包括：

步骤 20：赋予所述可插拔光模块的读写寄存器的存取权限。

14、根据权利要求 13 所述的电子标签的识别方法，其特征在于，所述的步骤 20 具体包括：

步骤 20-1：检测所述光模块的在位状态；

步骤 20-2：判断光模块是否在位；如果在位，执行步骤 20-3，否则，执行步骤 20-4；

步骤 20-3：根据存储权限密码入口地址写入的权限密码和/或所述光模块的在位状态控制位，赋予所述的读写寄存器的存取权限；

步骤 20-4：指示所述的光模块不在位。

15、根据权利要求 12 所述的电子标签的识别方法，其特征在于，还包括：

步骤 24：指示所述的可插拔光模块的真伪，关闭对所述可插拔光模块的读写寄存器的存储权限。

16、根据权利要求 14 所述的电子标签的识别方法，其特征在于，所述存取权限密码的入口地址为 A2H 的 120-127 字节。

17、根据权利要求 12 所述的电子标签的识别方法，其特征在于，所述的可插拔光模块的读写寄存器为地址 A2H 处的 128-247 字节。

18、一种根据权利要求 10-11 任意一项所述电子标签的识别装置，用以识别所述的可插拔光模块的真伪，其特征在于，包括：

读取单元，从所述的电子标签存储单元中读出数字签名信息和防伪源码信息；

解密单元：用加/解密算法对所述的数字签名信息进行解密；

识别单元，将解密后的结果信息与源码信息进行比较，判断所述的可插拔光模块的真伪。

19、根据权利要求 18 所述的电子标签的识别装置，其特征在于，所述的装置还包括：

检测单元，检测所述光模块的在位状态；

判断单元，根据检测结果，判断光模块是否在位；

权限处理单元，根据存储权限密码入口地址写入的权限密码和/或所述光模块的在位状态控制位，确定是否赋予所述读写寄存器的存取权限。

20、根据权利要求 18 所述的电子标签的识别装置，其特征在于，所述的可插拔光模块为 ESFP、GBIC、XFP 以及 XENPAK。

光模块的电子标签、制作和识别方法及识别装置

技术领域

本发明涉及一种光模块(Transceiver)的防伪技术,特别涉及一种可插拔(Small Form Pluggable,简称 SFP)光模块的电子标签、电子标签的制作方法、利用设备主机识别光模块的电子标签方法及其应用的识别装置。

背景技术

随着信息的传输和交换正向光网络发展,光纤通信成为现代信息网络的主要传输手段。人们对光纤通信网络的核心器件——光收发一体模块的需求也迅速增长。为了满足系统不断增长的需求,光模块正不断朝智能化、高速度和高密度互联的方向发展。

当前,光收发模块技术,智能 SFP 模块、增强型小封装可插拔模块(Enhanced Small Form-factor Pluggable,简称 ESFP),千兆以太网接口转换器(Gigabit Interface Converter,简称 GBIC),万兆以太网接口小封装可插拔光模块(10-Gigabit small Form-factor Pluggable transceiver,简称 XFP)、万兆以太网接口光模块集成封装(10 Gigabit Ether Net Transceiver Package,简称 XENPAK)以及并行光纤模块,成为了新一代光收发一体模块中的亮点。

小型封装可插拔光模块,采用先进的精密光学及电路集成工艺制作,尺寸只有普通双工 SC(1X9)型光纤收发模块的一半,因此,在同样空间可以增加一倍的光端口数,可以增加线路端口密度,降低每端口的系统成本;特别是光模块还支持热插拔功能,即无需切断电源,光模块即可以与设备主机连接或断开,网络管理人员无需关闭网络就可升级和扩展系统,对在线用户不会造成什么影响。

然而,在正常的光纤通信网络的运行过程中,总会产生一些不安全的隐患,如设备主机制造厂商在网络升级和扩展系统时,如果所选用的可插拔光模块不是本厂家所生产的产品,特别是所使用的光模块为一些

不合格厂家生产的假冒伪劣产品，这样，不仅损害了正规生产厂家的利益，而且，不能满足兼容性的要求，使整个系统没有任何可靠性可言，甚至无法正常进行。此外，如果系统发生故障时，最终用户不能够很好地使用和管理它们的光收发模块，同时，也增加了网络管理人员调试和维护工作的难度。

