(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 105933112 B
(45)授权公告日 2020.04.21

(21)申请号 201610383825.5

(22)申请日 2016.06.01

(65)同一申请的已公布的文献号
申请公布号 CN 105933112 A

(43)申请公布日 2016.09.07

(73)专利权人 深圳市证通电子股份有限公司
地址 518000 广东省深圳市南山区南油天安工业村八座3A单元

(72)发明人 秦云川 万新

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
CN 101047978 A,2007.10.03,
CN 101877157 A,2010.11.03,
CN 105450620 A,2016.03.30,
CN 101981864 A,2011.02.23,
WO 2009/133869 A1,2009.11.05,
朱欣荣.《银行前置系统的模块化设计与优化》.《中国优秀硕士学位论文全文数据库信息科技辑》.2012,(第8期),

审查员 张洁

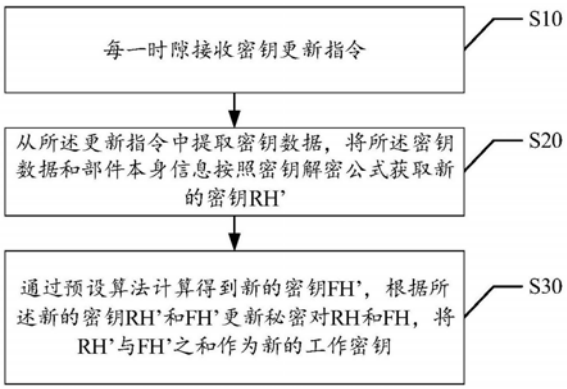
权利要求书2页 说明书8页 附图5页

(54)发明名称

无人值守终端的密钥更新方法及装置

(57)摘要

本发明公开了一种无人值守终端的密钥更新方法,包括步骤:终端部件每一时隙接收密钥管理中心下发的密钥更新指令;从所述更新指令中提取密钥数据;将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH',通过预设算法计算得到新的密钥FH',根据所述新的密钥RH'和FH'更新秘密对RH和FH,将RH'和FH'之和作为新的工作密钥。本发明还公开了一种无人值守终端的密钥更新装置。本发明降低了密钥被读取和窃取的风险,提高了密钥的安全性及密钥管理的效率,进而提高了部件与无人值守终端通信的安全性。



CN 105933112 B

1.一种无人值守终端的密钥更新方法,其特征在于,包括步骤:

每一时隙接收密钥管理中心下发的密钥更新指令;

从所述更新指令中提取密钥数据,将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH',所述部件本身信息包括当前周期的秘密值;

通过单相哈希算法FH'=H(FH)计算得到新的密钥FH',根据所述新的密钥RH'和FH'更新秘密对RH和FH,将RH'与FH'之和作为新的工作密钥;

所述获取新的密钥RH'的步骤之后,还包括:

对所述新的密钥RH'进行一次哈希运算进行验证,以验证所述新的密钥RH'是否来自密钥管理中心;

在验证通过后,判定所述新的密钥RH'来自密钥管理中心,为有效密钥;

其中,所述秘密值的生成方式包括:

由密钥管理中心按照正向哈希算法加密随机数生成F组密钥,由密钥管理中心按照反向哈希算法加密随机数生成R组密钥;

根据部件本身信息按照预设公式计算部件的秘密值;

在部件初始化时,按照部件的标识信息ID向部件注入F组密钥初始值FH、R组密钥初始值RH和各时隙相应的秘密值。

2.如权利要求1所述的无人值守终端的密钥更新方法,其特征在于,所述将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH'的步骤包括:

获取密钥数据中密钥管理中心下发的多项式系数信息;

将多项式系数信息及部件本身信息代入解密公式获取到新的密钥RH'。

3.如权利要求1所述的无人值守终端的密钥更新方法,其特征在于,所述方法还包括:

在部件接收到攻击操作后,自动删除部件所存储的秘密信息,所述秘密信息包括秘密对FH、RH,秘密值和新的工作密钥。

4.一种无人值守终端的密钥更新装置,其特征在于,包括:

接收模块,用于每一时隙接收密钥管理中心下发的密钥更新指令;

提取模块,用于从所述更新指令中提取密钥数据;

计算模块,用于将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH',通过单相哈希算法FH'=H(FH)计算得到新的密钥FH',所述部件本身信息包括当前周期的秘密值;

更新模块,用于根据所述新的密钥RH'和FH'更新秘密对RH和FH,将RH'与FH'之和作为新的工作密钥;

还包括:

验证模块,用于对所述新的密钥RH'进行一次哈希运算进行验证,以验证所述新的密钥RH'是否来自密钥管理中心;在验证通过后,判定所述新的密钥RH'来自密钥管理中心,为有效密钥;

所述秘密值的生成方式包括:由密钥管理中心按照正向哈希算法加密随机数生成F组密钥,由密钥管理中心按照反向哈希算法加密随机数生成R组密钥;根据部件本身信息按照预设公式计算部件的秘密值;在部件初始化时,按照部件的标识信息ID向部件注入F组密钥初始值FH、R组密钥初始值RH和各时隙相应的秘密值。

5.如权利要求4所述的无人值守终端的密钥更新装置,其特征在于,所述计算模块,还用于获取密钥数据中密钥管理中心下发的多项式系数信息;将多项式系数信息及部件本身信息代入解密公式获取到新的密钥RH'。

