(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104618104 B
(45)授权公告日 2019.11.29

(21)申请号 201410779695.8

(22)申请日 2014.12.15

(65)同一申请的已公布的文献号
申请公布号 CN 104618104 A

(43)申请公布日 2015.05.13

(73)专利权人 惠州TCL移动通信有限公司
地址 516006 广东省惠州市仲恺高新区和畅七路西86号

(72)发明人 胡学龙 郭爱平 赵士青

(74)专利代理机构 深圳市威世博知识产权代理事务所(普通合伙) 44280
代理人 何青瓦

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)

(56)对比文件
CN 102045167 A,2011.05.04,
CN 101163014 A,2008.04.16,
EP 1580924 A2,2005.09.28,
US 2014270173 A1,2014.09.18,

审查员 赵冰

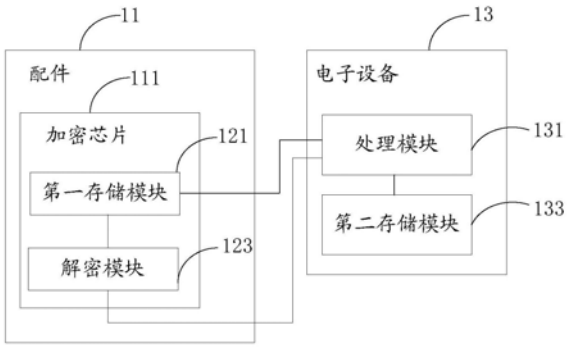
权利要求书2页 说明书6页 附图1页

(54)发明名称

配件、电子设备及实现配件认证的系统

(57)摘要

本发明公开了一种配件、电子设备及实现配件认证的系统，所述配件包括加密芯片，所述加密芯片包括第一存储模块，用于存储私有认证密钥以及至少由公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥，以使电子设备的处理模块在所述电子设备和所述配件进行物理连接时按照与所述预定规则匹配的算法从所述混合认证密钥中至少提取出所述公共认证密钥，并使用所述公共认证密钥对所述配件进行认证。通过上述方式，本发明能够提高密钥的安全性，以提高电子设备使用配件的安全性和可靠性。



CN 104618104 B

1.一种配件,其特征在于,包括加密芯片,所述加密芯片包括第一存储模块;

所述第一存储模块用于存储由私有认证密钥、公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥,以使电子设备的处理模块在所述电子设备和所述配件进行物理连接时按照与所述预定规则匹配的算法从所述混合认证密钥中提取出所述私有认证密钥以及所述公共认证密钥,并使用所述公共认证密钥对所述配件进行认证;

同时所述加密芯片还包括与所述第一存储模块连接的密钥产生模块,用于在所述配件和所述电子设备进行物理连接时产生所述私有认证密钥、公共认证密钥以及伪密钥,并将所述私有认证密钥、所述公共认证密钥以及所述伪密钥按照预定规则进行组合以得到所述混合认证密钥,其中,在每次所述配件和所述电子设备进行物理连接时,所述密钥产生模块产生的公共认证密钥和私有认证密钥不相同;

所述加密芯片还包括解密模块,所述解密模块用于接收所述处理模块按照与所述预定规则匹配的算法从所述混合认证密钥中提取出的所述私有认证密钥,并使用所述私有认证密钥对所述配件进行认证。

2.根据权利要求1所述的配件,其特征在于,

所述加密芯片还包括计数模块,所述计数模块用于累计并存储所述配件被认证的次数。

3.根据权利要求1所述的配件,其特征在于,

所述加密芯片具有唯一的序列号。

4.一种电子设备,其特征在于,包括处理模块;

所述处理模块用于在所述电子设备和配件进行物理连接时,从所述配件的加密芯片中的第一存储模块读取由私有认证密钥、公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥,并按照与所述预定规则匹配的算法从所述混合认证密钥中提取所述私有认证密钥以及所述公共认证密钥,以使用所述公共认证密钥对所述配件进行认证,同时所述处理模块还将所述私有认证密钥发送给所述配件中的解密模块,以使所述解密模块使用所述私有认证密钥对所述配件进行认证,