目前，光模块的防伪方案也就是在模块外壳上粘贴防伪标签（例如，条形码或激光防伪标签），并且，通过目测的方法来检测可插拔光模块的真伪，以达到防伪的目的。

然而，粘贴防伪标签的方案，从造假难度来讲，造假门槛比较低，伪造者可以很容易制造防伪标签，或者，通过购买防伪标签方式来达到仿造目的；并且，从成本上来讲，正规的设备生产厂家为了提高防伪标签的识别难度，在防伪标签上投入的制作成本也越来越高。因此，为了不断提高防伪标签的不可复制性（标识的唯一性），保证大量使用光模块设备的光纤通信网络的正常运行，减少维护成本，使用目测的方法来检测可插拔光模块的真伪，已不能满足设备制造商对防伪标签的识别难度和成本的要求。

发明内容

本发明的目的在于，提供一种可插拔光模块的防伪和设备主机的识别技术，该技术利用光模块内部具有用户的读写区域和厂家自定义区域的特点，即利用设备主机对光模块的读写区域有存取权限（密码保护）的特点，通过向光模块内部读写区域写入厂家特定信息，以及结合设备主机软件，来达到防伪目的。

基于上述目的，本发明提供一种电子标签的制作方法，所述的电子标签位于可插拔光模块中，包括：

步骤 11：将所述的可插拔光模块的读写寄存器划分出源码区域和数字签名区域；

步骤 12：在所述的源码区域存储可插拔光模块的防伪源码信息；

步骤 13：在所述的数字签名区域存储用以识别所述源码信息的数字签名信息。

根据所述的电子标签的制作方法，所述的数字签名信息为经加/解密算法加密后的防伪源码信息。

根据所述的电子标签的制作方法，所述的源码信息为固定信息和/或可变信息。

根据所述的电子标签的制作方法，所述的可变信息为光模块的生产序列号和/或调试日期。

根据所述的电子标签的制作方法还包括：步骤 10：使用权限密码，赋予所述的读写寄存器的存取权限。

根据所述的电子标签的制作方法，所述权限密码的入口地址为 A2H 的 120-127 字节。

根据所述的电子标签的制作方法，所述的可插拔光模块的读写寄存器为地址 A2H 处的 128-247 字节。

根据所述的电子标签的制作方法，所述的可插拔光模块为 ESFP、GBIC、XFP 以及 XENPAK。

本发明还提供一种电子标签的生成装置，所述的装置包括：生成单元，用以产生所述电子标签中的防伪源码信息，以及经加/解密算法对所述的源码信息进行加密后的数字签名信息；写入单元，用以将生成的源码信息和数字签名信息存入所述电子标签的读写寄存器中。

本发明还提供一种根据上述方法制作的可插拔光模块的电子标签，其包括：电子标签存储单元，位于所述的可插拔光模块的读写寄存器中，其包含防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息。

根据所述的可插拔光模块的电子标签，其还包括：权限密码存储单元，位于所述的可插拔光模块的寄存器中，其中，所述的权限密码用以赋予所述的读写寄存器的存取权限。

本发明又提供一种上述电子标签的识别方法，所述的电子标签适用于所述的可插拔光模块中；其中，所述的电子标签的存储单元，位于所述的可插拔光模块的读写寄存器中，其包含防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息；该方法包括：