6.如权利要求4所述的无人值守终端的密钥更新装置,其特征在于,还包括:

删除模块,用于在部件接收到攻击操作后,自动删除部件所存储的秘密信息,所述秘密信息包括秘密对FH、RH,秘密值和新的工作密钥。

无人值守终端的密钥更新方法及装置

技术领域

[0001] 本发明涉及终端密钥管理技术领域，尤其涉及无人值守终端的密钥更新方法及装置。

背景技术

[0002] 随着社会的发展，金融业、出入境、医院、零售等各种终端随处可见，为生活和工作等方面带来很多便捷服务。随着人们安全意识的增加，金融行业终端信息的安全，也得到越来越多人的关注。一般终端都是通过工控主板控制各类外接部件，外接的与金融服务相关的敏感部件往往是攻击者的首选，而对于无人值守的终端设备，攻击者有相对充足的时间对设备部件进行攻击，比较容易窃取、篡改通信信息。如在终端输入个人密码(PIN)时有可能被攻击者截取到密码，发卡类的设备有可能被攻击者篡改信息发放伪造卡。目前信息传输前都进行了加密，来提高通信的安全性，常采用的密钥管理方法有两种，一种是非对称密钥加密管理，另一种是对称密钥加密管理。

[0003] 非对称密钥管理需要在主控板与每一设备形成一个公、私密钥对，加密算法复杂，加密和解密的速度比较慢。每一设备需要对应一套公、私密钥，当外设数量越来越多管理度越高，不能进行高效的密钥管理。

[0004] 对称算法要求通信双方共享一个秘密数据作为加密密钥，对密钥的管理与交换变得稍微复杂。目前对称密钥体系中较常使用的是密钥分散算法，利用多个分散因子完成密钥分散操作。密钥分散技术相对复杂和繁琐，自身实现的分散衍生算法安全性不能得到保障；分散过程中参与的分散因子数量众多，不利于密钥分散的可操作性。另外，通过上述密钥分散技术，可能会导致相同的密钥和分散因子衍生出不同的密钥，或者不同的密钥和分散因子衍生出相同的密钥，因此存在较大的安全隐患。

[0005] 综上所述，现有密钥技术在自助终端中多个部件共享下载密钥导致密钥容易被读出，安全性差及管理效率差。

[0006] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0007] 本发明的主要目的在于提供一种无人值守终端的密钥更新方法及装置，旨在解决现有密钥技术在自助终端中多个部件共享下载密钥导致密钥容易被读出，安全性差的问题。

[0008] 为实现上述目的，本发明提供的一种无人值守终端的密钥更新方法，包括步骤：

[0009] 每一时隙接收密钥更新指令；

[0010] 从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH’；

[0011] 通过预设算法计算得到新的密钥FH’，根据所述新的密钥RH’和FH’更新秘密对RH

和FH，将RH’与FH’之和作为新的工作密钥。

[0012] 优选地，所述方法还包括：

[0013] 由密钥管理中心按照正向哈希算法加密随机数生成F组密钥，由密钥管理中心按照反向哈希算法加密随机数生成R组密钥；

[0014] 根据部件本身信息按照预设公式计算部件的秘密值；

[0015] 在部件初始化时，按照部件的标识信息ID向部件注入F组密钥初始值和各时隙相应的秘密值。

[0016] 优选地，所述将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH’的步骤包括：

[0017] 获取密钥数据中密钥管理中心下发的多项式系数信息；

[0018] 将多项式系数信息及部件本身信息代入解密公式获取到新的密钥RH’。

[0019] 优选地，所述获取新的密钥RH’的步骤之后，还包括：

[0020] 对所述新的密钥RH’进行一次哈希运算进行验证，以验证所述新的密钥RH’是否来自密钥管理中心；

[0021] 在验证通过后，判定所述新的密钥RH’来自密钥管理中心，为有效密钥。

[0022] 优选地，所述方法还包括：

[0023] 在部件接收到攻击操作后，自动删除部件所存储的秘密信息。

[0024] 此外，为实现上述目的，本发明还提供一种无人值守终端的密钥更新装置，包括：

[0025] 接收模块，用于每一时隙接收密钥更新指令；

[0026] 提取模块，用于从所述更新指令中提取密钥数据；

[0027] 计算模块，用于将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH’，通过预设算法计算得到新的密钥FH’；

[0028] 更新模块，用于根据所述新的密钥RH’和FH’更新秘密对RH和FH，将RH’与FH’之和作为新的工作密钥。

[0029] 优选地，还包括：

[0030] 生成模块，用于由密钥管理中心按照正向哈希算法加密随机数生成F组密钥，由密钥管理中心按照反向哈希算法加密随机数生成R组密钥；

[0031] 所述计算模块，还用于根据部件本身信息按照预设公式计算部件的秘密值；

[0032] 初始化模块，用于在部件初始化时，按照部件的标识信息ID向部件注入F组密钥初始值和各时隙相应的秘密值。

[0033] 优选地，所述计算模块，还用于获取密钥数据中密钥管理中心下发的多项式系数信息；将多项式系数信息及部件本身信息代入解密公式获取到新的密钥RH’。

[0034] 优选地，还包括：

[0035] 验证模块，用于对所述新的密钥RH’进行一次哈希运算进行验证，以验证所述新的密钥RH’是否来自密钥管理中心；在验证通过后，判定所述新的密钥RH’来自密钥管理中心，为有效密钥。

