



(12) 发明专利

(10) 授权公告号 CN 113242549 B

(45) 授权公告日 2022. 10. 28

(21) 申请号 202110472861.X

(56) 对比文件

(22) 申请日 2021.04.29

CN 102348017 A, 2012.02.08

(65) 同一申请的已公布的文献号

审查员 白雪慧

申请公布号 CN 113242549 A

(43) 申请公布日 2021.08.10

(73) 专利权人 中国联合网络通信集团有限公司

地址 100033 北京市西城区金融大街21号

(72) 发明人 刘煜 翟京卿

(74) 专利代理机构 北京天昊联合知识产权代理

有限公司 11112

专利代理师 彭瑞欣 冯建基

(51) Int. Cl.

H04W 12/0433 (2021.01)

H04W 12/37 (2021.01)

H04W 12/40 (2021.01)

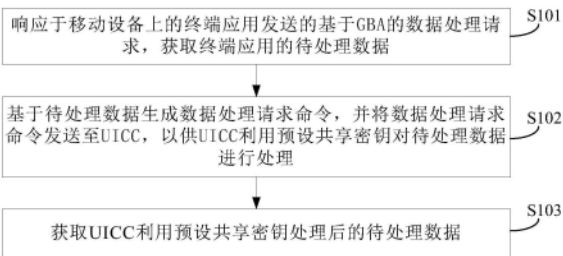
权利要求书3页 说明书15页 附图7页

(54) 发明名称

数据处理方法、移动设备、UICC及终端

(57) 摘要

本发明提供一种数据处理方法,涉及通信技术领域,包括:响应于所述移动设备上的终端应用发送的基于GBA的数据处理请求,获取所述终端应用的待处理数据;基于所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC,以供所述UICC利用预设共享密钥对所述待处理数据进行处理;获取所述UICC利用所述预设共享密钥处理后的所述待处理数据。本发明还提供一种移动设备、UICC及终端。



1. 一种数据处理方法,其特征在于,应用于用户终端的移动设备,所述用户终端包括所述移动设备和UICC,所述数据处理方法包括:

响应于所述移动设备上的终端应用发送的基于GBA的数据处理请求,获取所述终端应用的待处理数据;

基于所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC,以供所述UICC利用预设共享密钥对所述待处理数据进行处理;其中,所述待处理数据包括多个第一待处理数据块,所述数据处理请求命令包括多个数据处理请求子命令,每个所述数据处理请求子命令对应包括一个所述第一待处理数据块;

获取所述UICC利用所述预设共享密钥处理后的所述待处理数据;其中,所述处理后的所述待处理数据包括多个第二待处理数据块。

2. 根据权利要求1所述的方法,其特征在于,所述根据所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC的步骤,包括:

针对多个所述第一待处理数据块中的当前所述第一待处理数据块,根据当前所述第一待处理数据块生成当前所述数据处理请求子命令;

向所述UICC发送当前所述数据处理请求子命令,当前所述数据处理请求子命令包括当前所述第一待处理数据块;

响应于所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块,以及

执行所述根据当前所述第一待处理数据块生成当前所述数据处理请求子命令的步骤。

3. 根据权利要求1所述的方法,其特征在于,所述根据所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC的步骤,包括:

根据完整的所述待处理数据生成所述数据处理请求命令,所述数据处理请求命令包含完整的所述待处理数据;

向所述UICC发送包含完整的所述待处理数据的所述数据处理请求命令。

4. 根据权利要求2所述的方法,其特征在于,所述向所述UICC发送当前所述数据处理请求子命令的步骤之后,还包括:

接收所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息;

若所述当前第一命令响应消息指示重传当前所述第一待处理数据块,则执行所述根据当前所述第一待处理数据块生成当前所述数据处理请求子命令的步骤;

若所述当前第一命令响应消息指示发送下一个所述第一待处理数据块,则执行所述响应于所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块的步骤。