步骤 21：从所述的电子标签存储单元中读出数字签名信息和源码信

息；

步骤 22：用加/解密算法对所述的数字签名信息进行解密；

步骤 23：将解密后的结果信息与源码信息进行比较，判断所述的可插拔光模块的真伪。

根据所述的电子标签的识别方法，所述的方法还包括：步骤 20：赋予所述可插拔光模块的读写寄存器的存取权限。

根据所述的电子标签的识别方法，所述的步骤 20 具体包括：

步骤 20-1：检测所述光模块的在位状态；

步骤 20-2：判断光模块是否在位；如果在位，执行步骤 20-3，否则，执行步骤 20-4；

步骤 20-3：根据存储权限密码入口地址写入的权限密码和/或所述光模块的在位状态控制位，赋予所述的读写寄存器的存取权限；

步骤 20-4：指示所述的光模块不在位。

根据所述的电子标签的识别方法，还包括步骤 24：指示所述的可插拔光模块的真伪，关闭对所述可插拔光模块的读写寄存器的存储权限。

根据所述的电子标签的识别方法，所述存取权限密码的入口地址为 A2H 的 120-127 字节。

根据所述的电子标签的识别方法，所述的可插拔光模块的读写寄存器为地址 A2H 处的 128-247 字节。

根据所述的电子标签的识别方法，所述的加/解密算法为 DES/3DES 或者 AES 算法。

本发明另又提供一种电子标签的识别装置，用以识别所述的可插拔光模块的真伪，包括：读取单元，从所述的电子标签存储单元中读出数字签名信息和防伪源码信息；解密单元：用加/解密算法对所述的数字签名信息进行解密；识别单元，将解密后的结果信息与源码信息进行比较，判断所述的可插拔光模块的真伪。

根据所述的电子标签的识别装置，所述的装置还包括：检测单元，检测所述光模块的在位状态；判断单元，根据检测结果，判断光模块是否在位；权限处理单元，根据存储权限密码入口地址写入的权限密码和/或所述光模块的在位状态控制位，确定是否赋予所述读写寄存器的存取

权限。

根据所述的电子标签的识别装置，所述的可插拔光模块为 ESFP、GBIC、XFP 以及 XENPAK。

使用本发明提供的可插拔光模块的防伪和设备主机的识别技术，利用 ESFP、GBIC、XFP 以及 XENPAK 等可插拔光模块在地址 A2H 处新增的 256 字节的 EEPROM 读写区域，写入厂家特定信息和数字签名信息，读写区域写入的数字签名，易于辨别是否有伪造产品出现，并且采用私有的密码控制访问 EEPROM 读写区域。因此，本发明在不增加任何成本的情况下，提高了光模块的仿造难度，保证了可插拔光模块的唯一性，减小了设备制造商的维护成本。

附图说明

图 1 为可插拔 ESFP 光模块的 EEPROM 的寄存器空间关系映射示意图；

图 2 为可插拔 ESFP 光模块的硬件管脚示意图；

图 3 为本发明电子标签制作方法的流程图；

图 4 为本发明电子标签识别方法的流程图；

图 5 为本发明的电子标签识别方法具体实施例的流程图。

具体实施方式

请参阅图 1 和图 2，图 1 为可插拔 ESFP 光模块的在地址 A0H 字段处的内容和地址 A2H 处 EEPROM 的寄存器空间关系映射示意图；图 2 为可插拔 ESFP 光模块的硬件管脚示意图。

如图所示，ESFP 光模块较 SFP 光模块除了定义在地址 A0H 字段处的内容外，还增加了一些与数字诊断有关的寄存器定义（这些寄存器在以前的规范中都为保留字段），并在地址 A2H 处又新增了一个 256 字节的存贮单元。这个新增存贮单元除了提供参数检测信息外，还定义了告警标志或告警条件，TX_FAULT、TX_DISABLE 和 RX_LOS 管脚的状态镜像，有限的数字控制能力和用户可写的存储单元。光模块的 A0H 字段在出厂前一般都由厂家写好，属性对用户来讲为只读，而 A2H 字段则部分地址对用户来说可读可写。具体的 A2H 地址空间寄存器详细定义如表 1 所示：

表 1

地址	内容
0...55	存放告警(ALARM)和预警(WARNING)门限值，目前包括 5 种参数的门限值（含上限和下限）：内部温度、工作电压、偏置电流、发送功率、接收功率。 占用地址 0...39，地址 40-55 保留用于未来增加参数。
56...95	采用外部校准时的校准常数。
96...119	实时诊断接口(24 bytes)，存放采集到的内部温度、工作电压、偏置电流、发送功率、接收功率的实时数据以及这些参数的告警和预警标志，实测参数存放在 96...105，告警标志存放在 112...113 的不同位上，预警标志存放在 116...117 的不同位上。 在字节 110 的 8 个 bit 上还分别存放了一些状态/控制信息，包括 TX Disable Digital State, Soft TX Disable, RX Rate Select State, Soft RX Rate Select, TX Fault Digital state, LOS, Data_Ready_Bar，按照 SFF-8472 的规定，这些是可选功能，厂家不一定全实现。
120...127	厂家自定(8 bytes)
128...247	用户可写的 EEPROM（120 个字节）
248...255	厂家自定(8 bytes)的控制函数，用户不应写入数据。