[0036] 优选地，还包括：

[0037] 删除模块，用于在部件接收到攻击操作后，自动删除部件所存储的秘密信息。

[0038] 本发明通过在部件初始化时注入秘密对和秘密值并存储，每一时隙密钥管理中心

下发更新指令，密钥管理中心下发的更新指令中携带密钥数据，部件根据密钥数据对存储的秘密信息进行更新。降低了密钥被读取和窃取的风险，提高了密钥的安全性，进而提高了部件与无人值守终端通信的安全性及管理效率。

附图说明

[0039] 图1为本发明无人值守终端的密钥更新方法的第一实施例的流程示意图；

[0040] 图2为本发明一实施例中主控连接外接部件的示意图；

[0041] 图3为本发明一实施例中生成秘密信息的流程示意图；

[0042] 图4为本发明一实施例中生成F组密钥的示意图；

[0043] 图5为本发明一实施例中生成R组密钥的示意图；

[0044] 图6为本发明无人值守终端的密钥更新方法的第二实施例的流程示意图；

[0045] 图7为本发明无人值守终端的密钥更新方法的第三实施例的流程示意图；

[0046] 图8为本发明一实施例密钥管理过程的流程示意图；

[0047] 图9为本发明无人值守终端的密钥更新装置的第一实施例的功能模块示意图；

[0048] 图10为本发明无人值守终端的密钥更新装置的第二实施例的功能模块示意图；

[0049] 图11为本发明无人值守终端的密钥更新装置的第三实施例的功能模块示意图。

[0050] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0051] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0052] 本发明实施例的主要解决方案是：通过在部件初始化时注入秘密对和秘密值并存储，每一时隙密钥管理中心下发更新指令，密钥管理中心下发的更新指令中携带密钥数据，部件根据密钥数据对存储的秘密信息进行更新。降低了密钥被读取和窃取的风险，提高了密钥的安全性，进而提高了部件与无人值守终端通信的安全性及管理效率。

[0053] 现有密钥技术存在自助终端中多个部件共享下载密钥导致密钥容易被读出，安全性差及管理效率差的问题。

[0054] 基于上述问题，本发明提供一种无人值守终端的密钥更新方法。

[0055] 参照图1，图1为本发明无人值守终端的密钥更新方法的第一实施例的流程示意图。

[0056] 在一实施例中，所述无人值守终端的密钥更新方法包括：

[0057] 步骤S10，每一时隙接收密钥更新指令；

[0058] 在本实施例中，参考图2，一般终端都是通过工控主板控制各类外接部件。在初始化时，无人值守终端的每个敏感部件都存储了一个相同的秘密对FH、RH和不相同的若干个秘密值(b1、b2、b3……bn)，FH、RH分别经过运算后得到F组密钥和R组密钥，RH是通过随机源生成的随机数执行n次H(.)运算得到，其中，H(.)运算是一种采用SHA、SM3等标准的单向哈希算法。密钥对是在初始状态、受控环境下、受保护地由密钥管理中心传输到敏感部件中并由敏感部件负责保护其私密性，每一时隙，密钥管理中心会下发密钥更新指令，各个敏感部件接收密钥管理中心下发的更新指令，所述更新指令中携带有密钥数据。

[0059] 参考图3，密钥管理中心生成秘密信息的过程包括：

[0060] 步骤S40，由密钥管理中心按照正向哈希算法加密随机数生成F组密钥，按照反向哈希算法加密随机数生成R组密钥；

[0061] 步骤S50，根据部件本身信息按照预设公式计算部件的秘密值；

[0062] 步骤S60，在部件初始化时，按照部件的标识信息ID向部件注入F组密钥初始值和各时隙相应的秘密值。

[0063] 具体的，由密钥管理中心按照正向哈希算法加密随机数生成F组密钥，由密钥管理中心按照反向哈希算法加密随机数生成R组密钥；根据部件本身信息按照预设公式计算部件的秘密值bi；在部件初始化时，按照部件的标识信息ID向部件注入秘密对FH、RH和相应的秘密值bi。终端每一敏感部件使用互不相同的秘密值，其生成多项式为F(X)公式1所示，通过该多项式，密钥管理中心可在部件初始化时，根据部件的ID选择性的将$F_1(ID)$的值注入相应终端成为该设备的秘密值bi。

[0064] $F_i(X)=a_nX^n+a_{n-1}X^{n-1}\cdots\cdots+a_1$ 公式1

[0065] 其中，X为部件的ID号，最高次n为外接部件的数量，i为时隙值。

[0066] 参考图4，为用哈希算法加密随机数FH生成F组密钥；参考图5，为用反向哈希加密随机数RS生成R组密钥。

[0067] 终端每一敏感部件使用互不相同的秘密值，其生成多项式为F(X)公式1所示，通过该多项式，密钥管理中心可在部件初始化时，根据部件的ID选择性的将$F_1(ID)$的值注入相应部件成为该部件的秘密值b1。

[0068] 对R组密钥引入干扰多项式δ(X)，多项式的系数由被攻击的敏感部件的标识和一些随机部件的标识构成，构建过程包括获取被攻击部件的标识信息以及随机部件标识；由所述被攻击部件的标识信息以及随机部件标识构建成干扰多项式。干扰多项式δ(X)会列出被攻击的部件标识信息，使被攻击的部件无法获取新时隙的密钥。