其中,所述私有认证密钥、所述公共认证密钥以及所述伪密钥是由所述配件的加密芯片中的与所述第一存储模块连接的密钥产生模块在所述配件和所述电子设备进行物理连接时产生的,且所述密钥产生模块将所述私有认证密钥、所述公共认证密钥和所述伪密钥按照预定规则进行组合以得到所述混合认证密钥,在每次所述配件和所述电子设备进行物理连接时,所述密钥产生模块产生的公共认证密钥和私有认证密钥不相同。

5.一种实现配件认证的系统,其特征在于,包括配件和电子设备,所述配件包括加密芯片,所述加密芯片包括第一存储模块以及与所述第一存储模块连接的密钥产生模块、解密模块,所述电子设备包括处理模块;

所述第一存储模块用于存储私有认证密钥、公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥;

所述密钥产生模块用于在所述配件和所述电子设备进行物理连接时产生所述私有认证密钥、公共认证密钥以及伪密钥,并将所述私有认证密钥、所述公共认证密钥和伪密钥按照预定规则进行组合以得到所述混合认证密钥,其中,在每次所述配件和所述电子设备进行物理连接时,所述密钥产生模块产生的公共认证密钥和私有认证密钥不相同;

所述处理模块在所述配件和所述电子设备进行物理连接时按照与所述预定规则匹配的算法从所述混合认证密钥中提取出所述私有认证密钥以及所述公共认证密钥，并使用所述公共认证密钥对所述配件进行认证以及将所述私有认证密钥发送给所述配件。

6.根据权利要求5所述的系统，其特征在于，

所述加密芯片还包括计数模块，所述计数模块用于累计并存储所述配件被认证的次数。

配件、电子设备及实现配件认证的系统

技术领域

[0001] 本发明涉及电子技术领域，特别是涉及一种配件、电子设备及实现配件认证的系统。

背景技术

[0002] 电子设备例如手机或平板等在日常使用过程中，常常会用到相关的配件(包括附件)，例如需要和充电器连接以进行充电，和数据线连接以进行数据传输，和耳机连接以进行接听等。

[0003] 但是，当电子设备在连接并使用配件时，如果配件的质量不合格，有可能会损坏电子设备，甚至会引起人身伤亡等重大事故的发生。并且，越来越多的非正规厂家为了谋取暴利而使用劣质材料或不严格的工艺制程来生产配件，导致配件的质量难以得到保证，一旦使用这些非法厂家生产的不合格配件，更容易损坏电子设备，或者造成重大伤亡事故。据资料显示，由于使用不合格的充电器充电时发生漏电致人死亡或导致电子设备损坏、燃烧等事件时有发生，给电子设备用户带来了极大的风险和安全隐患。

[0004] 为了解决上述技术问题，现有技术中，在电子设备使用配件之前，通常先对配件进行认证以确认配件是否为合法配件。当配件通过认证时，则电子设备正常使用配件的功能，如果配件认证失败，则电子设备与配件不进行功能性连接，即不使用该配件，由此确保电子设备能够使用合法的配件。现有对配件的认证方法中，通常采用非对称加密算法对配件进行认证。非对称加密算法中需要两个密钥，公钥和私钥，当采用公钥进行加密时，只有通过配对的私钥才能进行解密，当采用私钥进行加密时，只有配对的公钥才能够解密。公钥是对外公开的，而私钥只有解密方知道。

[0005] 然而，公钥和私钥一般都是直接存储至存储器中的安全部分，即现有技术中通常不会对公钥和私钥进行任何处理，使用公钥和私钥进行加解密时只需要从存储器中直接获取即可，这种存储方式使得公钥和私钥的安全级别降低，极容易被黑客破解密钥，尤其是公钥一旦被黑客破解，将可能导致配件的整个认证发生错误，有可能出现将不合法的配件认证为合法配件的现象。

