(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 107005577 B
(45)授权公告日 2021.06.25

(21)申请号 201780000038.0
(22)申请日 2017.01.25
(65)同一申请的已公布的文献号
申请公布号 CN 107005577 A
(43)申请公布日 2017.08.01
(85)PCT国际申请进入国家阶段日
2017.02.10
(86)PCT国际申请的申请数据
PCT/CN2017/072711 2017.01.25
(87)PCT国际申请的公布数据
WO2018/137225 ZH 2018.08.02
(73)专利权人 深圳市汇顶科技股份有限公司
地址 518045 广东省深圳市福田保税区腾飞工业大厦B座13层

(72)发明人 孔维国 王兵 孙文彬
(74)专利代理机构 上海晨皓知识产权代理事务所(普通合伙) 31260
代理人 成丽杰
(51)Int.Cl.
H04L 29/06(2006.01)
G06K 9/00(2006.01)
(56)对比文件
CN 105678226 A,2016.06.15
CN 1841993 A,2006.10.04
CN 103646202 A,2014.03.19
审查员 吴超

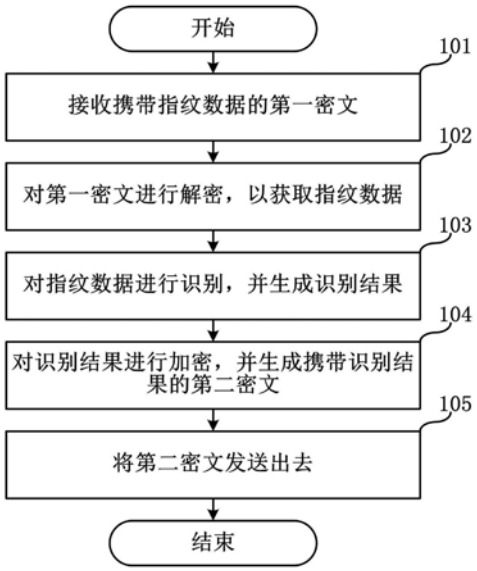
权利要求书3页 说明书10页 附图7页

(54)发明名称

指纹数据的处理方法及处理装置

(57)摘要

本发明实施例涉及数据处理技术领域，公开了一种指纹数据的处理方法及处理装置。本发明实施例中，指纹数据的处理方法包括：接收携带指纹数据的第一密文；对所述第一密文进行解密，以获取所述指纹数据；对所述指纹数据进行识别，并生成识别结果；对所述识别结果进行加密，并生成携带所述识别结果的第二密文；将所述第二密文发送出去。本发明实施例还提供了一种指纹数据的处理装置，本发明实施例使得指纹数据能够以密文形式传输，保证了指纹数据的机密性，从而提高了指纹数据的安全性。



CN 107005577 B

1.一种指纹数据的处理方法,其特征在于,应用于电子设备内的主机端,所述主机端运行在可信执行环境中,所述方法包括:

接收所述电子设备内的指纹传感器端发送的携带指纹数据的第一密文;

对所述第一密文进行解密,以获取所述指纹数据;

对所述指纹数据进行识别,并生成识别结果;

对所述识别结果进行加密,并生成携带所述识别结果的第二密文;

将所述第二密文发送至所述电子设备内的应用程序端;

其中,在所述对所述识别结果进行加密,并生成携带所述识别结果的第二密文中,具体包括:

采用消息认证码算法生成所述识别结果对应的第三消息认证码;

采用第二加密算法对所述识别结果与所述第三消息认证码进行加密,并生成所述第二密文。

2.根据权利要求1所述的指纹数据的处理方法,其特征在于,在所述对所述第一密文进行解密,以获取所述指纹数据中,具体包括:

采用第一解密算法对所述第一密文进行解密,以获取所述指纹数据与所述指纹数据对应的第一消息认证码;

采用消息认证码算法生成所述指纹数据对应的第二消息认证码;

当判定所述第一消息认证码与所述第二消息认证码匹配时,判定获取的所述指纹数据有效;

其中,所述指纹数据与所述第一消息认证码被第一加密算法加密后得到所述第一密文;所述第一解密算法与所述第一加密算法相匹配。

3.根据权利要求2项所述的指纹数据的处理方法,其特征在于,所述消息认证码算法的参数包括所述指纹数据与第一会话密钥;

在所述接收携带指纹数据的第一密文之前,还包括:

根据预置的共享密钥生成所述第一会话密钥;

根据所述第一会话密钥与所述第一密文的发送方建立第一会话通道;其中,所述第一会话通道用于所述第一密文的传输。

4.根据权利要求3项所述的指纹数据的处理方法,其特征在于,所述共享密钥的预置方式为出厂预置。

5.根据权利要求1所述的指纹数据的处理方法,其特征在于,在对所述指纹数据进行识别,并生成识别结果之前,还包括:

获取携带指纹模板的第三密文;

对所述第三密文进行解密,以获取所述指纹模板;

所述对所述指纹数据进行识别,并生成识别结果中,具体为:对所述指纹数据与所述指纹模板进行匹配识别,并生成所述识别结果。

6.根据权利要求1所述的指纹数据的处理方法,其特征在于,所述消息认证码算法的参数包括第二会话密钥与所述识别结果;

在所述对所述识别结果进行加密,并生成携带所述识别结果的第二密文之前,还包括:

根据DH密钥协商算法和身份认证算法生成所述第二会话密钥;

根据所述第二会话密钥与所述第二密文的接收方建立第二会话通道;其中,所述第二会话通道用于所述第二密文的传输。

7.根据权利要求3、4或6中的任一项所述的指纹数据的处理方法,其特征在于,所述消息认证码算法的参数还包括内置计数器的计数值。

8.一种指纹数据的处理装置,其特征在于,包含在电子设备的主机端内且所述主机端运行在可信执行环境中,所述装置包括:

数据接收模块,用于接收所述电子设备内的指纹传感器端发送的携带指纹数据的第一密文;

数据解密模块,用于对所述第一密文进行解密,以获取所述指纹数据;

数据识别模块,用于对第一明文进行识别,并生成识别结果;

数据加密模块,用于对所述识别结果进行加密,并生成携带所述识别结果的第二密文;

数据发送模块,用于将所述第二密文发送至所述电子设备内的应用程序端;

其中,所述数据加密模块具体包括:

第三消息认证码生成单元,用于采用消息认证码算法生成所述识别结果对应的第三消息认证码;

加密单元,用于采用第二加密算法对所述识别结果与所述第三消息认证码进行加密,并生成携带所述识别结果的所述第二密文。

9.根据权利要求8项所述的指纹数据的处理装置,其特征在于,所述数据解密模块包括:

解密单元,用于采用第一解密算法对所述第一密文进行解密,以获取所述指纹数据与所述指纹数据对应的第一消息认证码;

第二消息认证码生成单元,用于采用消息认证码算法生成所述指纹数据对应的第二消息认证码;

认证码匹配单元,用于在判定所述第一消息认证码与所述第二消息认证码匹配时,判定获取的所述指纹数据有效;

其中,所述指纹数据与所述第一消息认证码被第一加密算法加密后得到所述第一密文;所述第一解密算法与所述第一加密算法相匹配。

10.根据权利要求9项所述的指纹数据的处理装置,其特征在于,所述消息认证码算法的参数包括所述指纹数据与第一会话密钥;所述指纹数据的处理装置还包括:

第一会话密钥生成模块,用于在所述数据接收模块接收携带指纹数据的第一密文之前,根据预置的共享密钥生成所述第一会话密钥;

第一会话通道建立模块,用于在所述第一会话密钥生成模块根据预置的共享密钥生成所述第一会话密钥之后,根据所述第一会话密钥与所述第一密文的发送方建立第一会话通道;其中,所述第一会话通道用于所述第一密文的传输。

11.根据权利要求10项所述的指纹数据的处理装置,其特征在于,所述共享密钥的预置方式为出厂预置。

12.根据权利要求10项所述的指纹数据的处理装置,其特征在于,所述指纹数据的处理装置还包括数据获取模块,用于获取携带指纹模板的第三密文;

所述数据解密模块还用于对所述第三密文进行解密,以获取所述指纹模板;

所述数据识别模块在用于对所述指纹数据进行识别，并生成识别结果中，具体为，所述数据识别模块用于对所述指纹数据与所述指纹模板进行匹配识别，并生成所述识别结果。

13.根据权利要求8项所述的指纹数据的处理装置，其特征在于，所述消息认证码算法的参数包括第二会话密钥与所述识别结果；所述指纹数据的处理装置还包括：

第二会话密钥生成模块，用于在所述数据加密模块对所述识别结果进行加密，并生成携带所述识别结果的第二密文之前，根据DH密钥协商算法和身份认证算法生成所述第二会话密钥；