[0069] 密钥管理中心下发给部件的更新指令中携带密钥多项式系数信息，该系数信息有密钥值RH'、干扰多项式及生成多项式组合而成，组合而成的多项式如公式3所示的$Z_i(X)$，其中X为部件ID，i为对应时隙。

[0070] $\delta(X)=(X-ID_1)\cdots(X-ID_i)(X-b_1)(X-b_i)\cdots(X-b_n)$ 公式2

[0071] $Z_i(X)=c_nX^n+c_{n-1}X^{n-1}+\cdots\cdots c_1$ 公式3

[0072] 步骤S20，从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH'；

[0073] 在部件接收到密钥管理中心发过来的时隙更新指令时，从所述更新指令中提取密钥数据。即，从所述更新指令中提取密钥值RH'、干扰多项式及生成多项式。部件在接收到密钥管理中心下发的更新指令后，将指令中所携带的多项式$Z_i(X)$的数据及该部件本身信息代入解密公式$R_i(X)$中来获取到新的密钥RH'。该部件本身信息包括但不限于当前周期的秘密值bi以及部件ID号等部件本身的标识信息，带入解密一元多项式后获取新的密钥RH'的多项式如公式4所示，其中i为时隙值，X的值是部件ID。

[0074] $Ri(X)=(Z_i+b_i)/\delta(X)$ 公式4

[0075] 根据上述公式4计算得到新的密钥RH'。

[0076] 步骤S30，通过预设算法计算得到新的密钥FH'，根据所述新的密钥RH'和FH'更新秘密对RH和FH，将RH'和FH'之和作为新的工作密钥。

[0077] 部件通过FH'＝H(FH)计算得到F组密钥。部件可获得当时时隙的新工作密钥S＝FH'+RH',并更新部件秘密值FH＝FH'及RH＝RH',将RH'和FH'之和作为新的工作密钥。使用新的工作密钥进行通信,进入下一时隙,通过上述步骤重新获取密钥。

[0078] 本实施例通过在部件初始化时注入秘密对和秘密值并存储,每一时隙密钥管理中心下发更新指令,密钥管理中心下发的更新指令中携带密钥数据,部件根据密钥数据对存储的秘密信息进行更新。降低了密钥被读取和窃取的风险,提高了密钥的安全性,进而提高了部件与无人值守终端通信的安全性及管理效率。

[0079] 参照图6,图6为本发明无人值守终端的密钥更新方法的第二实施例的流程示意图。基于无人值守终端的密钥更新上述方法的第一实施例,所述步骤S20之后,还包括:

[0080] 步骤S70,对所述新的密钥RH'进行一次哈希运算进行验证,以验证所述新的密钥RH'是否来自密钥管理中心;

[0081] 步骤S80,在验证通过后,判定所述新的密钥RH'来自密钥管理中心,为有效密钥。

[0082] 在本实施例中,为了进一步提高密钥管理的安全性,在生成新的密钥RH'之后,将新的密钥RH'进行一次哈希运算来进行验证,通过验证RH是否等于(RH')来判断该密钥是否来自密钥管理中心,可提高密钥安全性,在RH＝(RH')时,验证成功。在验证成功后,进行FH'＝H(FH)运算获取到密钥FH',获取F组密钥,此时部件可获得新的工作密钥S＝FH'+RH',更新部件秘密值FH＝FH',RH＝RH'。其中,F组密钥用来判断设备是否为我方设备,S组可用来判别设备是否正常。在获取新的工作密钥后,使用新的工作密钥进行通信,进入下一时隙,按照上述过程重新获取新的工作密钥。

[0083] 参照图7,图7为本发明无人值守终端的密钥更新方法的第三实施例的流程示意图。为了进一步提高部件工作的安全性,所述方法还包括:

[0084] 步骤S90,在部件接收到攻击操作后,自动删除部件存储的秘密信息。

[0085] 秘密对是由密钥管理中心传输到每一个敏感部件中,并由敏感部件负责保护其私密性,当部件受到攻击时会清除存储在部件中的秘密信息,所述秘密信息包括但不限于秘密对FH、RH,秘密值bi和新的工作密钥。

[0086] 为了更好的描述本发明实施例的密钥更新过程,参考图8,包括:

[0087] S101,部件进行初始化;本发明技术方案为无人值守终端的每一个敏感部件都存储了一个秘密对FH、RH,秘密值FH、RH是设备部件在初始化、受控环境下、受保护地由密钥管理中心传输到敏感部件中,并由敏感部件负责保护其私密性,当部件受到攻击时会清除存储在部件中的秘密信息。RH是随机数SR通过执行n次H(.)运算得到,其中H(.)运算是一种采用SHA、SM3等标准的单向哈希算法。FH、SR分别通过对应运算得到密钥组F组、R组中的密钥。

[0088] S102,部件接收密钥更新指令。每一时隙部件会接收到密钥更新的指令,收到指令后部件开始进行工作密钥的更新。

[0089] S103,密钥更新指令中携带构造密钥下发多项式的数据,该多项式的数据由R_i、干扰多项式δ(X)及生成多项式Fi(X)组合而成,其中干扰多项式δ(X)由被攻击的敏感部件的部件标识和一些随机部件标识构成,即该多项式能列出受攻击设备编号,受到攻击的设备将无法获取新的密钥。

[0090] S104,设备部件在接收到密钥管理中心下发的指令后,可将指令中所带多项式的数据及该部件本身信息代入解密公式4来获取新的时隙密钥RH'即R组中的密钥,其部件本