本发明涉及的可插拔光模块的电子标签，就是利用 A0h 和 A2h 相关寄存器的内容和 EEPROM 的寄存器空间，来制作光模块的防伪电子标签。光模块的电子标签的制作可以使用专用读写装置实现，也可以用设备主机完成；在本实施例中，所述的功能由设备主机中的软件实现。

请参阅图 3，图 3 本发明电子标签的制作方法的流程图；该制作方法包括：

步骤 10：使用权限密码，赋予所述的读写寄存器的存取权限。

步骤 11：将所述的可插拔光模块的读写寄存器划分出源码区域和数字签名区域；

步骤 12：在所述的源码区域存储可插拔光模块的防伪源码信息；

步骤 13：在所述的数字签名区域存储用以识别所述源码信息的数字签名信息。

上述步骤制作的光模块电子标签包括电子标签存储单元和权限密码存储单元。权限密码存储单元位于所述的可插拔光模块的寄存器中，例如，所述权限密码的入口地址为 A2H 的 120-127 字节；权限密码用以赋予设备主机或其它读写设备光模块读写寄存器的存取权限，使设备主机或其它读写设备能将厂家特定信息写入光模块内部的读写区域中。

电子标签存储单元位于可插拔光模块的读写寄存器（例如，表 1 中的地址 A2H 处 128-247 字节）中，设备主机厂商可以将该读写寄存器划分出防伪源码区域和数字签名区域，分别用以存储防伪源码信息和数字签名信息；源码信息为固定信息和/或可变信息，可变信息为光模块的生产序列号和/或调试日期；数字签名信息为经加/解密算法（例如为 DES/3DES 或者 AES 算法）加密后的防伪源码信息。

例如，防伪源码信息可以为 ESFP 光模块上的生产序列号和调测日期，格式为：“生产序列号（20 字节）+模块调测日期（8 字节）+1 字节空格+H3C(3 字节)”共 32 字节，经过加密处理后生成数字签名。例如，某光模块的生产序列号为 213410A0000054000251，光模块调测日期为 20061030，则生成的用于防伪源码信息为 213410A000005400025120061030 H3C；其中，20 字节的生产序列号，每个光模块有唯一的生产序列号，字段 A0000054000251 随着光模块种类和生产批次的不同而不同（可变信息）；8 字节的光模块调测日期，随着调测日期的不同而变化（可变信息）；H3C 为 4 字节为固定填充字符（固定信息）。源码 213410A000005400025120061030 H3C 经过对称加密算法 DES/3DES 或者 AES 算法加密处理后的数字签名信息为 34215876930210605279868941232691。

设备制造商可以在 ESFP 光模块在发货前对设备上进行全面的调测时，在 ESFP 光模块内部写入特定的防伪信息（例如上述的防伪源码信息和数字签名信息）。

电子标签的制作装置包括生成单元和写入单元；生成单元用以产生所述电子标签中的防伪源码信息，以及经加/解密算法对所述的源码信息进行加密后的数字签名信息；写入单元，用以将生成的源码信息和数字签名信息存入所述电子标签的读写寄存器中。

对 ESFP 光模块 A2H 的 128-247 字节的读写操作可以通过设置密码来限制存取权限，即设备制造商可以要求光模块厂商设置自己独特的密码，来限制其它人对可写区段的读写。在一般情况下，密码入口地址为 A2H 的 120-127 字节。假设，对 ESFP 光模块的可写字段 128-247 字节的控制密码为 1234，那么，ESFP 光模块 A2H 区域密码入口地址分配如表 2 所示：

表2

Byte	Bit	名称	说明
120-122	All	Reserved	保留
123	All	Password Byte 3	32 个 bit 密码的最高字节
124	All	Password Byte 2	32 个 bit 密码的次高字节
125	All	Password Byte 1	32 个 bit 密码的次低字节
126	All	Password Byte 0	32 个 bit 密码的最低字节
127	All	User EEPROM Select	写入 1 后可以访问字节 128-247

设备制造商从光模块厂商获得控制密码（1234）后，就可以使用设备主机或其它读写设备的写入功能将生成的源码信息和数字签名信息存入所述电子标签的读写寄存器中。在光模块调测时，设备主机通过控制程序将数字签名信息和生产序列号及调测日期存放到A2H可读写区域128-247的相关字节中，如表3所示。