第二会话通道建立模块，用于在所述第二会话密钥生成模块根据DH密钥协商算法和身份认证算法生成所述第二会话密钥之后，根据所述第二会话密钥与所述第二密文的接收方建立第二会话通道；其中，所述第二会话通道用于所述第二密文的传输。

14.根据权利要求10、11或13中的任一项所述的指纹数据的处理装置，其特征在于，所述消息认证码算法的参数还包括内置计数器的计数值。

指纹数据的处理方法及处理装置

技术领域

[0001] 本发明实施例涉及数据处理技术领域，特别涉及一种指纹数据的处理方法及处理装置。

背景技术

[0002] 指纹识别系统广泛应用于电子设备，一般来说，指纹识别系统可以简单的划分为在主控上进行指纹匹配的方案(MOH)和在指纹传感器芯片上进行指纹匹配的方案(MOC)。其中，在主控上进行指纹匹配的方案(MOH)，当应用于电子设备时，其安全性一直是人们关注的问题之一。

[0003] 目前，在主控上进行指纹匹配的方案(MOH)，在指纹处理(指纹注册或指纹匹配)过程中，首先是指纹传感器采集指纹数据，然后指纹传感器将采集到的指纹数据直接通过数据总线传输给主机端，实际上也就是传输至主机端(X86或者X64)的运行环境中，主机端的指纹算法处理程序处理接收到的指纹数据；若是指纹注册过程，将保存指纹模板或者更新指纹模板；若是指纹匹配过程，将返回匹配结果至对应的应用程序。

[0004] 然而，现有的在主控上进行指纹匹配的方案(MOH)应用于电子设备时，除了主机端的运行环境容易遭受攻击，使得运行在主机端的指纹算法处理程序的执行环境的安全性较低外，在数据的传输过程中，主要存在如下两大安全隐患：

[0005] (1)指纹传感器传输至主机端的传输数据容易被录制和重放；

[0006] (2)主机端匹配结果的返回过程也没有进行安全性保护，易受篡改或重放攻击。

[0007] 也即是说，现有的方案中，指纹数据在传输过程中没有进行安全性的特别处理，基本以明文形式进行传输，无法保证用户指纹数据的机密性，使得指纹数据在传输过程的各个环节易受攻击，无法得到全面的、多方位的安全性保护。

发明内容

[0008] 本发明实施例实施方式的目的在于提供一种指纹数据的处理方法及处理装置，使得指纹数据能够以密文形式传输，保证了指纹数据的机密性，指纹数据在可信执行环境中处理，提高了指纹数据的安全性。

[0009] 为解决上述技术问题，本发明的实施方式提供了一种指纹数据的处理方法，包括：接收携带指纹数据的第一密文；对所述第一密文进行解密，以获取所述指纹数据；对所述指纹数据进行识别，并生成识别结果；对所述识别结果进行加密，并生成携带所述识别结果的第二密文；将所述第二密文发送出去。

[0010] 本发明的实施方式还提供了一种指纹数据的处理装置，包括：数据接收模块，用于接收携带指纹数据的第一密文；数据解密模块，用于对所述第一密文进行解密，以获取所述指纹数据；数据识别模块，用于对所述第一明文进行识别，并生成识别结果；数据加密模块，用于对所述识别结果进行加密，并生成携带所述识别结果的第二密文；数据发送模块，用于将所述第二密文发送出去。

[0011] 本发明的实施例相对于现有技术而言，接收携带指纹数据的第一密文；即，指纹数据以密文形式由发送方传输至接收方，有效避免了指纹数据可能被录制或重放的情况。对识别结果进行加密，并生成携带识别结果的第二密文；即，第一密文通过接收方的处理后，并在接收方完成加密处理，以第二密文的形式离开接收方，使得识别结果以密文的形式从第一密文的接收方传输至第二密文的接收方，对识别结果的返回过程做了安全性保护，有效避免识别结果在传输的过程中可能遭受攻击的情况。总的来说，本发明实施例中，指纹数据得到了多方位的安全性保护，保证了指纹数据的机密性，从而提高了指纹数据的安全性。

[0012] 另外，在所述对所述第一密文进行解密，以获取所述指纹数据中，具体包括：采用第一解密算法对所述第一密文进行解密，以获取所述指纹数据与所述指纹数据对应的第一消息认证码；采用消息认证码算法生成所述指纹数据对应的第二消息认证码；当判定所述第一消息认证码与所述第二消息认证码匹配时，判定获取的所述指纹数据有效；其中，所述指纹数据与所述第一消息认证码被第一加密算法加密后得到所述第一密文；所述第一解密算法与所述第一加密算法相匹配。本实施例中，第一密文的发送方将指纹数据进行加密，传输至第一密文的接收方，采用消息认证码算法生成第二消息认证码，保证了指纹数据的完整性与真实性。

[0013] 另外，消息认证码算法的参数包括所述指纹数据与第一会话密钥；在所述接收携带指纹数据的第一密文之前，还包括：根据预置的共享密钥生成所述第一会话密钥；根据所述第一会话密钥与所述第一密文的发送方建立第一会话通道；其中，所述第一会话通道用于所述第一密文的传输。本实施例中，根据预置的共享密钥生成第一会话密钥，相对于现有技术根据实时产生的共享密钥生成第一会话密钥的方式，预置的共享密钥降低了对第一密文的发送方(例如指纹传感器)的性能要求，使得较低性能的发送方也可以适用于本实施例，增加了本实施例的应用范围。

[0014] 另外，共享密钥的预置方式为出厂预置；本实施例中，提供了共享密钥的一种预置方式，采用出厂预置的方式，使得每一台电子设备的主机端与第一密文的发送方具有一机一密的共享密钥，从而主机端与发送方实现了一对一的绑定关系；且在共享密钥写入成功之后，将内存中的该共享密钥立刻销毁，以开启读写保护。

[0015] 另外，在对所述指纹数据进行识别，并生成识别结果之前，还包括：获取携带指纹模板的第三密文；对所述第三密文进行解密，以获取所述指纹模板；所述对所述指纹数据进行识别，并生成识别结果中，具体为：对所述指纹数据与所述指纹模板进行匹配识别，并生成所述识别结果。本实施例中，指纹模板实际上以第三密文的形式存储(存储在预设存储区)，以第三密文的形式传输至第一密文的接收方；即指纹模板以密文形式传输，进一步提高了指纹数据的安全性。

[0016] 另外，消息认证码算法的参数还包括内置计数器的计数值。本实施例中，在消息认证码算法的参数中加入内置计数器的计数值，可有效抵御重放攻击。

附图说明

[0017] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明，这些示例性说明并不构成对实施例的限定，附图中具有相同参考数字标号的元件表示为类似的元件，除非有特别申明，附图中的图不构成比例限制。

[0018] 图1是根据第一实施方式的指纹数据的处理方法的具体流程图；

[0019] 图2是根据第二实施方式的指纹数据的处理方法的具体流程图；

[0020] 图3是根据第二实施方式的第一密文的生成过程的示意图；

[0021] 图4是根据第二实施方式的第一消息认证码的生成过程的示意图；

[0022] 图5是根据第三实施方式的指纹数据的处理方法的具体流程图；

[0023] 图6是根据第四实施方式的指纹数据的处理方法的具体流程图；

[0024] 图7是根据第五实施方式的指纹数据的处理装置的示意图；

[0025] 图8是根据第六实施方式的指纹数据的处理装置的示意图；

[0026] 图9是根据第七实施方式的指纹数据的处理装置的示意图；

[0027] 图10是根据第八实施方式的指纹数据的处理装置的示意图。

具体实施方式

[0028] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明的各实施方式进行详细的阐述。然而，本领域的普通技术人员可以理解，在本发明各实施方式中，为了使读者更好地理解本申请而提出了许多技术细节。但是，即使没有这些技术细节和基于以下各实施方式的种种变化和修改，也可以实现本申请所要求保护的技术方案。