身信息包括当前周期的秘密值bi以及如部件ID号等部件本身的标识信息。

[0091] S105,对RH'组密钥进行验证。R组密钥是反向取的哈希运算的结果,所以新密钥可进行一次哈希运算来验证所得密钥是与上一密钥相等。即RH=H(RH')是否成立,若成立则验证通过,否则密钥验证不成功。

[0092] S106,密钥通过验证后每个部件通过FH'=H(FH)计算得到F组密钥。

[0093] S107,部件可获得当时时隙的新工作密钥S=FH'+RH',并更新部件秘密值FH=FH'及RH=RH'。使用新的工作密钥进行通信,进入下一时隙,通过上述步骤重新获取密钥。

[0094] 上述第一至第三实施例的无人值守终端的密钥更新方法的执行主体均可以为部件或与部件通信连接的终端。更进一步地,该无人值守终端的密钥更新方法可以由安装在部件或终端上的客户端检测程序实现,其中,该部件可以包括但不限于打印机、键盘或发卡器等与工控主板连接的电子设备。所述终端包括但不限于手机、pad、笔记本电脑等。

[0095] 本发明进一步提供一种无人值守终端的密钥更新装置。

[0096] 参照图9,图9为本发明无人值守终端的密钥更新装置的第一实施例的功能模块示意图。

[0097] 在一实施例中,所述无人值守终端的密钥更新装置包括:接收模块10、生成模块20、计算模块30、初始化模块40、提取模块50及更新模块60。

[0098] 所述接收模块10,用于每一时隙接收密钥更新指令;

[0099] 在本实施例中,参考图2,一般终端都是通过工控主板控制各类外接部件。在初始化时,无人值守终端的每个敏感部件都存储了一个相同秘密对FH、RH和不相同的若干个秘密值(b1、b2、b3……bn),FH、RH分别经过运算后得到F组密钥和R组密钥,RH是通过随机源生成的随机数执行n次H(.)运算得到,其中,H(.)运算是一种采用SHA、SM3等标准的单向哈希算法。密钥对是在初始状态、受控环境下、受保护地由密钥管理中心传输到敏感部件中并由敏感部件负责保护其私密性,每一时隙,密钥管理中心会下发密钥更新指令,各个敏感部件接收密钥管理中心下发的更新指令,所述更新指令中携带有密钥数据。

[0100] 所述生成模块20,用于由密钥管理中心按照正向哈希算法加密随机数生成F组密钥,由密钥管理中心按照反向哈希算法加密随机数生成R组密钥;

[0101] 所述计算模块30,用于根据部件本身信息按照预设公式计算部件的秘密值;

[0102] 所述初始化模块40,用于在部件初始化时,按照部件的标识信息ID向部件注入F组密钥初始值和各时隙相应的秘密值。

[0103] 具体的,由部件按照正向哈希算法加密随机数生成F组密钥,由密钥管理中心按照反向哈希算法加密随机数生成R组密钥;根据部件本身信息按照预设公式计算部件的秘密值bi;在部件初始化时,按照部件的标识信息ID向部件注入秘密对FH、RH和相应的秘密值bi。执行过程中生成模块20可调用分别安装于部件及密钥管理中心的控件来执行F组密钥和R组密钥的生成操作。终端每一敏感部件使用互不相同的秘密值,其生成多项式为F(X)公式1所示,通过该多项式,密钥管理中心可在部件初始化时,根据部件的ID选择性的将F_1(ID)的值注入相应部件成为该部件的秘密值bi。

[0104] $F_i(X)=a_nX^n+a_{n-1}X^{n-1}\cdots\cdots+a_1$ 公式1

[0105] 其中,X为部件的ID号,最高次n为外接部件的数量,i为时隙值。

[0106] 参考图4,为用哈希算法加密随机数FH生成F组密钥;参考图5,为用反向哈希加密

随机数RS生成R组密钥。

[0107] 终端每一敏感部件使用互不相同的秘密值，其生成多项式为F(X)公式1所示，通过该多项式，密钥管理中心可在部件初始化时，根据部件的ID选择性的将$F_1(ID)$的值注入相应部件成为该部件的秘密值b1。

[0108] 对R组密钥引入干扰多项式δ(X)，多项式的系数由被攻击的敏感部件的标识和一些随机部件的标识构成，构建过程包括获取被攻击部件的标识信息以及随机部件标识；由所述被攻击部件的标识信息以及随机部件标识构建成干扰多项式。干扰多项式δ(X)会列出被攻击的部件标识信息，使被攻击的部件无法获取新时隙的密钥。

[0109] 密钥管理中心下发给部件的更新指令中携带密钥多项式系数信息，该系数信息有密钥值RH'、干扰多项式及生成多项式组合而成，组合而成的多项式如公式3所示的$Z_i(X)$，其中X为部件ID，i为对应时隙。