5. 根据权利要求1所述的方法,其特征在于,所述获取所述UICC利用所述预设共享密钥处理后的所述待处理数据的步骤,包括:

接收所述UICC返回的数据处理响应消息,所述数据处理响应消息包含所述处理后的所述待处理数据。

6. 根据权利要求1所述的方法,其特征在于,所述获取所述UICC利用所述预设共享密钥

处理后的所述待处理数据的步骤,包括:

接收所述UICC返回的当前数据处理响应消息,当前数据处理响应消息包含多个第二待处理数据块中的当前所述第二待处理数据块,以及用于指示通过发送命令获取下一个所述第二待处理数据块的信息;

检测所述当前数据处理响应消息是否存在异常;

若检测出所述当前数据处理响应消息存在异常,生成用于指示所述UICC重传当前第二待处理数据块的当前数据获取请求命令,并向所述UICC发送该当前数据获取请求命令,以供所述UICC响应于该当前数据获取请求命令,基于当前所述第二待处理数据块重新生成当前数据处理响应消息;

若检测出所述当前数据处理响应消息不存在异常,生成用于指示所述UICC传送下一个所述第二待处理数据块的当前数据获取请求命令,并向所述UICC发送该当前数据获取请求命令,以供所述UICC响应于该当前数据获取请求命令,将下一个所述第二待处理数据块作为当前所述第二待处理数据块,并基于当前所述第二待处理数据块生成当前数据处理响应消息;

执行所述接收所述UICC返回的当前数据处理响应消息的步骤。

7.一种数据处理方法,其特征在于,应用于用户终端的UICC,所述用户终端包括移动设备和所述UICC,所述数据处理方法包括:

接收所述移动设备发送的数据处理请求命令,所述数据处理请求命令为所述移动设备基于终端应用发送的基于GBA的待处理数据生成的命令;其中,所述待处理数据包括多个第一待处理数据块,所述数据处理请求命令包括多个数据处理请求子命令,每个所述数据处理请求子命令对应包括一个所述第一待处理数据块;

利用预设共享密钥对所述待处理数据进行处理;

将处理后的所述待处理数据发送至所述移动设备;其中,所述处理后的所述待处理数据包括多个第二待处理数据块。

8.根据权利要求7所述的方法,其特征在于,所述接收所述移动设备发送的数据处理请求命令的步骤包括:

接收所述移动设备发送的当前所述数据处理请求子命令,当前所述数据处理请求子命令包括当前所述第一待处理数据块;

响应于当前所述数据处理请求子命令,生成当前第一命令响应消息,并将所述当前第一命令响应消息发送至所述移动设备,以供所述移动设备针对当前所述第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块,并根据当前所述第一待处理数据块生成当前所述数据处理请求子命令;

执行所述接收所述移动设备发送的当前所述数据处理请求子命令的步骤。

9.根据权利要求7所述的方法,其特征在于,所述接收所述移动设备发送的数据处理请求命令的步骤包括:

接收所述移动设备发送的数据处理请求命令,所述数据处理请求命令为所述移动设备根据完整的所述待处理数据生成,所述数据处理请求命令包含完整的所述待处理数据。

10.根据权利要求8所述的方法,其特征在于,所述接收所述移动设备发送的当前所述数据处理请求子命令的步骤之后,还包括:

检测当前所述数据处理请求子命令是否存在异常；

若检测出当前所述数据处理请求子命令存在异常，则生成用于指示所述移动设备重传当前所述第一待处理数据块的当前第一命令响应消息，以供所述移动设备根据当前所述第一待处理数据块生成当前所述数据处理请求子命令；

若检测出当前所述数据处理请求子命令不存在异常，则生成用于指示所述移动设备传送下一个所述第一待处理数据块的当前第一命令响应消息，以供所述移动设备针对当前所述第一命令响应消息，将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块，并根据当前所述第一待处理数据块生成当前所述数据处理请求子命令。