[0029] 本发明的第一实施方式涉及一种指纹数据的处理方法，应用于电子设备，本实施例的具体流程如图1所示，包括：

[0030] 步骤101，接收携带指纹数据的第一密文。

[0031] 本实施方式中，可以接收由电子设备的指纹传感器发送的携带指纹数据的第一密文，然实际中不限于此，还可以接收其他发送方发送的携带指纹数据的第一密文。

[0032] 本实施方式中，携带指纹数据的第一密文，即由明文形式的指纹数据经过加密后获得。本实施例中，可以采用加密算法加密对应的明文以获得第一密文，采用的加密算法例如为高级加密标准(AES加密算法)，然本实施例对加密算法的具体类型不作任何限制，例如加密算法还可以为数据加密算法(DES算法)。

[0033] 本实施例中，第一密文的接收方运行于可信执行环境(TEE)，使得接收方能够得到TEE的硬件保护，使得恶意程序无法破坏或篡改接收方的执行环境。本实施例中，第一密文的接收方例如为主机端的指纹算法处理程序，然不限于此。

[0034] 步骤102，对第一密文进行解密，以获取指纹数据。

[0035] 本实施方式中，对第一密文的解密方式不作任何限制。

[0036] 步骤103，对指纹数据进行识别，并生成识别结果。

[0037] 步骤104，对识别结果进行加密，并生成携带识别结果的第二密文。

[0038] 本实施方式中，可以采用加密算法对识别结果进行加密，可以与第一密文的加密算法相同，也可以不同，本实施例对此不作任何限制。

[0039] 步骤105，将第二密文发送出去。

[0040] 本实施方式中，将第二密文发送至对应的应用代理或应用程序。其中，应用代理工作于可信执行环境(TEE)中，能够得到TEE的硬件保护。

[0041] 本发明的实施例相对于现有技术而言，第一密文的接收方工作于可信执行环境(TEE)中，使得接收方能够得到TEE的硬件保护，使得恶意程序无法破坏或篡改接收方的执

行环境。本实施例中，接收携带指纹数据的第一密文；即，指纹数据以密文形式由发送方传输至接收方，有效避免了指纹数据可能被录制或重放的情况。对识别结果进行加密，并生成携带识别结果的第二密文；即，第一密文通过接收方的处理后，并在接收方完成加密处理，以第二密文的形式离开接收方，使得识别结果以密文的形式从第一密文的接收方传输至第二密文的接收方，对识别结果的返回过程做了安全性保护，有效避免识别结果在传输的过程中可能遭受攻击的情况。总的来说，本发明实施例指纹数据得到了多方位的安全性保护，保证了指纹数据的机密性以及不可重放性，从而提高了指纹数据的安全性。

[0042] 上面各种方法的步骤划分，只是为了描述清楚，实现时可以合并为一个步骤或者对某些步骤进行拆分，分解为多个步骤，只要包括相同的逻辑关系，都在本专利的保护范围内；对算法中或者流程中添加无关紧要的修改或者引入无关紧要的设计，但不改变其算法和流程的核心设计都在该专利的保护范围内。

[0043] 本发明的第二实施方式涉及一种指纹数据的处理方法。第二实施方式在第一实施方式的基础上作出细化，主要细化之处在于：在本发明第二实施方式中，从第一密文中获取明文形式的指纹数据的具体实现方式。

[0044] 本实施方式的指纹数据的处理方法的流程图如图2所示，其中，步骤203、步骤205至207与第一实施方式中的步骤101、步骤103至105对应相同，本实施例在此不再赘述，不同之处在于，本实施例新增了步骤201、202，且对步骤204进行了细化，具体说明如下：

[0045] 步骤201，根据预置的共享密钥生成第一会话密钥。

[0046] 本实施方式中。由于第一密文的发送方(例如指纹传感器)是一个独立于主机端(主控芯片)的元件，一般处理能力相对较弱，采用预置的共享密钥，相对于现有技术根据实时产生的共享密钥生成第一会话密钥的方式，预置的共享密钥降低了对第一密文的发送方(例如指纹传感器)的性能要求，使得较低性能的发送方也可以适用于本实施例，增加了本实施例的应用范围。

[0047] 本实施例中，以出厂预置的方式预置共享密钥。具体而言，在工厂生产阶段，产线工具可以为每一台电子设备的主机端与指纹传感器端随机生成一机一密的共享密钥，并将共享密钥存储到电子设备的主机端与指纹传感器端，从而主机端与发送方实现了一对一的绑定关系；等待共享密钥写入成功之后，产线工具立刻销毁内存中的该共享密钥，以主机端和发送方开启读写保护。然本实施例对共享密钥的预置方式不作任何限制。

[0048] 本实施方式中，可以根据预置的共享密钥与双方产生的随机数生成第一会话密钥，且不同的会话，生成的第一会话密钥不同。具体而言，主机端与指纹传感器端执行安全协议的握手协议，主机端与指纹传感器端分别产生一个随机数，并将自己产生的随机数发送给对方；主机端与指纹传感器端分别根据预置的共享密钥与双方的随机数生成第一会话密钥；然本实施例对第一会话密钥的生成方式不作任何限制。示例的，共享密钥为PMK，主机端与指纹传感器端执行安全协议的握手协议，主机端产生了一个随机数A，指纹传感器端产生了一个随机数B。主机端将产生的随机数A发送给指纹传感器端，指纹传感器端将产生的随机数B发送给主机端，主机端根据共享密钥PMK与双方的随机数A、B生成第一会话密钥；指纹传感器端根据共享密钥PMK与双方的随机数A、B生成第一会话密钥。然这里只是示例性说明，实际中不限于此。

[0049] 本实施例中，安全协议可以为安全传输层协议(TLS)，然本实施例对安全协议的类

型不作任何限制。

[0050] 本实施例中，由于主机数据接收模块运行于可信执行环境(TEE)，因此，主机端的安全协议的工作环境也位于TEE环境中，以得到硬件保护。

[0051] 步骤202，根据第一会话密钥与第一密文的发送方建立第一会话通道。

[0052] 本实施方式中，第一密文的发送方，可以为电子设备的指纹传感器，然本实施例对此不作任何限制。

[0053] 本实施例中，根据第一会话密钥与第一密文的发送方建立第一会话通道，使得第一会话通道处于安全协议的保护之下。

[0054] 本实施例中，第一会话通道用于第一密文的传输；即，第一会话通道是为第一密文建立的安全传输通道。

[0055] 本实施方式中，可以利用第一会话密钥验证对方的身份，以保证对方身份的真实性，从而实现建立第一会话通道。具体的，本实施例中，主机端与指纹传感器端分别将各自之前发送的及接收的所有数据利用第一会话密钥进行加密得到第一身份密文，并将第一身份密文发送至对方，然后主机端与指纹传感器端分别将接收到的第一身份密文与自己的第一身份密文进行对比，若密文数据相同，则双方身份验证成功，表示第一会话通道建立成功。

[0056] 步骤204，对第一密文进行解密，以获取指纹数据。

[0057] 本实施例中，步骤204包括子步骤2041至子步骤2044，具体如下：

[0058] 子步骤2041，采用第一解密算法对第一密文进行解密，以获取指纹数据与指纹数据对应的第一消息认证码；

[0059] 本实施方式中，在第一密文的发送方，指纹数据与第一消息认证码被第一加密算法加密后得到第一密文。其中，第一消息认证码可以为哈希运算消息认证码(HMAC)(然不限于此)。示例的，如图3所示，为指纹数据与第一消息认证码的加密过程(即第一密文的生成过程)；指纹数据与第一消息认证码HMAC被第一加密算法加密后得到第一密文。然这里只是示例性说明，实际中不限于此。

[0060] 其中，在第一密文的发送方，第一消息认证码的生成方式如图4所示，采用消息认证码算法，根据指纹数据与第一会话密钥计算出第二消息认证码。

[0061] 本实施方式中，第一密文的解密过程，实际上为加密过程的逆过程，即为如图3所示的逆过程，本实施例在此不再赘述。

[0062] 本实施方式中，第一解密算法与第一加密算法相匹配。例如本实施例中，第一加密算法为高级加密标准(AES算法)时，则第一解密算法为与高级加密标准(AES算法)相匹配的解密算法；然第一加密算法还可以为数据加密算法(DES)或三重数据加密算法(3DES)，本实施例对第一加密算法的类型不作任何限制。