[0110] $\delta(X)=(X-ID_1)\cdots(X-ID_i)(X-b_1)(X-b_i)\cdots(X-b_n)$ 公式2

[0111] $Z_i(X)=c_nX^n+c_{n-1}X^{n-1}+\cdots\cdots c_1$ 公式3

[0112] 所述提取模块50，用于从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH'；

[0113] 在部件接收到密钥管理中心发过来的时隙更新指令时，从所述更新指令中提取密钥的更新数据。即，从所述更新指令中提取密钥值RH'、干扰多项式及生成多项式。

[0114] 所述计算模块30，还用于通过预设算法计算得到新的密钥FH'；

[0115] 所述更新模块60，用于根据所述新的密钥RH'和FH'更新秘密对RH和FH，将RH'和FH'之与作为新的工作密钥。

[0116] 部件在接收到密钥管理中心下发的更新指令后，将指令中所携带的多项式$Z_i(X)$的数据及该部件本身信息代入解密公式$R_i(X)$中来获取到新的密钥RH'。该部件本身信息包括但不限于当前周期的秘密值bi以及部件ID号等部件本身的标识信息，带入解密一元多项式后获取新的密钥RH'的多项式如公式4所示，其中i为时隙值，X的值是部件ID。

[0117] $Ri(X)=(Z_i+b_i)/\delta(X)$ 公式4

[0118] 根据上述公式4计算得到新的密钥RH'。

[0119] 计算模块30通过FH'=H(FH)计算得到F组密钥，可获得当时时隙的新工作密钥S=FH'+RH'，更新模块60更新部件秘密值FH=FH'及RH=RH'，将RH'和FH'之和作为新的工作密钥。使用新的工作密钥进行通信，进入下一时隙，通过上述步骤重新获取密钥。

[0120] 本实施例通过在部件初始化时注入秘密对和秘密值并存储，每一时隙密钥管理中心下发更新指令，密钥管理中心下发的更新指令中携带密钥数据，部件根据密钥数据对存储的秘密信息进行更新。降低了密钥被读取和窃取的风险，提高了密钥的安全性，进而提高了部件与无人值守终端通信的安全性及管理效率。

[0121] 参照图10，图10为本发明无人值守终端的密钥更新装置的第二实施例的功能模块示意图。还包括：验证模块70，用于对所述新的密钥RH'进行一次哈希运算进行验证，以验证所述新的密钥RH'是否来自密钥管理中心；在验证通过后，判定所述新的密钥RH'来自密钥管理中心，为有效密钥。

[0122] 在本实施例中，为了进一步提高密钥管理的安全性，在生成密钥RH'之后，将新的密钥RH'进行一次哈希运算来进行验证，通过验证RH是否等于(RH')来判断该密钥是否来自

密钥管理中心，可提高密钥安全性，在R H＝(RH')时，验证成功。在验证成功后，进行FH'＝H(FH)运算获取到密钥FH'，获取F组密钥，此时部件可获得新的工作密钥S＝FH'+RH'，更新部件秘密值FH＝FH'，RH＝RH'。其中，F组密钥用来判断设备是否为我方设备，S组可用来判别设备是否正常。在获取新的工作密钥后，使用新的工作密钥进行通信，进入下一时隙，按照上述过程重新获取新的工作密钥。

[0123] 参照图11，图11为本发明无人值守终端的密钥更新装置的第三实施例的功能模块示意图。还包括：删除模块80，

[0124] 所述删除模块80，用于在部件接收到攻击操作后，自动删除部件存储的秘密信息。

[0125] 秘密对是由密钥管理中心传输到每一个敏感部件中，并由敏感部件负责保护其私密性，当部件受到攻击时会清除存储在部件中的秘密信息，所述秘密信息包括但不限于秘密对FH、RH，秘密值bi和新的工作密钥。

[0126] 以上仅为本发明的优选实施例，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。

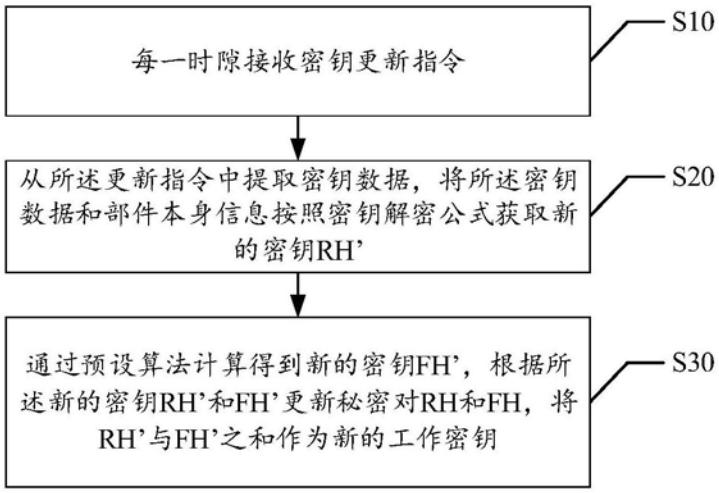

每一时隙接收密钥更新指令
S10
从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH’
S20
通过预设算法计算得到新的密钥FH’，根据所述新的密钥RH’和FH’更新秘密对RH和FH，将RH’与FH’之和作为新的工作密钥
S30