发明内容

[0006] 本发明主要解决的技术问题是提供一种配件、电子设备及实现配件认证的系统，能够提高密钥的安全级别，以提高电子设备使用配件时的安全性和可靠性。

[0007] 为解决上述技术问题，本发明采用的一个技术方案是：提供一种配件，包括加密芯片，所述加密芯片包括第一存储模块；所述第一存储模块用于存储私有认证密钥以及至少由公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥，以使电子设备的处理模块在所述电子设备和所述配件进行物理连接时按照与所述预定规则匹配的算法从所述混合认证密钥中至少提取出所述公共认证密钥，并使用所述公共认证密钥对所述配件进行认证。

[0008] 其中，所述加密芯片还包括与所述第一存储模块连接的密钥产生模块，用于在所述配件和所述电子设备进行物理连接时产生所述私有认证密钥、公共认证密钥以及伪密钥，并至少将所述公共认证密钥和伪密钥按照预定规则进行组合以得到所述混合认证密钥，其中，在每次所述配件和所述电子设备进行物理连接时，所述密钥产生模块产生的公共认证密钥和私有认证密钥不相同。

[0009] 其中，所述加密芯片还包括解密模块；所述密钥产生模块用于将所述私有认证密钥、所述公共认证密钥以及所述伪密钥按照预定规则进行组合以得到所述混合认证密钥，并将所述混合认证密钥存储至所述第一存储模块中；所述解密模块用于接收所述处理模块按照与所述预定规则匹配的算法从所述混合认证密钥中提取出的所述私有认证密钥，并使用所述私有认证密钥对所述配件进行认证。

[0010] 其中，所述加密芯片还包括计数模块，所述计数模块用于累计并存储所述配件被认证的次数。

[0011] 其中，所述加密芯片具有唯一的序列号。

[0012] 为解决上述技术问题，本发明采用的另一个技术方案是：提供一种电子设备，包括处理模块，所述处理模块用于在所述电子设备和配件进行物理连接时，从所述配件的加密芯片中的第一存储模块读取至少由公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥，并按照与所述预定规则匹配的算法从所述混合认证密钥中至少提取所述公共认证密钥，以使用所述公共认证密钥对所述配件进行认证。

[0013] 为解决上述技术问题，本发明采用的另一个技术方案是：提供一种实现配件认证的系统，包括配件和电子设备，所述配件包括加密芯片，所述加密芯片包括第一存储模块，所述电子设备包括处理模块；所述第一存储模块用于存储私有认证密钥以及至少由公共认证密钥和伪密钥按照预定规则组合之后的混合认证密钥；所述处理模块在所述配件和所述电子设备进行物理连接时按照与所述预定规则匹配的算法从所述混合认证密钥中至少提取出所述公共认证密钥，并使用所述公共认证密钥对所述配件进行认证。

[0014] 其中，所述加密芯片还包括与所述第一存储模块连接的密钥产生模块，用于在所述配件和所述电子设备进行物理连接时产生所述公共认证密钥、私有认证密钥以及伪密钥，并至少将所述公共认证密钥和伪密钥按照预定规则进行组合以得到所述混合认证密钥，其中，在每次所述配件和所述电子设备进行物理连接时，所述密钥产生模块产生的公共认证密钥和私有认证密钥不相同。

[0015] 其中，所述加密芯片还包括解密模块；所述密钥产生模块用于将所述私有认证密钥、所述公共认证密钥以及所述伪密钥按照预定规则进行组合以得到所述混合认证密钥，并将所述混合认证密钥存储至所述第一存储模块中；所述处理模块用于按照与所述预定规则匹配的算法从所述混合认证密钥中提取所述私有认证密钥，并将所述私有认证密钥发送给所述解密模块，所述解密模块用于接收所述私有认证密钥，并使用所述私有认证密钥对所述配件进行认证。

[0016] 其中，所述加密芯片还包括计数模块，所述计数模块用于累计并存储所述配件被认证的次数。

[0017] 本发明的有益效果是：区别于现有技术的情况，本发明的配件中配置有加密芯片，加密芯片用于存储私有认证密钥以及至少由公共认证密钥和伪密钥按照预定规则组合之