[0063] 子步骤2042，采用消息认证码算法生成指纹数据对应的第二消息认证码。

[0064] 本实施方式中，第二消息认证码为哈希运算消息认证码(HMAC)，然实际中不限于此。

[0065] 本实施方式中，在主机端，第二消息认证码的生成方式与在第一密文的发送方生成第二消息认证码的方式相同，此处不在赘述。

[0066] 较佳的，本实施例中，消息认证码算法的参数还包括内置计数器的计数值。即，在

计算第二消息认证码的过程中，带入指纹传感器端内置计数器的计数值，可有效抵御重放攻击。

[0067] 步骤2043，判断第一消息认证码与第二消息认证码是否匹配；若是，进入子步骤2044，否则直接结束。

[0068] 本实施方式中，将第一消息认证码与第二消息认证码进行比对，从而判断出第一消息认证码与第二消息认证码是否匹配。

[0069] 步骤2044，判定获取的指纹数据有效。

[0070] 本实施方式中，当第一消息认证码与第二消息认证码匹配时，则判定获取的指纹数据有效。即表示接收到的指纹数据是完整且真实的。

[0071] 本发明的实施例相对于第一实施方式而言，将安全协议应用于指纹数据的处理方法中。根据预置的共享密钥生成第一会话密钥，降低了第一密文的发送方的性能要求。本实施例中，第一密文的发送方将指纹数据进行加密，传输至第一密文的接收方，保证了指纹数据的机密性；采用消息认证码算法生成第二消息认证码，保证了指纹数据的完整性与真实性。

[0072] 本发明的第三实施方式涉及一种指纹数据的处理方法。第三实施方式在第一实施方式的基础上进行细化，主要细化之处在于：在本发明第三实施方式中，提供了识别结果一种具体生成方式。

[0073] 本实施方式的指纹数据的处理方法的流程图如图5所示，其中，步骤501至502、步骤506至507与第一实施方式中的步骤101至102、步骤104至105对应相同，本实施例在此不再赘述，不同之处在于，本实施例新增了步骤503、504以及505，具体说明如下：

[0074] 步骤503，获取携带指纹模板的第三密文。

[0075] 本实施方式中，可以预设存储区用于存储第三密文。用户可以预先进行指纹注册，且指纹注册产生的指纹模板在可信执行环境(TEE)下进行加密，最后一第三密文的形式保存在预设存储区。

[0076] 本实施方式中，第一密文的接收方可以从预设存储区获取第三密文。

[0077] 步骤504，对第三密文进行解密，以获取指纹模板。

[0078] 本实施方式中，可以采用解密算法对第三密文进行解密，从而获取指纹模板。其中，第三密文的解密算法，与第三密文的加密算法相匹配。

[0079] 步骤505，对指纹数据与指纹模板进行匹配识别，并生成识别结果。

[0080] 实际上，本步骤即为第一实施例中步骤103的具体实现方式。

[0081] 于实际上，本实施例也可以为在第二实施方式的基础上细化的方案。

[0082] 本发明的实施例相对于第一实施方式而言，指纹模板以第三密文的形式存储于预设存储区且以第三密文的形式从预设存储区传输至第一密文的接收方，保证了指纹数据的机密性。并且，将指纹数据与指纹模板进行匹配识别并生成识别结，提供了生成识别结果的一种具体方式。

[0083] 本发明的第四实施方式涉及一种指纹数据的处理方法。第四实施方式在第一实施方式的基础上进行细化，主要细化之处在于：在本发明第四实施方式中，提供了生成第二密文的具体实现方式。

[0084] 本实施方式的指纹数据的处理方法的流程图如图6所示，其中，步骤601至603以及

步骤607与第一实施方式中的步骤101至103以及步骤105对应相同，本实施例在此不再赘述，不同之处在于，本实施例新增了步骤604、605，且对步骤606进行了细化，具体说明如下：

[0085] 步骤604，根据DH密钥协商算法和身份认证算法生成第二会话密钥。

[0086] 实际上，本实施例中，第二会话密钥采用DH密钥协商算法结合身份认证算法生成，身份认证算法可以采用例如RSA或者DSA签名算法。虽然RSA、DSA签名算法运算量大，但由于第二会话密钥的生成方运行于主机端(主控芯片)，主机端的处理能力一般比较强大，因此，本实施例中，此处的共享密钥可以采用实时产生的方式，简单方便。

[0087] 步骤605，根据第二会话密钥与第二密文的接收方建立第二会话通道。

[0088] 本实施方式中，第二密文的接收方，可以为对应的应用程序，然不限于此。

[0089] 本实施方式中，第二会话通道用于第二密文的传输；即，第二会话通道是为第二密文建立的安全通信信道。

[0090] 本实施方式中，可以利用数字签名验证对方身份(即主机端与第二密文的接收方的身份)，以保证对方身份的真实性，从而实现协商第二会话通道的会话密钥(第二密钥)。具体的，本实施例中，在生成第二密钥的过程中，主机端和第二密文接收方分别有发送数据给对方，双方在发送之前，利用自身的证书信息(比如私钥)对待发送数据进行签名，而后把数据和该数据的签名一起发送给对方。接收方收到数据后，利用签名算法对数据进行校验，并将合法数据交给密钥协商算法进一步处理。从而获得第二密钥，建立第二回话通道。

[0091] 步骤606，对识别结果进行加密，并生成携带识别结果的第二密文。

[0092] 本步骤中，包括以下子步骤：

[0093] 子步骤6061，采用消息认证码算法生成识别结果对应的第三消息认证码。

[0094] 本实施方式中，消息认证码算法的参数包括第二会话密钥与识别结果。

[0095] 较佳的，消息认证码算法的参数还包括内置计数器的计数值。主机端与应用程序端分别维护一套保持同步的内置计时器；在计算第三消息认证码的过程中，带入主机端内置计数器的计数值，可有效抵御重放攻击。

[0096] 子步骤6062，采用第二加密算法对识别结果与第三消息认证码进行加密，并生成第二密文。

[0097] 本实施方式中，第二加密算法可以为高级加密标准(AES算法)，然实际中不限于此，第二加密算法还可以为数据加密算法(DES)或三重数据加密算法(3DES)，本实施例对第二加密算法的类型不作任何限制。

[0098] 于实际上，本实施例也可以为在第二或第三实施方式的基础上细化的方案。

[0099] 本实施方式相对于第一实施方式而言，通过第二会话密钥验证建立传输第二密文的第二会话通道，使得第二密文能够在安全通信信道中传输，为识别结果的返回过程采取了安全性保护措施。另外，采用消息认证码算法生成第三消息认证码，保证了识别结果的完整性与真实性。并且第三消息认证码与识别结果生成第二密文，保证了识别结果的机密性。

[0100] 本发明的第五实施方式涉及一种指纹数据的处理装置，如图7所示，包括：

[0101] 数据接收模块1，用于接收携带指纹数据的第一密文。

[0102] 数据解密模块2，用于对第一密文进行解密，以获取指纹数据。

[0103] 数据识别模块3，用于对第一明文进行识别，并生成识别结果。

[0104] 数据加密模块4，用于对识别结果进行加密，并生成携带识别结果的第二密文。

[0105] 数据发送模块5，用于将第二密文发送出去。

[0106] 本实施方式相对于现有技术而言，第一密文的接收方工作于可信执行环境(TEE)中，使得接收方能够得到TEE的硬件保护，使得恶意程序无法破坏或篡改接收方的执行环境。本实施例中，接收携带指纹数据的第一密文；即，指纹数据以密文形式由发送方传输至接收方，有效避免了指纹数据可能被录制或重放的情况。对识别结果进行加密，并生成携带识别结果的第二密文；即，第一密文通过接收方的处理后，并在接收方完成加密处理，以第二密文的形式离开接收方，使得识别结果以密文的形式从第一密文的接收方传输至第二密文的接收方，对识别结果的返回过程做了安全性保护，有效避免识别结果在传输的过程中可能遭受攻击的情况。总的来说，本发明实施例指纹数据得到了多方位的安全性保护，保证了指纹数据的机密性以及不可重放性，从而提高了指纹数据的安全性。

[0107] 不难发现，本实施方式为与第一实施方式相对应的系统实施例，本实施方式可与第一实施方式互相配合实施。第一实施方式中提到的相关技术细节在本实施方式中依然有效，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第一实施方式中。

[0108] 值得一提的是，本实施方式中所涉及到的各模块均为逻辑模块，在实际应用中，一个逻辑单元可以是一个物理单元，也可以是一个物理单元的一部分，还可以以多个物理单元的组合实现。此外，为了突出本发明的创新部分，本实施方式中并没有将与解决本发明所提出的技术问题关系不太密切的单元引入，但这并不表明本实施方式中不存在其它的单元。