表3

Byte	字节	名称	说明	举例
128-149	22	生产序列号	在生产调测阶段直接从模块上获取，ASCII 字符，预留 2 字节向后兼容	213410A0000054000251
150-157	8	模块调测日期	写入电子标签当天的日期，由装备取计算机当天的日期。ASCII 字符	20061030
158-189	32	数字签名域	由加密软件加密后生成的数字签名	34215876930210605279868941232691

由于每个光模块上的生产序列号是唯一的，并且是各不相同的，所以加密后的数字签名也将是唯一的且各不相同，即一个光模块对应一个唯一的数字签名，并且每个数字签名各不相同，因此，这样形成的光模块电子标签具有唯一性。

对于上述光模块电子标签的识别功能，同样可以使用专用电子标签的识别装置实现，也可以用设备主机完成；在本实施例中，所述的功能由设备主机中的软件实现。

请参阅图 4，图 4 本发明的电子标签的识别方法的流程图。在步骤 20 中，赋予了设备主机厂商对所述可插拔光模块的读写寄存器的存取权限。步骤 20 需执行的具体操作包括：

- 步骤 20-1：检测所述光模块的在位状态；
- 步骤 20-2：判断光模块是否在位；如果在位，执行步骤 20-3，否则，

执行步骤 20-4;

步骤 20-3: 根据存储权限密码入口地址写入的权限密码和/或所述光模块的在位状态控制位, 赋予所述的读写寄存器的存取权限;

步骤 20-4: 指示所述的光模块不在位。

请结合图 2 参阅图 4, 当光模块插入到设备主机中时, 由设备主机中的检测单元, 检测所述光模块的在位状态, 设备主机检测到光模块在位状态发生变化后, 设备主机中的判断单元根据检测结果, 判断光模块是否在位; 如果判断结果为光模块在位, 设备主机中的权限处理单元, 从存储权限密码入口地址写入权限密码和光模块的在位状态控制位, 取得 A2H 用户可写区域的操作权。

接下来, 在步骤 21 中, 从所述的电子标签存储单元中的读出数字签名信息和源码信息; 在步骤 22 中, 用加/解密算法对所述的数字签名信息进行解密; 在步骤 23 中, 将解密后的结果信息与源码信息进行比较, 判断所述的可插拔光模块的真伪; 在步骤 24 中, 指示所述的可插拔光模块的真伪, 关闭对所述可插拔光模块的读写寄存器的存储权限。

也就是说, 设备主机中的读取单元从电子标签存储单元中读出数字签名信息和防伪源码信息; 解密单元对读取的数字签名域的内容, 用加/解密 (例如 DES/3DES 或者 AES 算法) 对数字签名信息进行解密; 识别单元将解密后的结果信息与源码信息进行比较, 判断所述的可插拔光模块的真伪。

下面通过具体的实例来进一步说明解释本发明。

在本实例中, 假设光模块中的电子标签的防伪源码信息和数字签名信息如表 3 所示。请参阅附图 5, 图 5 为本发明的电子标签识别方法具体实施例的流程图。如图所示, 当光模块插入到设备主机中时, 光模块的在位信号管脚触发设备主机的 CPLD 或 CPU 中的相关寄存器值发生改变, 设备主机中的内部软件检测到光模块在位状态发生变化后, 设备主机通过其内部软件在密码入口地址(120-127 字节)写入正确的密码和控制位, 取得 A2H 用户可写区域的操作权, 然后, 设备主机中的内部软件在地址 A2H 的 123-126 字节写入密码 (例如 1234), 同时, 在 127 字节处写入 1; 并且, 经密码 1234 和控制位与其内部的私有密钥进行比对, 如果结

果相符合，就取得了设备主机厂商对字节 128-247 的控制权。

然后，设备主机中的内部软件读取地址 A2H 的 158-189 字节的数字签名域的内容 34215876930210605279868941232691，用加/解密 DES/3DES 或者 AES 算法对数字签名信息进行解密；并且，将解密结果中的前 20 字节与光模块 A2H 区域字节 128-149（生产序列号）中的内容进行比较，并且解密结果中的前 21-28 字节与光模块 A2H 区域字节 150-157（模块调测日期）的内容进行比较，如果两个结果均相同，则设备主机认为该光模块为可识别的合法光模块，如果有一个结果不相同，则主机认为该光模块为不可识别的非法光模块，并且，由主机控制台给用户发出告警信息，提示设备厂商该光模块不可识别。这样，客户就可以知道该光模块是否为伪造模块。