11. 根据权利要求7所述的方法，其特征在于，所述将处理后的所述待处理数据发送至所述移动设备的步骤包括：

根据处理后的所述待处理数据生成数据处理响应消息，所述数据处理响应消息包括处理后的所述待处理数据；

将所述数据处理响应消息发送至所述移动设备。

12. 根据权利要求7所述的方法，其特征在于，所述将处理后的所述待处理数据发送至所述移动设备的步骤包括：

针对多个所述第二待处理数据块中的当前所述第二待处理数据块，根据当前所述第二待处理数据块生成当前数据处理响应消息；

向所述移动设备发送当前所述数据处理响应消息，当前所述数据处理响应消息包括当前所述第二待处理数据块；

响应于所述移动设备针对当前所述数据处理响应消息返回的当前数据获取请求命令指示传送下一个所述第二待处理数据块，将多个所述第二待处理数据块中的下一个所述第二待处理数据块作为当前所述第二待处理数据块，并执行所述根据当前所述第二待处理数据块生成当前数据处理响应消息的步骤；

响应于所述移动设备针对当前所述数据处理响应消息返回的当前数据获取请求命令指示重传当前所述第二待处理数据块，直接执行所述根据当前所述第二待处理数据块生成当前数据处理响应消息的步骤。

13. 根据权利要求7-12任一项所述的方法，其特征在于，所述预设共享密钥为Ks_int_NAF密钥。

14. 一种移动设备，其特征在于，包括：存储模块和至少一个处理器，所述存储模块中存储有计算机程序，所述计算机程序被至少一个所述处理器执行时实现权利要求1-6中任一项所述的数据处理方法。

15. 一种UICC，其特征在于，包括：存储模块和至少一个处理器，所述存储模块中存储有计算机程序，所述计算机程序被至少一个所述处理器执行时实现权利要求7-13中任一项所述的数据处理方法。

16. 一种终端，其特征在于，包括移动设备和UICC，其中，所述移动设备采用权利要求14所述的移动设备，所述UICC采用权利要求15所述的UICC。

数据处理方法、移动设备、UICC及终端

技术领域

[0001] 本发明涉及通信技术领域,具体涉及一种数据处理方法、移动设备、UICC及终端。

背景技术

[0002] 在第三代无线通信标准中,通用鉴权框架(Generic Authentication Architecture,简称GAA)是多种应用业务实体使用的一个用于完成对用户身份进行验证的通用结构,应用GAA可实现用户终端(UE)与应用服务器(Network Application Function,简称NAF)之间的通信加密处理。GAA包含两种认证机制,一种为基于通信实体间的共享密钥进行认证(General Bootstrapping Architecture,简称GBA),另一种为基于公钥的证书进行认证。GBA机制通过生成UE与NAF之间的共享密钥,而使UE与NAF之间通过共享密钥进行通信。根据UE的实体能力和分工不同,GBA可分为GBA_ME和GBA_U两种,其中,UE的实体包括移动设备(Mobile Equipment,ME)和通用集成电路卡(Universal Integrated Circuit Card,简称UICC),GBA_ME是指密钥的协商和生成在UE的移动设备(简称ME)上完成,GBA_U是指密钥的协商和生成都在UICC上完成,GBA_U相较于GBA_ME具有更高的安全性。

[0003] 在GBA_U机制下,UICC生成的共享密钥包含两个,其中一个共享密钥存储于UICC中,不泄露给UE的ME,而另一个共享密钥则由UICC发送至ME进行存储。现有技术中,对于UE的移动设备和UICC相互关联的应用而言,UE中安装于ME中的应用在与NAF进行通信时,通常将存储于ME中的密钥作为共享密钥,而安装于UICC中的应用在与NAF进行通信时,通常将存储于UICC中的密钥作为共享密钥,ME侧的应用和UICC侧的应用共同支撑业务功能的实现,如UICC侧的应用提供安全能力、证书的存储和使用等,ME侧的应用提供用户服务和本地管理等。在这种情况下,ME侧的应用和UICC侧的应用均可能需要进行GBA业务,如ME侧的应用的接入认证业务和UICC侧的应用的证书加密传输业务等。在进行GBA业务过程中,对于ME应用和UICC应用公用的NAF来说,NAF也需要使用不同的共享密钥来分别对ME应用的通信数据和UICC应用的通信数据进行数据处理,这导致NAF管理共享密钥的复杂度较高,不便于对共享密钥进行统一管理。