[0109] 本发明第六实施方式涉及一种指纹数据的处理装置。第六实施方式在第五实施方式的基础上进行细化，主要细化之处在于：如图8所示，在本发明第六实施方式中，数据解密模块5包括解密单元51、第二消息认证码生成单元52以及认证码匹配单元53。

[0110] 本实施方式中，指纹数据的处理装置还包括第一会话密钥生成模块56以及第一会话通道建立模块7，具体如下：

[0111] 第一会话密钥生成模块6，用于在数据接收模块1接收携带指纹数据的第一密文之前，根据预置的共享密钥生成第一会话密钥。

[0112] 其中，共享密钥的预置方式为出厂预置。

[0113] 第一会话通道建立模块7，用于在第一会话密钥生成模块6根据预置的共享密钥生成第一会话密钥之后，根据第一会话密钥与第一密文的发送方建立第一会话通道。

[0114] 其中，第一会话通道用于第一密文的传输。

[0115] 本实施方式中，数据解密模块2包括解密单元21、第二消息认证码生成单元22以及认证码匹配单元23，具体如下：

[0116] 解密单元21，用于采用第一解密算法对第一密文进行解密，以获取指纹数据与指纹数据对应的第一消息认证码。

[0117] 第二消息认证码生成单元22，用于采用消息认证码算法生成指纹数据对应的第二消息认证码。

[0118] 其中，消息认证码算法的参数包括指纹数据与第一会话密钥。

[0119] 较佳的，消息认证码算法的参数还包括内置计数器的计数值。

[0120] 认证码匹配单元23，用于在判定第一消息认证码与第二消息认证码匹配时，判定

获取的指纹数据有效。

[0121] 本实施方式相对于第五实施方式而言，将安全协议应用于指纹数据的处理方法中。根据预置的共享密钥生成第一会话密钥，降低了第一密文的发送方的性能要求。本实施例中，第一密文的发送方将指纹数据进行加密，传输至第一密文的接收方，保证了指纹数据的机密性；采用消息认证码算法生成第二消息认证码，保证了指纹数据的完整性与真实性。

[0122] 由于第二实施方式与本实施方式相互对应，因此本实施方式可与第二实施方式互相配合实施。第二实施方式中提到的相关技术细节在本实施方式中依然有效，在第二实施方式中所能达到的技术效果在本实施方式中也同样可以实现，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第二实施方式中。

[0123] 本发明第七实施方式涉及一种指纹数据的处理装置。第七实施方式在第五实施方式的基础上进行细化，主要细化之处在于：如图9所示，在本发明第七实施方式中，指纹数据的处理装置还包括数据获取模块8。

[0124] 数据获取模块8，用于获取携带指纹模板的第三密文。

[0125] 数据解密模块2还用于对第三密文进行解密，以获取指纹模板。

[0126] 数据识别模块3在用于对指纹数据进行识别，并生成识别结果中，具体为，数据识别模块3用于对指纹数据与指纹模板进行匹配识别，并生成识别结果。

[0127] 于实际上，本实施例也可以为在第六实施方式的基础上细化的方案。

[0128] 本实施方式相对于第五实施方式而言，指纹模板以第三密文的形式存储于预设存储区且以第三密文的形式从预设存储区传输至第一密文的接收方，保证了指纹数据的机密性。并且，将指纹数据与指纹模板进行匹配识别并生成识别结，提供了生成识别结果的一种具体方式。

[0129] 由于第三实施方式与本实施方式相互对应，因此本实施方式可与第三实施方式互相配合实施。第三实施方式中提到的相关技术细节在本实施方式中依然有效，在第三实施方式中所能达到的技术效果在本实施方式中也同样可以实现，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第三实施方式中。

[0130] 本发明第八实施方式涉及一种指纹数据的处理装置。第八实施方式在第五实施方式的基础上进行细化，主要细化之处在于：如图10所示，在本发明第八实施方式中，数据加密模块4包括第三消息认证码生成单元41以及加密单元42。

[0131] 本实施方式中，指纹数据的处理装置还包括第二会话密钥生成模块9以及第二会话通道建立模块10，具体如下：

[0132] 第二会话密钥生成模块9，用于在数据加密模块对识别结果进行加密，并生成携带识别结果的第二密文之前，根据DH密钥协商算法和身份认证算法生成第二会话密钥；

[0133] 第二会话通道建立模块10，用于在第二会话密钥生成模块根据DH密钥协商算法和身份认证算法生成第二会话密钥之后，根据第二会话密钥与第二密文的接收方建立第二会话通道。

[0134] 其中，第二会话通道用于第二密文的传输。

[0135] 数据加密模块4具体包括第三消息认证码生成单元41以及加密单元42，具体如下：

[0136] 第三消息认证码生成单元41，用于采用消息认证码算法生成识别结果对应的第三消息认证码；

[0137] 其中，消息认证码算法的参数包括第二会话密钥与识别结果。

[0138] 较佳的，消息认证码算法的参数还包括内置计数器的计数值。

[0139] 加密单元42，用于采用第二加密算法对识别结果与第三消息认证码进行加密，并生成携带识别结果的第二密文。

[0140] 于实际上，本实施例也可以为在第六或第七实施方式的基础上细化的方案。

[0141] 本实施方式相对于第五实施方式而言，通过第二会话密钥验证建立传输第二密文的第二会话通道，使得第二密文能够在安全通信信道中传输，为识别结果的返回过程采取了安全性保护措施。另外，采用消息认证码算法生成第三消息认证码，保证了识别结果的完整性与真实性。并且第三消息认证码与识别结果生成第二密文，保证了识别结果的机密性。

[0142] 由于第四实施方式与本实施方式相互对应，因此本实施方式可与第四实施方式互相配合实施。第四实施方式中提到的相关技术细节在本实施方式中依然有效，在第四实施方式中所能达到的技术效果在本实施方式中也同样可以实现，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第四实施方式中。

[0143] 本领域技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序存储在一个存储介质中，包括若干指令用以使得一个设备(可以是单片机，芯片等)或处理器(processor)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0144] 本领域技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序存储在一个存储介质中，包括若干指令用以使得一个设备(可以是单片机，芯片等)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0145] 本领域的普通技术人员可以理解，上述各实施方式是实现本发明的具体实施例，而在实际应用中，可以在形式上和细节上对其作各种改变，而不偏离本发明的精神和范围。

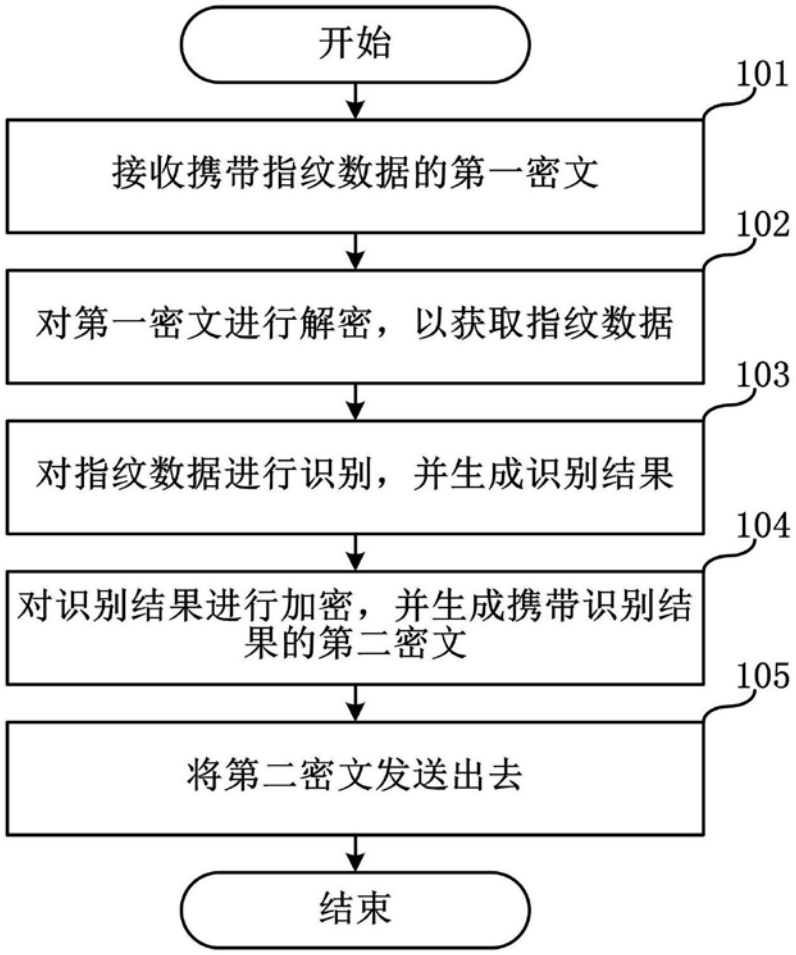

开始
101
接收携带指纹数据的第一密文
102
对第一密文进行解密，以获取指纹数据
103
对指纹数据进行识别，并生成识别结果
104
对识别结果进行加密，并生成携带识别结果的第二密文
105
将第二密文发送出去
结束