综上所述，本发明利用设备主机对光模块的读写区域有存取权限（密码保护）的特点，通过向光模块内部读写区域写入厂家特定信息，以及结合设备主机软件，实现了可插拔光模块的防伪需求。

需要声明的是，上述发明内容及具体实施方式意在证明本发明所提供技术方案的实际应用，不应解释为对本发明保护范围的限定。本领域技术人员在本发明的精神和原理内，当可作各种修改、等同替换、或改进。本发明的保护范围以所附权利要求书为准。

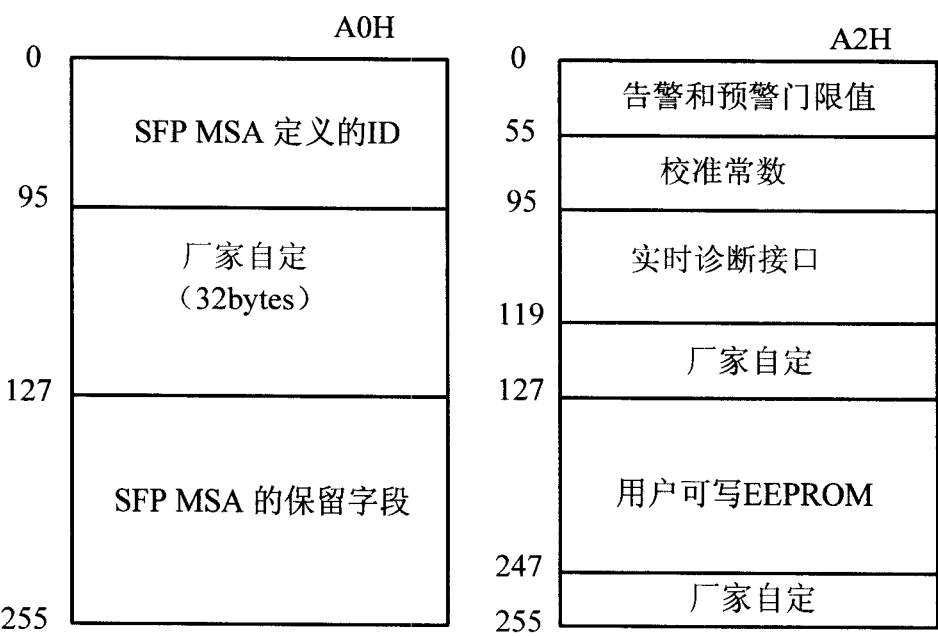


图 1

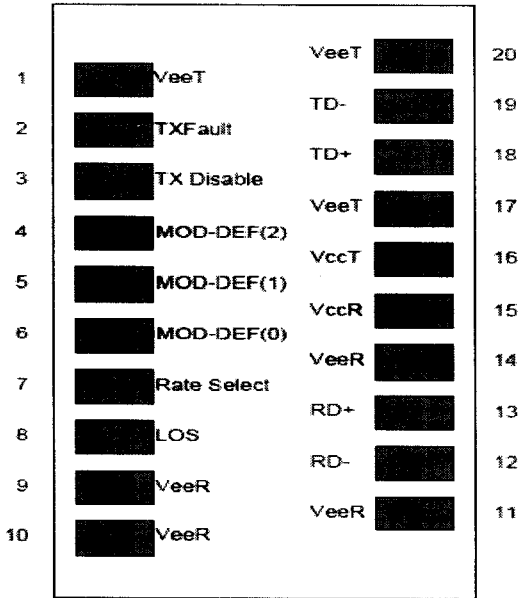