后的混合认证密钥，从而使得电子设备在和配件进行物理连接时，需先按照与预定规则匹配的算法从混合认证密钥中提取出公共认证密钥，才能使用公共认证密钥对配件进行认证，通过将公共认证密钥和伪密钥混合在一起，利用伪密钥将公共认证密钥进行隐藏，由此可减小密钥被黑客破解的几率，有利于提高密钥的安全级别。

附图说明

[0018] 图1是本发明实现配件认证的系统一实施方式的结构示意图；

[0019] 图2是本发明实现配件认证的系统另一实施方式的结构示意图。

具体实施方式

[0020] 下面将结合附图和具体的实施方式对本发明进行详细说明。

[0021] 参阅图1，本发明实现配件认证的系统一实施方式中，包括配件11和电子设备13。其中，配件11可以为充电器、数据线、耳机等，电子设备13可以是手机、平板电脑或其他电子设备。

[0022] 配件11包括加密芯片111，以实现对配件的加密功能。加密芯片111包括第一存储模块121和解密模块123，第一存储模块121用于存储私有认证密钥以及由公共认证密钥和伪密钥组合之后的混合认证密钥。本实施方式中，采用非对称加密算法和真假密钥的方法同时对配件11进行加密。非对称加密算法需要两个密钥，即公共认证密钥和私有认证密钥。公共认证密钥和私有认证密钥为一对验证密钥对，若使用公共认证密钥进行加密，则只能使用对应的私有认证密钥才能解密，若使用私有认证密钥进行加密，则只能使用对应的公共认证密钥才能解密。

[0023] 其中，第一存储模块121所存储的混合认证密钥是将公共认证密钥和伪密钥按照预定规则进行混合后得到的密钥数据。

[0024] 本实施方式中，公共认证密钥和伪密钥的组合方式为将公共认证密钥和多个伪密钥进行排列，例如真的公共认证密钥为A，伪密钥有B1、B2、B3、B4，可以将A、B1、B2、B3、B4五个密钥按照一定的顺序进行排列，如将A排在第三位，即五个密钥的排列顺序为B1、B2、A、B3、B4，然后将排列组合后得到的数据存储至第一存储模块201中以得到混合认证密钥。

[0025] 电子设备13包括处理模块131。处理模块131用于在电子设备13和配件11进行物理连接(即电性连接，实现功能性连接前)时，从第一存储模块121中读取混合认证密钥，并按照预定算法从混合认证密钥中提取公共认证密钥，并使用公共认证密钥验证配件是否为合法配件。电子设备13和配件11之间的连接可以是有线连接(例如通过USB通道进行连接)也可以是无线连接。

[0026] 其中，预定算法为和所述预定规则相匹配的算法，该算法和该预定规则可以是电子设备厂商和合法的配件厂商进行协商制定，该预定规则仅是被电子设备厂商和合法的配件厂商所知。以上述公共认证密钥A和四个伪密钥B1、B2、B3、B4的组合方式为例，公共认证密钥A和伪密钥的组合方式应是按照B1、B2、A、B3、B4的方式进行排列，从而处理模块301只需根据预先制定好的规则从混合认证密钥中提取第三位密钥，即可得到真的公共认证密钥。通过将真的公共认证密钥混合在伪密钥中，利用伪密钥对真的公共认证密钥进行隐藏，因此除非是获知公共认证密钥和伪密钥的组合方式，否则将难以获知哪一个才是真的公共

认证密钥，由此提高了公共认证密钥的安全级别，使得黑客难以发现真的公共认证密钥，降低了密钥被黑客破解的几率，以确保密钥的可靠性。

[0027] 为了进一步确定所使用公共认证密钥是正确的，即确认公共认证密钥没有被篡改过，电子设备13还包括第二存储模块133，用于存储公共验证密钥，该公共验证密钥为和私有认证密钥为一对验证密钥对。处理模块131从混合认证密钥中获取公共认证密钥后，使用公共验证密钥对公共认证密钥进行验证，即将公共认证密钥和公共验证密钥进行比较，当公共认证密钥和公共验证密钥相一致时，则该公共认证密钥被验证为正确的公共认证密钥，从而处理模块131使用被验证后的公共认证密钥对配件进行认证。