图1

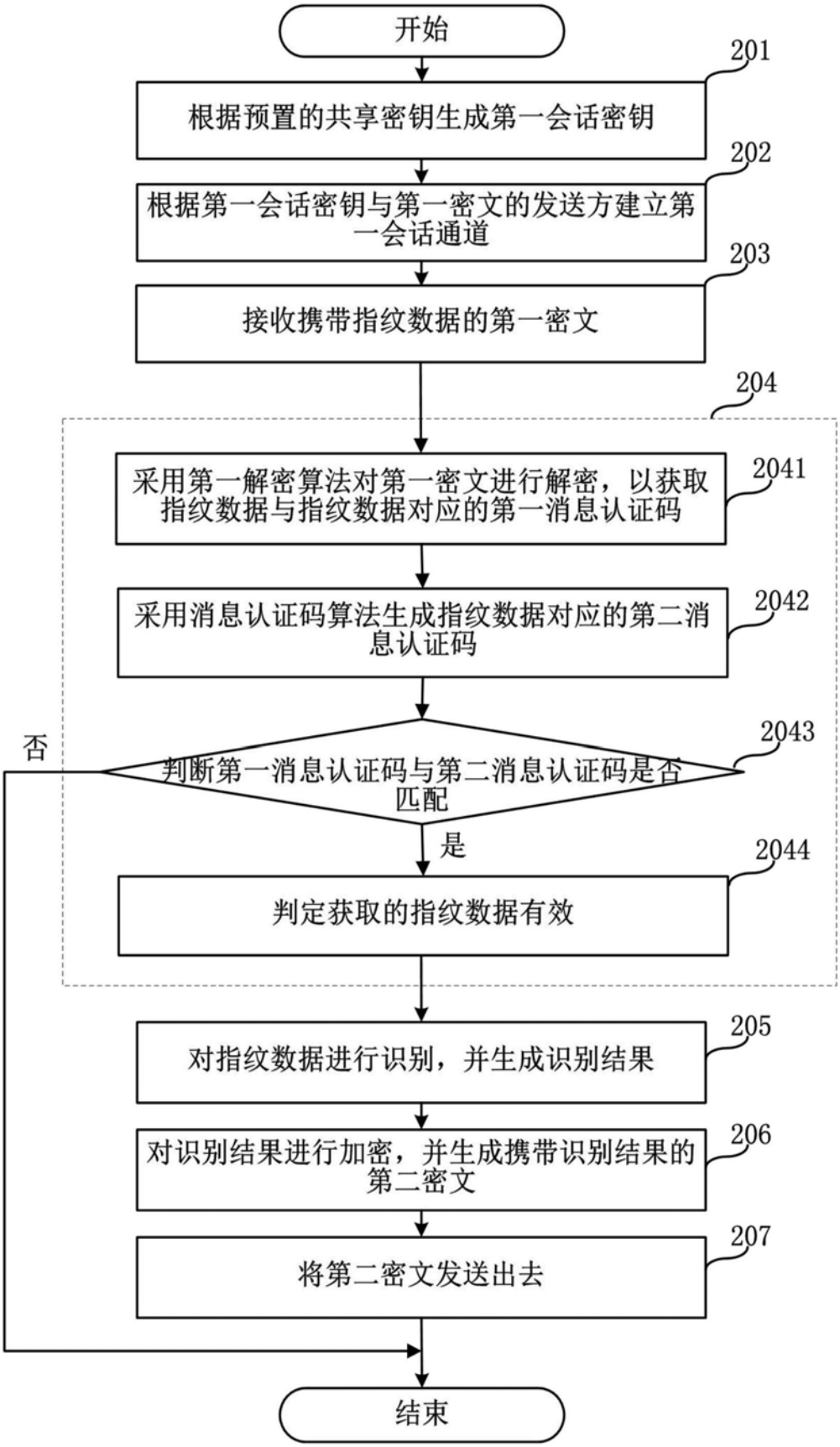

开始
201
根据预置的共享密钥生成第一会话密钥
202
根据第一会话密钥与第一密文的发送方建立第一会话通道
203
接收携带指纹数据的第一密文
204
2041
采用第一解密算法对第一密文进行解密，以获取指纹数据与指纹数据对应的第一消息认证码
2042
采用消息认证码算法生成指纹数据对应的第二消息认证码
2043
判断第一消息认证码与第二消息认证码是否匹配
否
是
2044
判定获取的指纹数据有效
205
对指纹数据进行识别，并生成识别结果
206
对识别结果进行加密，并生成携带识别结果的第二密文
207
将第二密文发送出去
结束