发明内容

[0004] 本发明旨在至少解决现有技术中存在的技术问题之一,提出了一种数据处理方法、移动设备、UICC及终端。

[0005] 第一方面,本发明提供一种数据处理方法,应用于用户终端的移动设备,所述用户终端包括所述移动设备和UICC,所述数据处理方法包括:

[0006] 响应于所述移动设备上的终端应用发送的基于GBA的数据处理请求,获取所述终端应用的待处理数据;

[0007] 基于所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC,以供所述UICC利用预设共享密钥对所述待处理数据进行处理;

[0008] 获取所述UICC利用所述预设共享密钥处理后的所述待处理数据。

[0009] 优选的,所述待处理数据包括多个第一待处理数据块,所述数据处理请求命令包括多个数据处理请求子命令,每个所述数据处理请求子命令对应包括一个所述第一待处理数据块;

[0010] 所述根据所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC的步骤,包括:

[0011] 针对多个所述第一待处理数据块中的当前所述第一待处理数据块,根据当前所述第一待处理数据块生成当前所述数据处理请求子命令;

[0012] 向所述UICC发送当前所述数据处理请求子命令,当前所述数据处理请求子命令包括当前所述第一待处理数据块;

[0013] 响应于所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块,以及

[0014] 执行所述根据当前所述第一待处理数据块生成当前所述数据处理请求子命令的步骤。

[0015] 优选的,所述根据所述待处理数据生成数据处理请求命令,并将所述数据处理请求命令发送至所述UICC的步骤,包括:

[0016] 根据完整的所述待处理数据生成所述数据处理请求命令,所述数据处理请求命令包含完整的所述待处理数据;

[0017] 向所述UICC发送包含完整的所述待处理数据的所述数据处理请求命令。

[0018] 优选的,所述向所述UICC发送当前所述数据处理请求子命令的步骤之后,还包括:

[0019] 接收所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息;

[0020] 若所述当前第一命令响应消息指示重传当前所述第一待处理数据块,则执行所述根据当前所述第一待处理数据块生成当前所述数据处理请求子命令的步骤;

[0021] 若所述当前第一命令响应消息指示发送下一个所述第一待处理数据块,则执行所述响应于所述UICC针对当前所述数据处理请求子命令返回的当前第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块的步骤。

[0022] 优选的,所述获取所述UICC利用所述预设共享密钥处理后的所述待处理数据的步骤,包括:

[0023] 接收所述UICC返回的数据处理响应消息,所述数据处理响应消息包含所述处理后的所述待处理数据。

[0024] 优选的,所述处理后的所述待处理数据包括多个第二待处理数据块;

[0025] 所述获取所述UICC利用所述预设共享密钥处理后的所述待处理数据的步骤,包括:

[0026] 接收所述UICC返回的当前数据处理响应消息,当前数据处理响应消息包含多个第二待处理数据块中的当前所述第二待处理数据块,以及用于指示通过发送命令获取下一个所述第二待处理数据块的信息;

[0027] 检测所述当前数据处理响应消息是否存在异常;

[0028] 若检测出所述当前数据处理响应消息存在异常,生成用于指示所述UICC重传当前

第二待处理数据块的当前数据获取请求命令,并向所述UICC发送该当前数据获取请求命令,以供所述UICC响应于该当前数据获取请求命令,基于当前所述第二待处理数据块重新生成当前数据处理响应消息;