图1

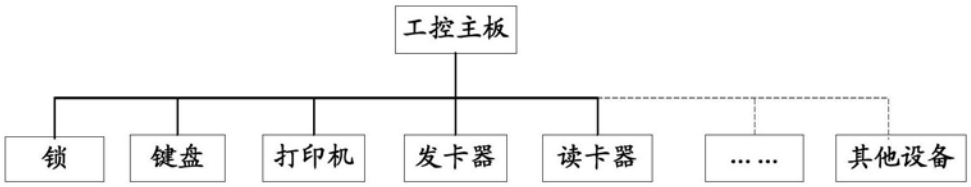

工控主板
锁
键盘
打印机
发卡器
读卡器
……
其他设备

图2

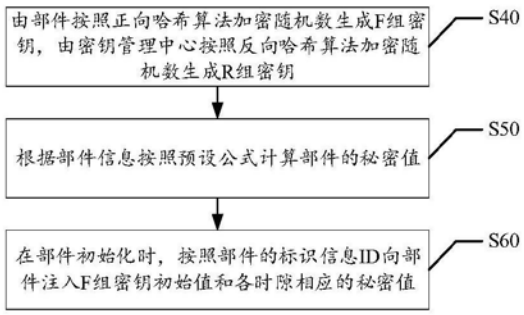

由部件按照正向哈希算法加密随机数生成F组密钥，由密钥管理中心按照反向哈希算法加密随机数生成R组密钥
S40
根据部件信息按照预设公式计算部件的秘密值
S50
在部件初始化时，按照部件的标识信息ID向部件注入F组密钥初始值和各时隙相应的秘密值
S60

图3

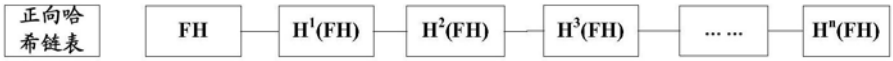

正向哈希链表
FH
H1(FH)
H2(FH)
H3(FH)
……
Hn(FH)

图4

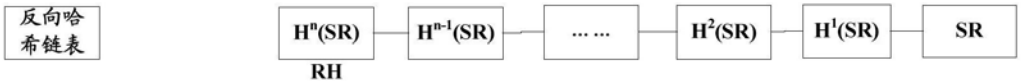

反向哈希链表
$H^n(SR)$
RH
$H^{n-1}(SR)$
……
$H^2(SR)$
$H^1(SR)$
SR

图5

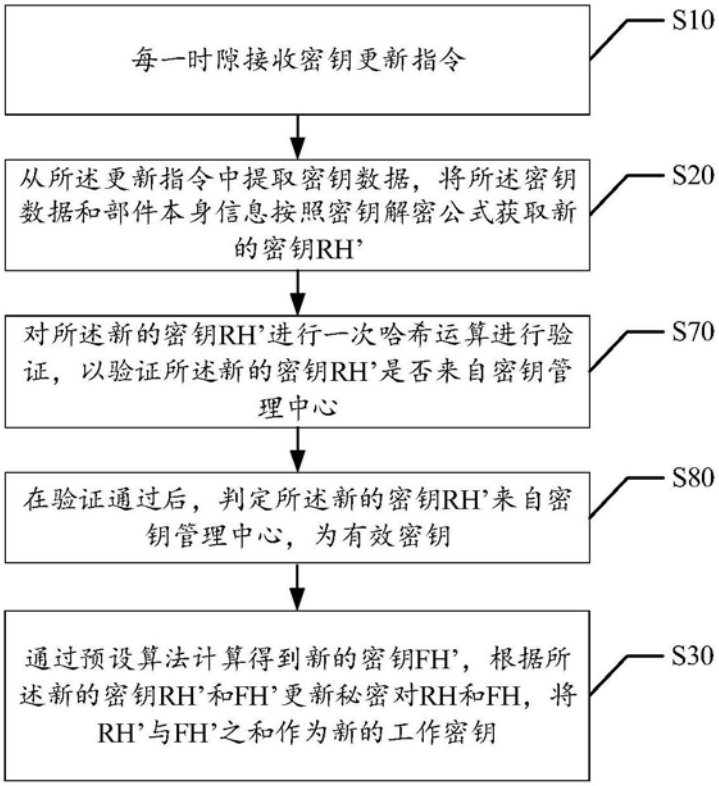

每一时隙接收密钥更新指令
S10
从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH'
S20
对所述新的密钥RH'进行一次哈希运算进行验证，以验证所述新的密钥RH'是否来自密钥管理中心
S70
在验证通过后，判定所述新的密钥RH'来自密钥管理中心，为有效密钥
S80
通过预设算法计算得到新的密钥FH'，根据所述新的密钥RH'和FH'更新秘密对RH和FH，将RH'与FH'之和作为新的工作密钥
S30

图6

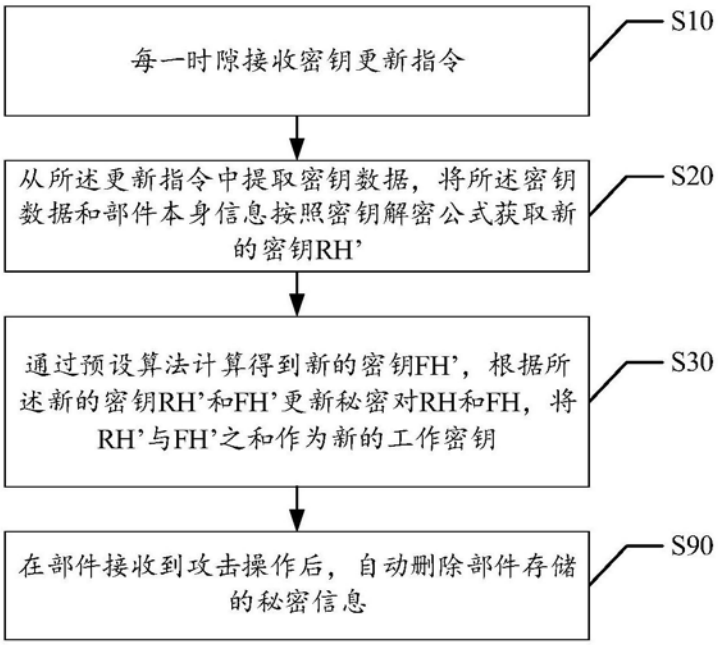

每一时隙接收密钥更新指令
S10
从所述更新指令中提取密钥数据，将所述密钥数据和部件本身信息按照密钥解密公式获取新的密钥RH’
S20
通过预设算法计算得到新的密钥FH’，根据所述新的密钥RH’和FH’更新秘密对RH和FH，将RH’与FH’之和作为新的工作密钥
S30
在部件接收到攻击操作后，自动删除部件存储的秘密信息
S90