图2

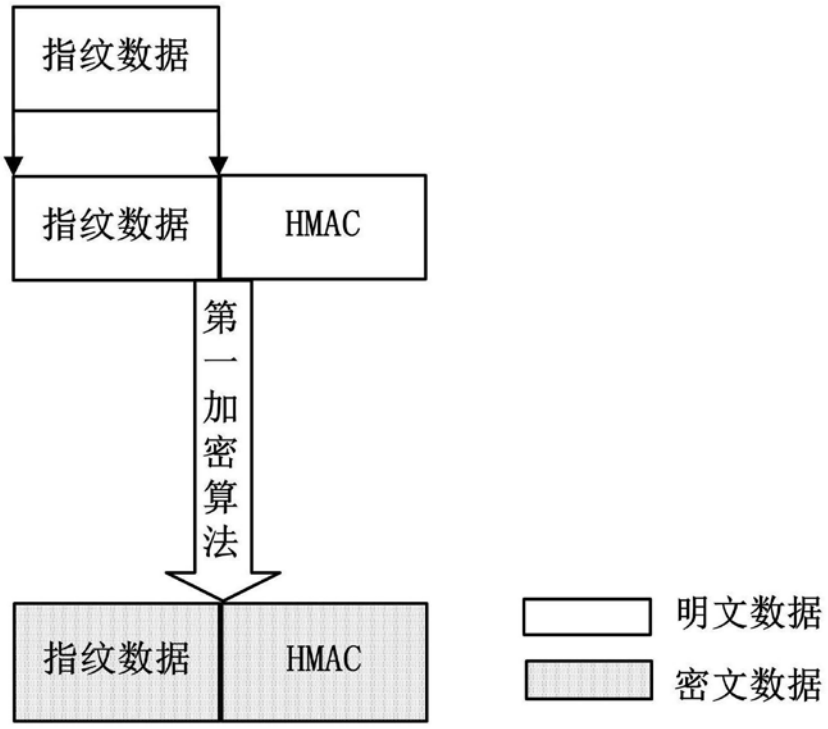

指纹数据
指纹数据
HMAC
第一加密算法
指纹数据
HMAC
明文数据
密文数据

图3

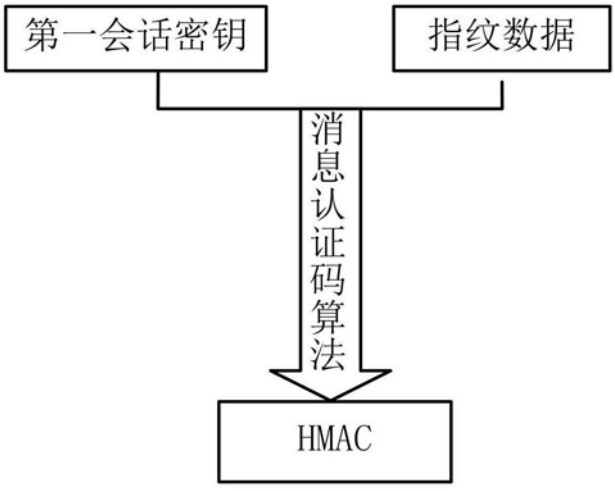

第一会话密钥
指纹数据
消息认证码算法
HMAC

图4

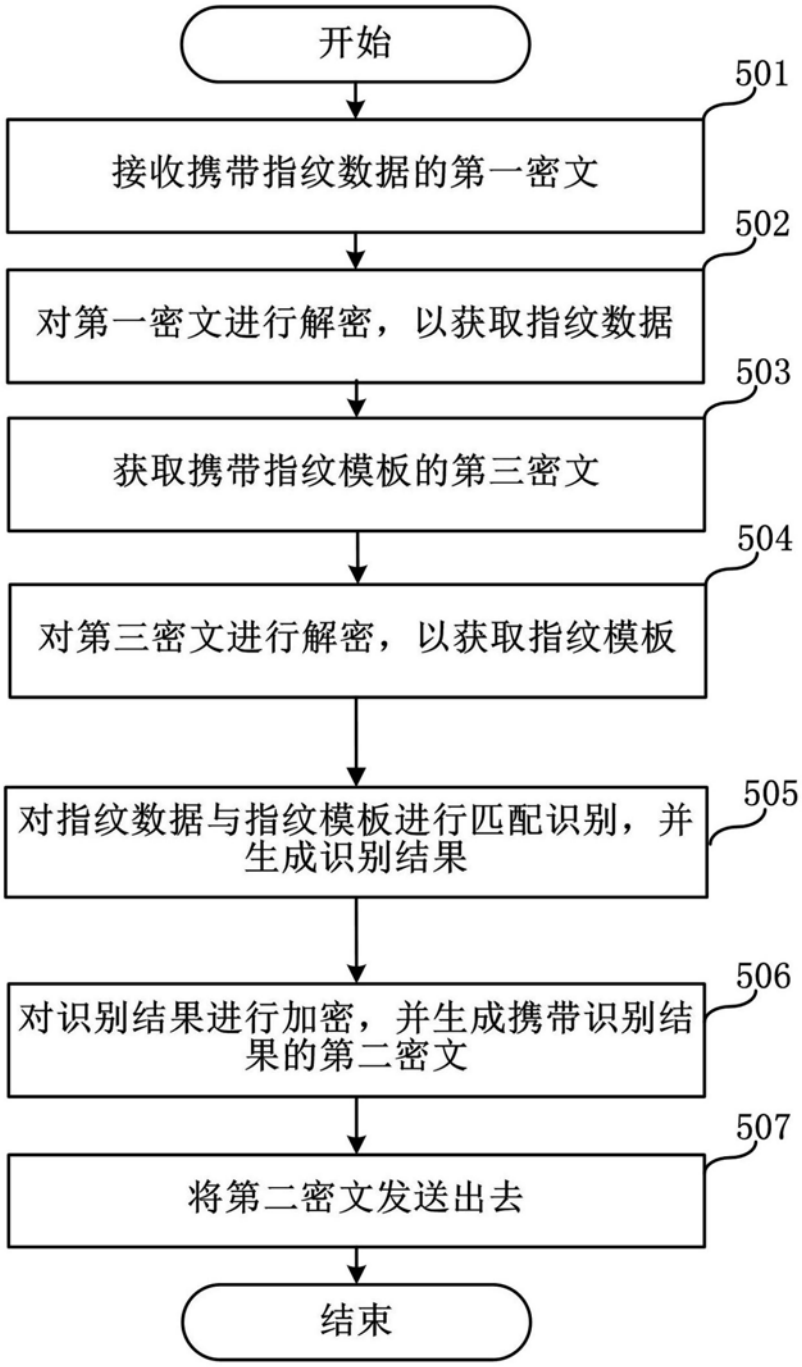

开始
501
接收携带指纹数据的第一密文
502
对第一密文进行解密，以获取指纹数据
503
获取携带指纹模板的第三密文
504
对第三密文进行解密，以获取指纹模板
505
对指纹数据与指纹模板进行匹配识别，并生成识别结果
506
对识别结果进行加密，并生成携带识别结果的第二密文
507
将第二密文发送出去
结束

图5

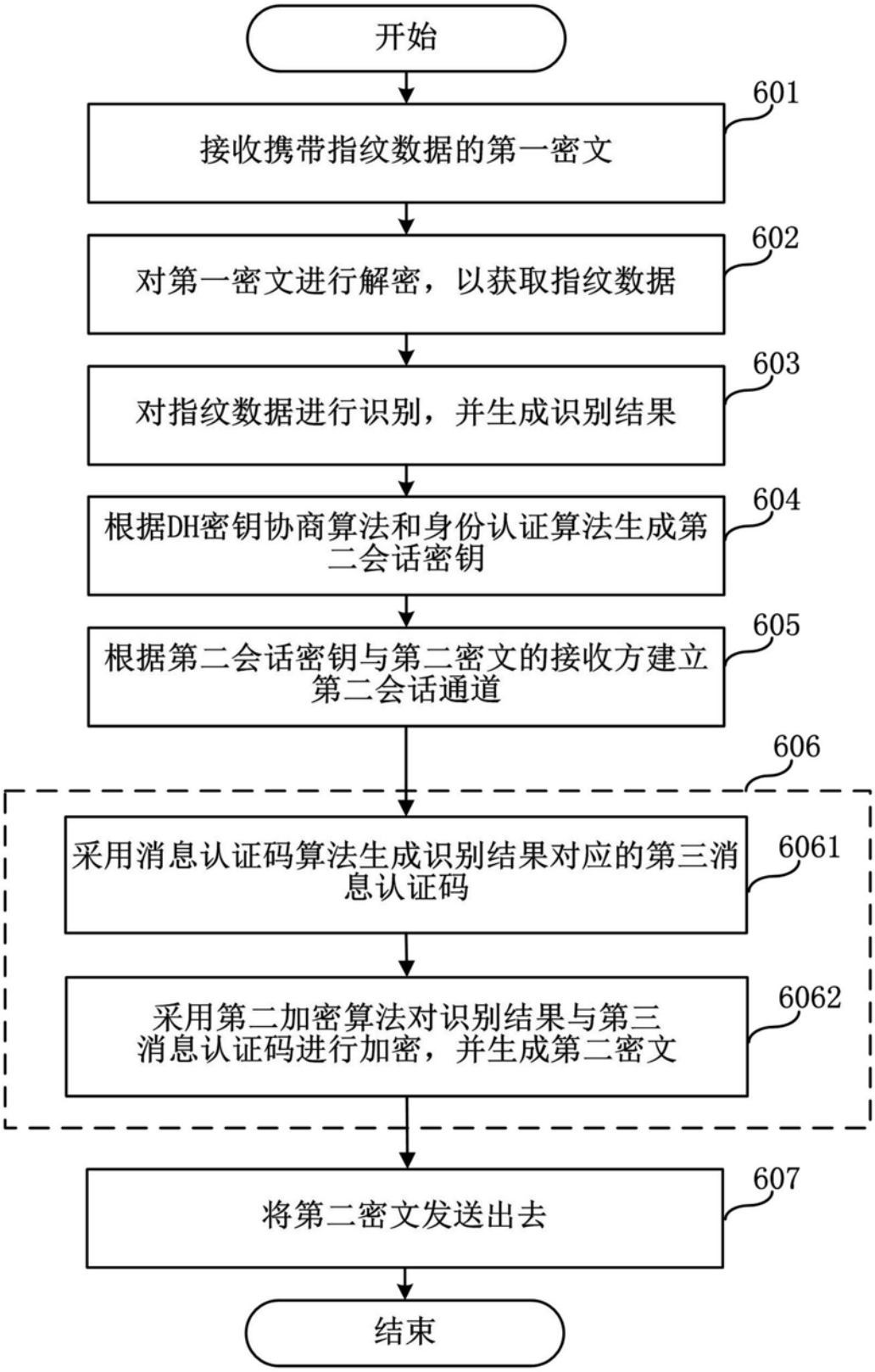

开始
601
接收携带指纹数据的第一密文
602
对第一密文进行解密，以获取指纹数据
603
对指纹数据进行识别，并生成识别结果
604
根据DH密钥协商算法和身份认证算法生成第二会话密钥
605
根据第二会话密钥与第二密文的接收方建立第二会话通道
606
6061
采用消息认证码算法生成识别结果对应的第三消息认证码
6062
采用第二加密算法对识别结果与第三消息认证码进行加密，并生成第二密文
607
将第二密文发送出去
结束