[0029] 若检测出所述当前数据处理响应消息不存在异常,生成用于指示所述UICC传送下一个所述第二待处理数据块的当前数据获取请求命令,并向所述UICC发送该当前数据获取请求命令,以供所述UICC响应于该当前数据获取请求命令,将下一个所述第二待处理数据块作为当前所述第二待处理数据块,并基于当前所述第二待处理数据块生成当前数据处理响应消息;

[0030] 执行所述接收所述UICC返回的当前数据处理响应消息的步骤。

[0031] 第二方面,本发明还提供一种数据处理方法,应用于用户终端的UICC,所述用户终端包括移动设备和所述UICC,所述数据处理方法包括:

[0032] 接收所述移动设备发送的数据处理请求命令,所述数据处理请求命令为所述移动设备基于终端应用发送的基于GBA的待处理数据生成的命令;

[0033] 利用预设共享密钥对所述待处理数据进行处理;

[0034] 将处理后的所述待处理数据发送至所述移动设备。

[0035] 优选的,所述待处理数据包括多个第一待处理数据块,所述数据处理请求命令包括多个数据处理请求子命令,每个所述数据处理请求子命令对应包括一个所述第一待处理数据块;

[0036] 所述接收所述移动设备发送的数据处理请求命令的步骤包括:

[0037] 接收所述移动设备发送的当前所述数据处理请求子命令,当前所述数据处理请求子命令包括当前所述第一待处理数据块;

[0038] 响应于当前所述数据处理请求子命令,生成当前第一命令响应消息,并将所述当前第一命令响应消息发送至所述移动设备,以供所述移动设备针对当前所述第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据块作为当前所述第一待处理数据块,并根据当前所述第一待处理数据块生成当前所述数据处理请求子命令;

[0039] 执行所述接收所述移动设备发送的当前所述数据处理请求子命令的步骤。

[0040] 优选的,所述接收所述移动设备发送的数据处理请求命令的步骤包括:

[0041] 接收所述移动设备发送的数据处理请求命令,所述数据处理请求命令为所述移动设备根据完整的所述待处理数据生成,所述数据处理请求命令包含完整的所述待处理数据。

[0042] 优选的,所述接收所述移动设备发送的当前所述数据处理请求子命令的步骤之后,还包括:

[0043] 检测当前所述数据处理请求子命令是否存在异常;

[0044] 若检测出当前所述数据处理请求子命令存在异常,则生成用于指示所述移动设备重传当前所述第一待处理数据块的当前第一命令响应消息,以供所述移动设备根据当前所述第一待处理数据块生成当前所述数据处理请求子命令;

[0045] 若检测出当前所述数据处理请求子命令不存在异常,则生成用于指示所述移动设备传送下一个所述第一待处理数据块的当前第一命令响应消息,以供所述移动设备针对当前所述第一命令响应消息,将多个所述第一待处理数据块中的下一个所述第一待处理数据

块作为当前所述第一待处理数据块,并根据当前所述第一待处理数据块生成当前所述数据处理请求子命令。

[0046] 优选的,所述将处理后的所述待处理数据发送至所述移动设备的步骤包括:

[0047] 根据处理后的所述待处理数据生成数据处理响应消息,所述数据处理响应消息包括处理后的所述待处理数据;

[0048] 将所述数据处理响应消息发送至所述移动设备。

[0049] 优选的,所述处理后的所述待处理数据包括多个第二待处理数据块;

[0050] 所述将处理后的所述待处理数据发送至所述移动设备的步骤包括:

[0051] 针对多个所述第二待处理数据块中的当前所述第二待处理数据块,根据当前所述第二待处理数据块生成当前数据处理响应消息;

[0052] 向所述移动设备发送当前所述数据处理响应消息,当前所述数据处理响应消息包括当前所述第二待处理数据块;

[0053] 响应于所述移动设备针对当前所述数据处理响应消息返回的当前数据获取请求命令指示传送下一个所述第二待处理数据块,将多个所述第二待处理数据块中的下一个所述第二待处理数据块作为当前所述第二待处理数据块,并