图 2

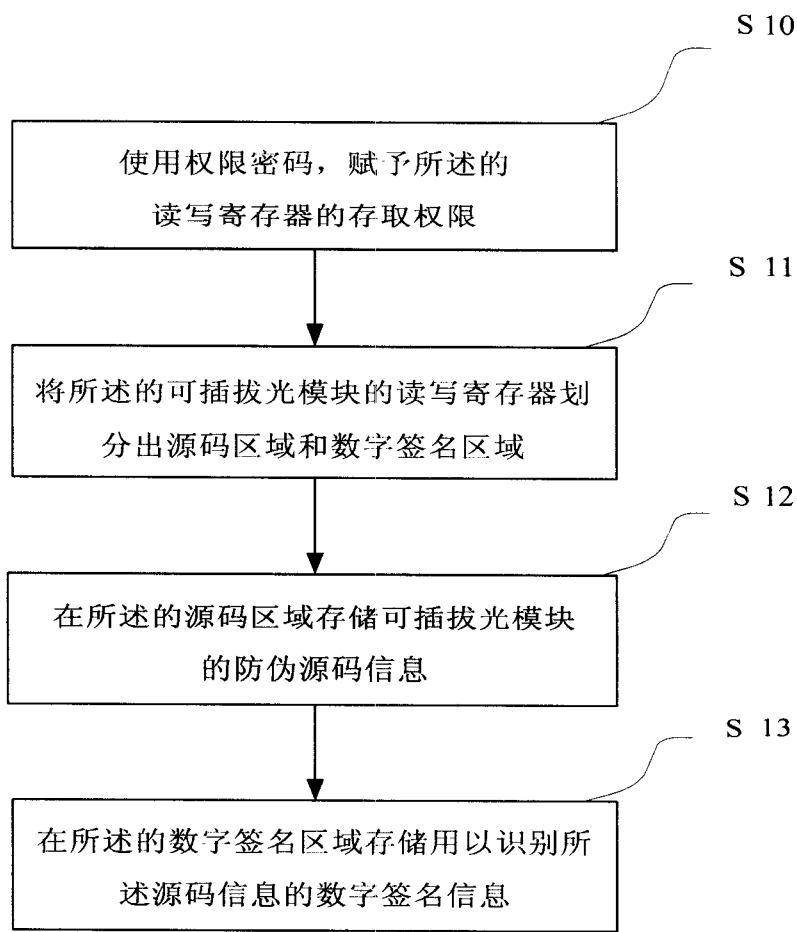


图 3

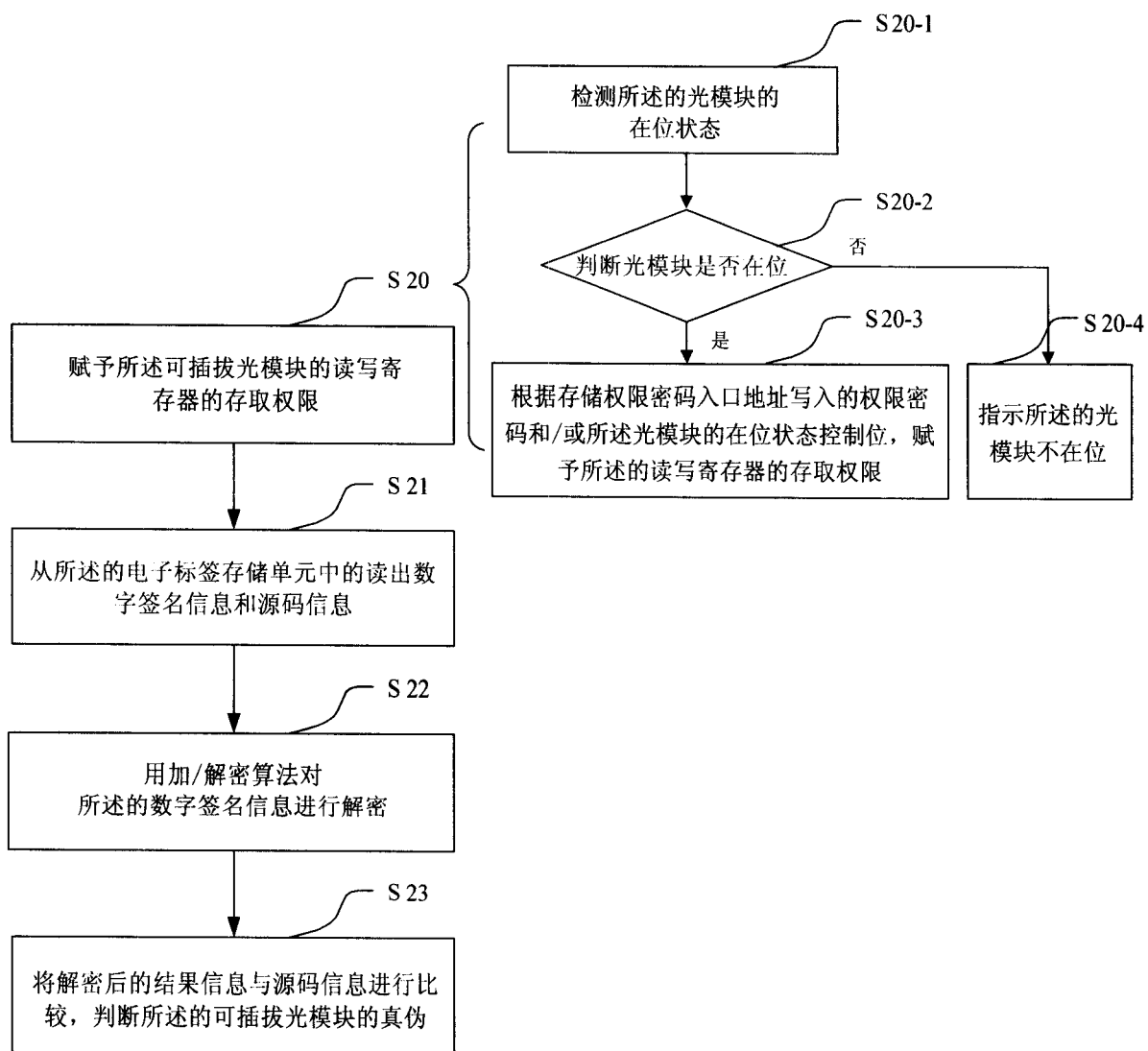


图 4

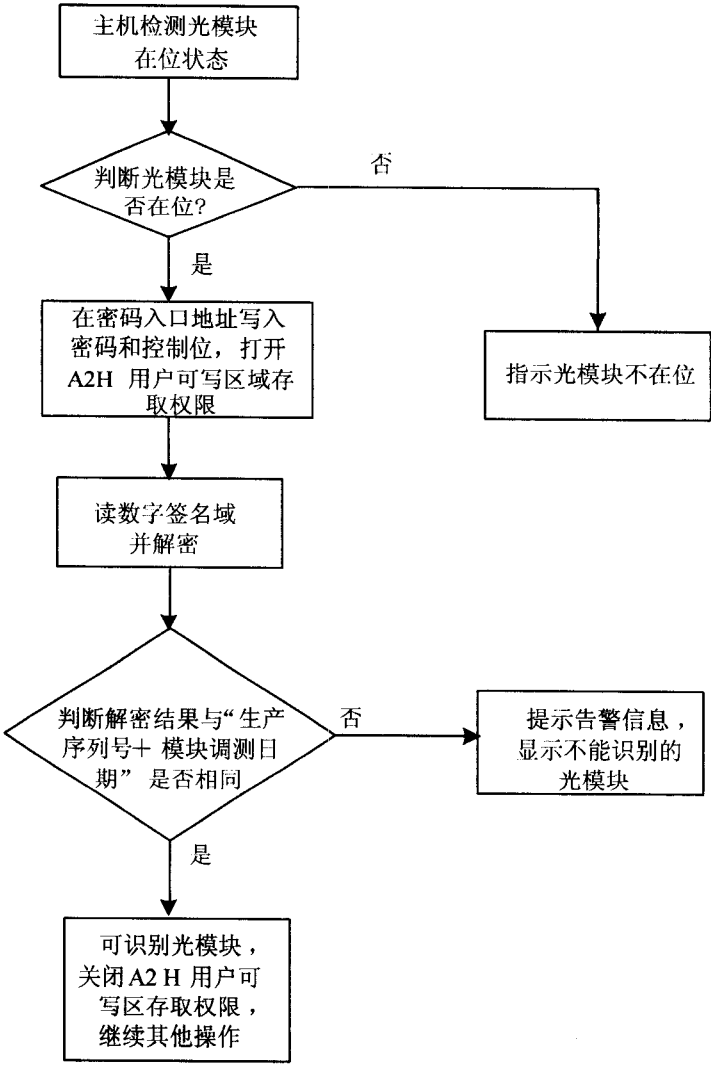


图 5