图6

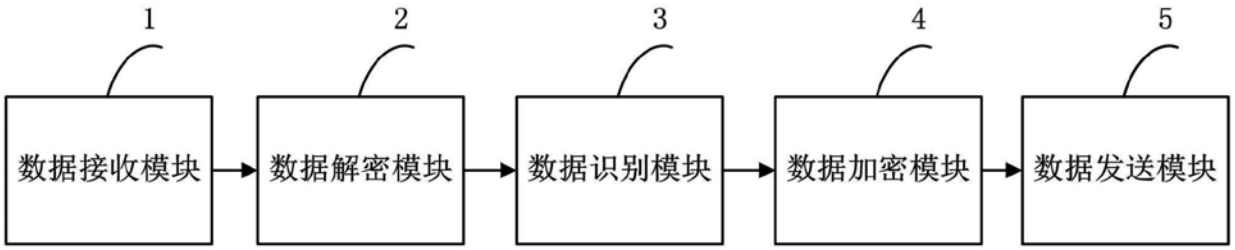

1
2
3
4
5
数据接收模块
数据解密模块
数据识别模块
数据加密模块
数据发送模块

图7

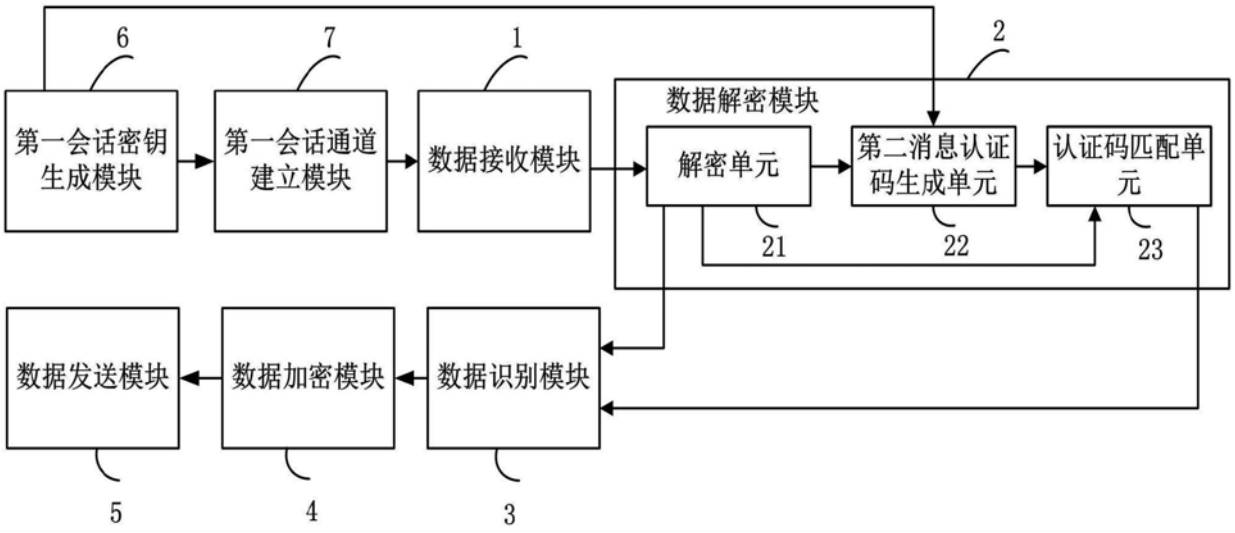

6
7
1
2
第一会话密钥生成模块
第一会话通道建立模块
数据接收模块
数据解密模块
解密单元
第二消息认证码生成单元
认证码匹配单元
21
22
23
数据发送模块
数据加密模块
数据识别模块
5
4
3

图8

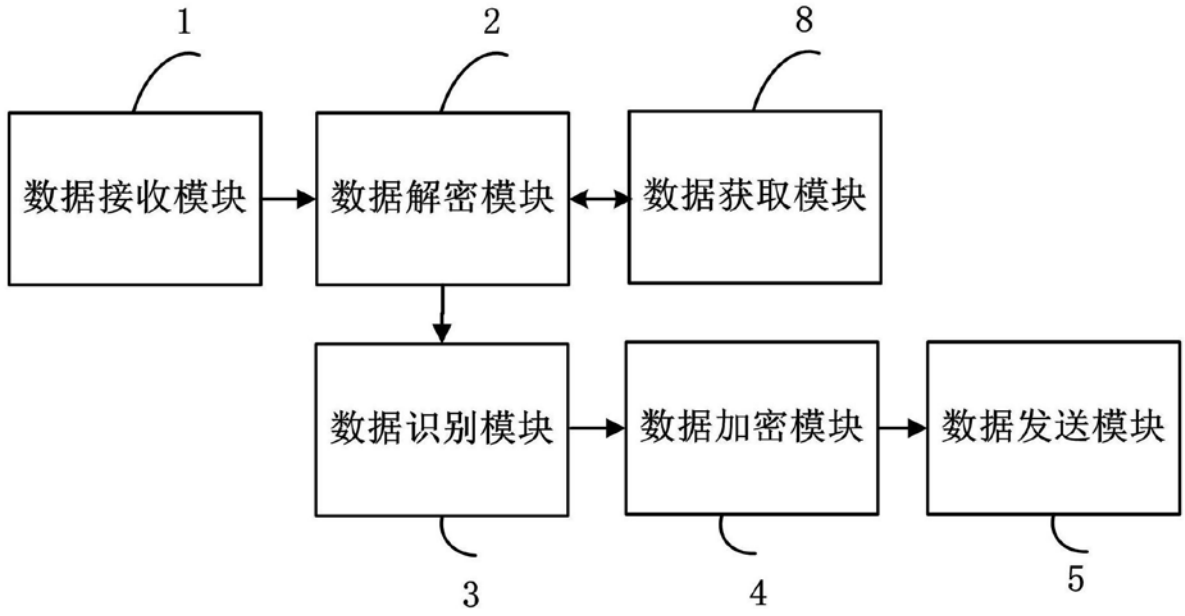

1
2
8
数据接收模块
数据解密模块
数据获取模块
数据识别模块
数据加密模块
数据发送模块
3
4
5

图9

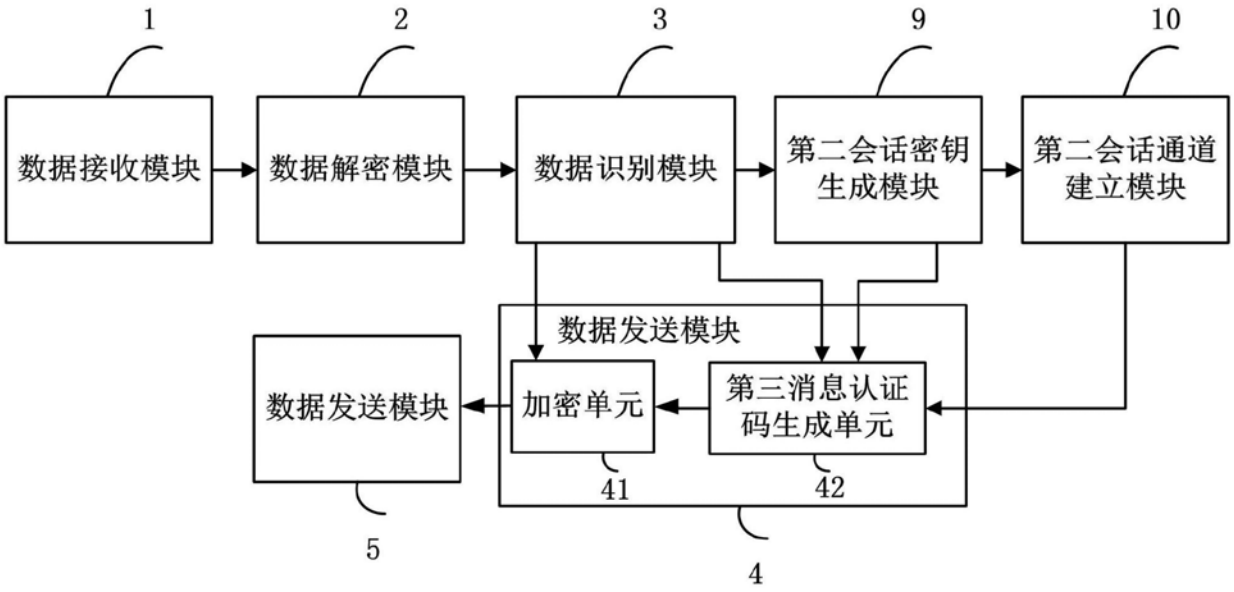

1
2
3
9
10
数据接收模块
数据解密模块
数据识别模块
第二会话密钥生成模块
第二会话通道建立模块
数据发送模块
数据发送模块
加密单元
第三消息认证码生成单元
41
42
5
4

图10