图7

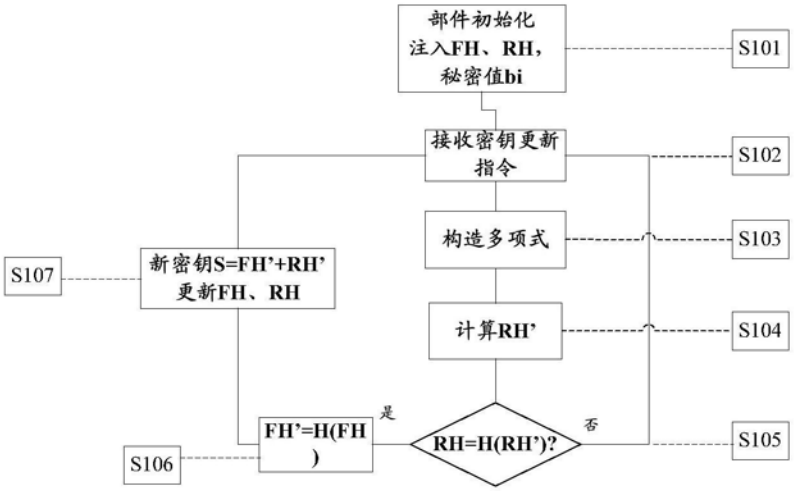

部件初始化
注入FH、RH，
秘密值bi
S101
接收密钥更新
指令
S102
构造多项式
S103
计算RH’
S104
RH=H(RH’)?
是
否
S105
FH’=H(FH
)
S106
新密钥S=FH’+RH’
更新FH、RH
S107

图8

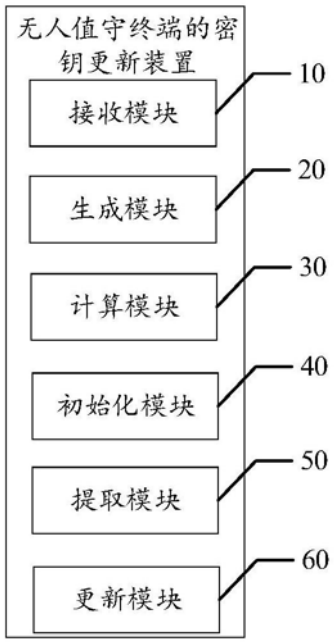

无人值守终端的密钥更新装置
接收模块
10
生成模块
20
计算模块
30
初始化模块
40
提取模块
50
更新模块
60

图9

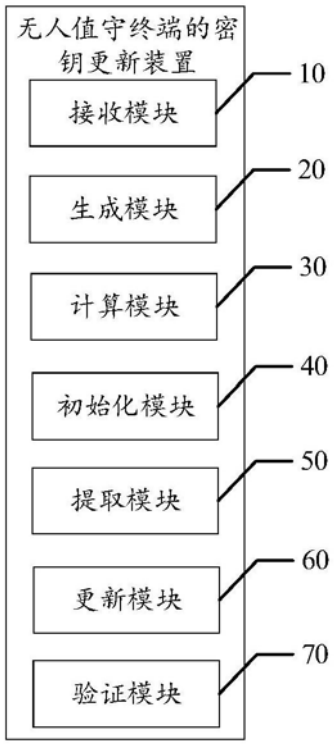

无人值守终端的密钥更新装置
接收模块
10
生成模块
20
计算模块
30
初始化模块
40
提取模块
50
更新模块
60
验证模块
70

图10

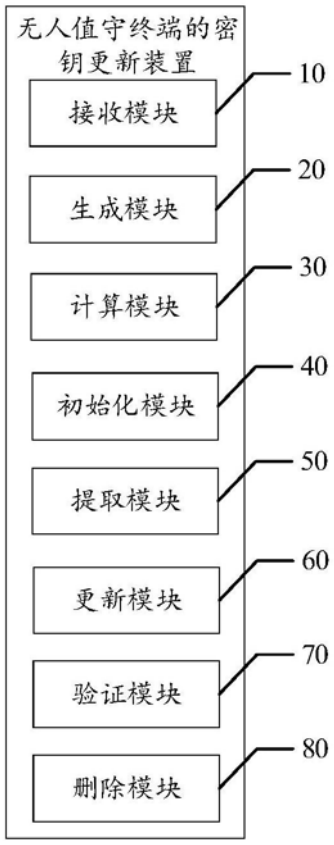

无人值守终端的密钥更新装置
接收模块
10
生成模块
20
计算模块
30
初始化模块
40
提取模块
50
更新模块
60
验证模块
70
删除模块
80

图11