[0028] 在认证过程中，处理模块131使用公共认证密钥对消息进行加密，并将加密后的消息发送给配件11。配件11的解密模块123接收该加密后的消息，并使用私有认证密钥对接收到的消息进行解密，然后将解密的消息作为响应发送给处理模块131。处理模块131确定该响应是否适当，若适当，则配件11被认证为合法的配件。从而，在认证配件11为合法的配件后，电子设备13和配件11由物理性连接变为功能性连接，电子设备13正常使用配件11的功能，例如进行充电、传输数据等。如果配件11不被认证，则配件11被禁用。由此，在使用配件11之前先对配件11进行认证，以确认配件11是否为原装或合法的配件，在确认为原装或合法的配件后，方使用配件11的功能，从而确保电子设备13所使用的配件为合法配件，进而提高电子设备13使用配件11的安全性和可靠性。

[0029] 其中，在认证过程中的加解密的数据通道可以利用电子设备13和配件11现有的连接通道实现。电子设备13通常设有外部通信接口，如USB、UART等，电子设备13和配件11之间可以使用现有的通信接口进行密钥、数据和控制指令等的数据传输，以充分利用现有的资源实现对配件11的认证。

[0030] 因此，本实施方式中，通过对配件11配置加密芯片111，以使得配件11具有加密功能，以实现对配件11的认证，不仅能够提高电子设备13使用配件11的安全性，且采用伪密钥将真的公共认证密钥进行隐藏的加密算法，可以提高密钥的安全级别，防止真的密钥被黑客破解。此外，通过加密芯片111，还可以实现对配件11的跟踪、识别好判断等，便于对配件11进行管理。

[0031] 在本发明实现配件认证的系统的其他实施方式中，公共认证密钥和伪密钥还可以按照其他预定规则进行组合，例如将组成公共认证密钥的数据混合至伪密钥中，然后电子设备提取预定位置的数据，并进行重新组合以得到公共认证密钥。举例而言，假设公共认证密钥为1100，伪密钥为2222，将公共认证密钥的四位数按照预定位置混合至伪密钥的四位数中得到一串八位数据，该八位数据例如为12212020，此时电子设备按照预定算法提取第一位、第四位、第六位以及第八位数字，并将所提取出的数字进行重新组合从而得到公共认证密钥。由于黑客难以获知公共认证密钥和伪密钥之间的组合规则，因此难以找到真的公共认证密钥，由此提高了密钥的安全级别，降低被黑客破解的几率。

[0032] 此外，在其他实施方式中，也可以将私有认证密钥混合到伪密钥中，即第一存储模块用于存储由私有认证密钥、公共认证密钥和伪密钥按照预定规则进行组合之后的混合认证密钥。此时，当配件和电子设备进行物理性连接时，电子设备的处理模块按照预定算法从混合认证密钥中提取出公共认证密钥和私有认证密钥，并将私有认证密钥发送给解密模块，从而解密模块利用该私有认证密钥进行解密，以实现对配件的认证。通过上述方式，可

以防止公共认证密钥和私有认证密钥被黑客破解，提高密钥的安全级别。

[0033] 本发明实现配件认证的系统的另一实施方式中，采用随机的密钥对配件进行认证，以提高认证的可靠性，进一步确保电子设备所使用的配件为合法的配件。具体地，参阅图2，加密芯片211还包括与第一存储模块221连接的密钥产生模块225。密钥产生模块225用于在配件21和电子设备23进行物理连接时产生私有认证密钥、公共认证密钥以及伪密钥，并至少将公共认证密钥和伪密钥按照预定规则进行组合以得到混合认证密钥。其中，本实施方式中，密钥产生模块225用于将私有认证密钥、公共认证密钥和伪密钥按照预定规则进行组合以得到混合认证密钥，第一存储模块221用于存储由私有认证密钥、公共认证密钥和伪密钥组合之后的混合认证密钥。

[0034] 此外，密钥产生模块225以随机产生密钥的方式产生公共认证密钥和私有认证密钥，即在每次配件21和电子设备23进行物理连接时，密钥产生模块225产生的私有认证密钥和公共认证密钥不相同。例如，在配件21和电子设备23第一次进行物理连接时，密钥产生模块225产生的一对私有认证密钥和公共认证密钥为CD，在配件21和电子设备23第二次进行物理连接时，密钥产生模块225产生的一对私有认证密钥和公共认证密钥为与密钥对CD不同的EF密钥对。

[0035] 进一步地，密钥产生模块225在每次产生密钥对时，产生的方式也不相同，其可以根据配件21被认证的次数来产生私有认证密钥和公共认证密钥，还可以根据当前时间来产生私有认证密钥和公共认证密钥。由此，通过将非对称加密算法、真假密钥算法和随机密钥算法同时用于对配件的加密，可使得黑客难以找到密钥，也无从找到密钥产生的规律，进而进一步提高密钥的安全性，有效地防止密钥被黑客攻击。

[0036] 本实施方式中，在对配件21进行认证时，电子设备23的处理模块231从第一存储模块221中读取混合认证密钥，并按照与所述的预定规则相匹配的算法从混合认证密钥中提取出公共认证密钥和私有认证密钥，并将私有认证密钥发送给解密模块223。之后，处理模块231使用公共验证密钥对提取出的公共认证密钥进行验证，在公共认证密钥被验证后，处理模块231使用公共认证密钥对消息进行加密，并将加密后的消息发送给解密模块223。解密模块223使用处理模块231发送过来的私有认证密钥对接收到的加密的消息进行解密，并将解密后的消息作为响应发送给处理模块231。处理模块231确定该响应是否正确，若正确，则配件21被认证，电子设备23正常使用配件21的功能，否则，配件21将被禁止，由此确保了电子设备23使用的配件21为合法配件，提高安全性和可靠性。

[0037] 当然，在其他实施方式中，还可以是由解密模块223从第一存储模块221中读取混合认证密钥，并从混合认证密钥中提取出私有认证密钥，以使用私有认证密钥进行解密；或者也可以是由解密模块223从混合认证密钥中提取出公共认证密钥和私有认证密钥，并将公共认证密钥发送给处理模块231，以使处理模块231使用该公共认证密钥对配件21进行认证。

[0038] 继续参阅图2，在本实施方式中，加密芯片211进一步还包括计数模块227。计数模块227用于累计并存储配件21被认证的次数。具体地，当解密模块223发生解密事件时，计数模块227在检测到解密模块223的解密事件后即加“1”，由此实现对认证次数的累计。电子设备23处理模块231可以通过读取配件21被认证的次数，以根据该被认证的次数进行相关处理，例如，可以根据被认证的次数获知配件21被使用的次数，进而进行收费管理，还可以根

据被认证的次数计算配件21的寿命等。

[0039] 此外，计数模块227还可以用于累计配件21的使用时长，以确定配件21的大约寿命。

[0040] 在本发明实现配件认证的系统的实施方式中，配件的加密芯片还具有唯一的序列号，以便于对配件进行管理和真伪识别。电子设备在使用密钥对配件进行人证之前，处理模块可以通过获取加密芯片的序列号来辨别配件是否是假冒伪略产品，例如可以通过网络云端将获取的序列号和正确的序列号进行比对以判定获取的序列号的真伪，并且在识别真伪后还可以对该序列号进行标注和管理，由此通过所标注的信息即可快速判断出序列号的真假。

[0041] 因此，通过为加密芯片配置唯一的序列号，从而保障配件的唯一性和排他性，为后续的配件认证增加了一道硬件屏障。

[0042] 本发明还提供配件的一实施方式，所述配件为上述任一实施方式中所描述的配件。

[0043] 本发明还提供电子设备的一实施方式，所述电子设备为上述任一实施方式中所描述的电子设备。

[0044] 以上所述仅为本发明的实施方式，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

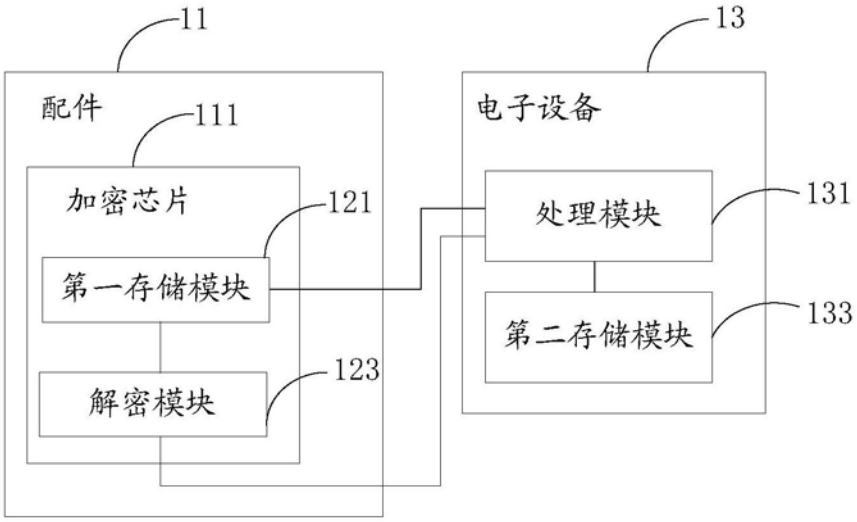

11
配件
111
加密芯片
121
第一存储模块
解密模块
123
13
电子设备
处理模块
131
第二存储模块
133

图1

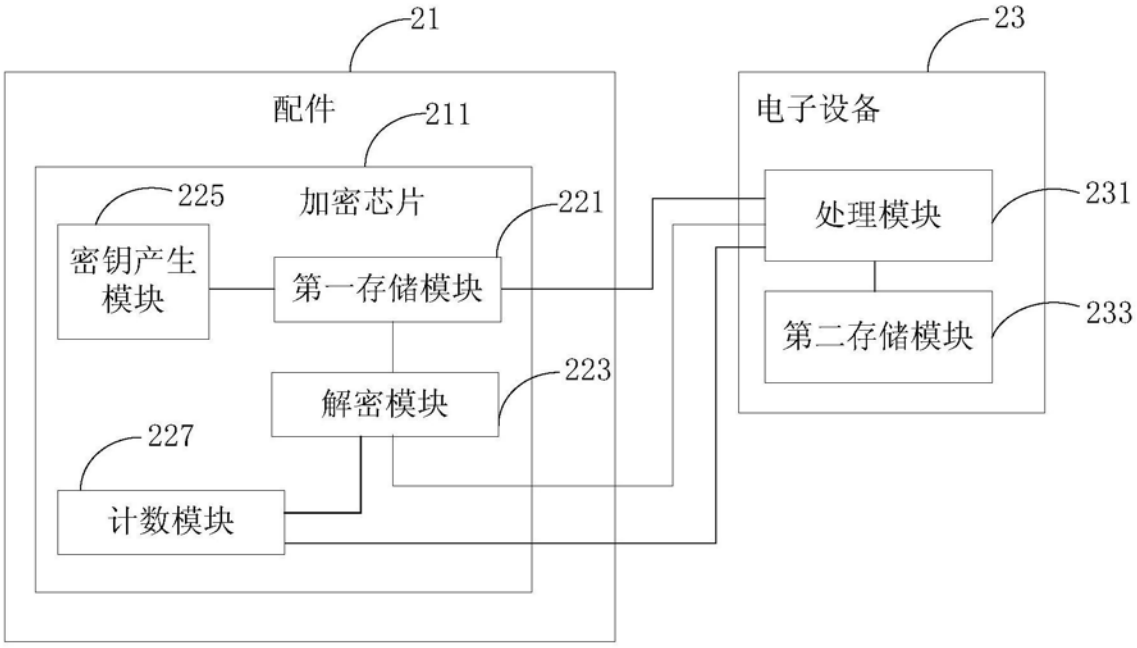

21
配件
211
加密芯片
225
密钥产生模块
221
第一存储模块
解密模块
223
227
计数模块
23
电子设备
处理模块
231
第二存储模块
233

图2