[0054] 执行所述根据当前所述第二待处理数据块生成当前数据处理响应消息的步骤;

[0055] 响应于所述移动设备针对当前所述数据处理响应消息返回的当前数据获取请求命令指示重传当前所述第二待处理数据块,直接执行所述根据当前所述第二待处理数据块生成当前数据处理响应消息的步骤。

[0056] 优选的,所述预设共享密钥为Ks_int_NAF密钥。

[0057] 第三方面,本发明提供一种移动设备,包括:存储模块和至少一个处理器,所述存储模块中存储有计算机程序,所述计算机程序被至少一个所述处理器执行时实现第一方面所提供的数据处理方法。

[0058] 第四方面,本发明提供一种UICC,包括:存储模块和至少一个处理器,所述存储模块中存储有计算机程序,所述计算机程序被至少一个所述处理器执行时实现本发明第二方面所提供的数据处理方法。

[0059] 第五方面,本发明还提供一种终端,包括移动设备和UICC,其中,所述移动设备采用本发明第三方面所提供的移动设备,所述UICC采用本发明第四方面所提供的UICC。

[0060] 本发明的有益技术效果:

[0061] 本发明提供的数据处理方法、移动设备、UICC及终端,安装于移动设备上的终端应用在基于GBA机制下需要与应用服务器进行通信时,将待处理数据发送至移动设备,移动设备基于该待处理数据生成基于GBA的数据处理请求命令,并将该数据处理请求命令发送至UICC,UICC响应于该数据处理请求命令而利用自身存储的预设共享密钥来对待处理数据进行处理,并将处理后的待处理数据返回至移动设备,以供终端应用使用,本发明实现了利用UICC内存储的共享密钥来对安装于移动设备中的终端应用的通信数据进行处理的过程,相较于现有技术,避免了使用不同的共享密钥来对用户终端上安装于不同模块(移动设备和UICC)的应用的通信数据进行处理,从而降低了应用服务器管理共享密钥的复杂度,实现了密钥的统一管理。

附图说明

- [0062] 图1为本发明实施例提供的一种用户终端的结构示意图；
- [0063] 图2为本发明实施例提供的一种数据处理方法的流程图；
- [0064] 图3为本发明实施例提供的另一种数据处理方法的流程图；
- [0065] 图4为本发明实施例提供的又一种数据处理方法的流程图；
- [0066] 图5为本发明实施例提供的再一种数据处理方法的流程图；
- [0067] 图6为本发明实施例提供的再一种数据处理方法的流程图；
- [0068] 图7为本发明实施例提供的再一种数据处理方法的流程图；
- [0069] 图8为本发明实施例提供的再一种数据处理方法的流程图；
- [0070] 图9为本发明实施例提供的再一种数据处理方法的流程图。

具体实施方式

[0071] 为使本领域的技术人员更好地理解本发明的技术方案,下面结合附图来对本发明提供的数据处理方法、移动设备、UICC及终端进行详细描述。

[0072] 本发明提供的数据处理方法用于处理用户终端与应用服务器进行通信时所涉及的数据,数据处理过程主要在用户终端内进行。图1为本发明实施例提供的一种用户终端的结构示意图,如图1所示,本发明中的用户终端(UE)具体包括移动设备1和UICC2,其中,UICC(Universal Integrated Circuit Card,通用集成电路卡)是一个通用智能卡平台,其上驻留有多种应用,例如USIM、银行及票务等智能卡应用,UICC为其上层应用提供统一的底层支撑。

[0073] 下面将分别以移动设备和UICC作为执行主体来对本发明提供的数据处理方法进行详细描述。

[0074] 图2为本发明实施例提供的一种数据处理方法的流程图,本实施例基于用户终端中的移动设备实现,如图2所示,该方法包括:

[0075] 步骤S101、响应于移动设备上的终端应用发送的基于GBA的数据处理请求,获取终端应用的待处理数据。

[0076] GBA((General Bootstrapping Architecture,简称GBA))为一种基于通信实体间的共享密钥进行认证的认证机制,GBA机制通过生成UE与NAF之间的共享密钥,而使UE与NAF之间通过该共享密钥进行通信,GBA因UICC功能的不同而分为GBA_ME和GBA_U两种,本发明实施例特别涉及GBA_U机制下的数据处理过程,GBA_U是指密钥的协商和生成都在UICC上完成的GBA过程。

[0077] 本发明实施例中,当安装于移动设备上的终端应用需要与应用服务器进行通信时,其向移动设备发送数据处理请求,该数据处理请求是基于GBA机制下的数据处理请求,移动设备在接收到终端应用发送的基于GBA的数据处理请求后,获取终端应用的待处理数据,优选的,移动设备获取终端应用的待处理数据的方式可以是终端应用通过基于GBA的数据处理请求将待处理数据发送至移动设备。

[0078] 步骤S102、基于待处理数据生成数据处理请求命令,并将数据处理请求命令发送至UICC,以供UICC利用预设共享密钥对待处理数据进行处理。

[0079] 移动设备在获取到待处理数据后,基于该待处理数据生成数据处理请求命令,并

将该数据处理请求命令发送至UICC,UICC通过该数据处理请求命令获取到待处理数据,并且UICC响应于该数据处理请求命令而利用自身存储的预设共享密钥来对待处理数据进行处理,具体的,该处理过程包括数据加密、身份认证等。

[0080] 本发明实施例中,数据处理请求命令是移动设备和UICC之间在GBA场景下的数据交互命令,满足了终端应用的待处理数据使用存储于UICC中的共享密钥来进行处理的要求,该数据处理请求命令可基于预设的第一命令格式生成。

[0081] 步骤S103、获取UICC利用预设共享密钥处理后的待处理数据。

[0082] UICC在对待处理数据进行处理后,将处理后的待处理数据返回至移动设备,以供移动设备上安装的终端应用使用。优选的,UICC可通过生成与上述数据处理请求命令对应的响应命令来将处理后的待处理数据反馈至移动设备。

[0083] 本发明实施例中,安装于移动设备上的终端应用在基于GBA机制下需要与应用服务器进行通信时,将待处理数据发送至移动设备,移动设备基于该待处理数据生成基于GBA的数据处理请求命令,并将该数据处理请求命令发送至UICC,UICC响应于该数据处理请求命令而利用自身存储的预设共享密钥来对待处理数据进行处理,并将处理后的待处理数据返回至移动设备,以供终端应用使用,本发明实施例实现了利用UICC内存储的共享密钥来对安装于移动设备中的终端应用的通信数据进行处理的过程,相较于现有技术,避免了使用不同的共享密钥来对用户终端上安装于不同模块(移动设备和UICC)的应用的通信数据进行处理,从而降低了应用服务器管理共享密钥的复杂度,实现了密钥的统一管理。

[0084] 在一些实施例中,当终端应用的待处理数据的数据量较大时,移动设备在基于待处理数据生成数据处理请求命令并发送至UICC时可基于数据分块传输的方式实现。即,将待处理数据被分割为多个第一待处理数据块,对应的,数据处理请求命令包括多个数据处理请求子命令,每个数据处理请求子命令对应包括一个第一待处理数据块。具体的,如图3所示,图3为本发明实施例提供的另一种数据处理方法的流程图,本实施例在图2所示实施例的基础上,步骤S102可具体包括:

[0085] 步骤S1021、针对多个第一待处理数据块中的当前第一待处理数据块,根据当前第一待处理数据块生成当前数据处理请求子命令。

[0086] 步骤S1022、向UICC发送当前数据处理请求子命令。

[0087] 步骤S1023、响应于UICC针对当前数据处理请求子命令返回的当前第一命令响应消息,将多个第一待处理数据块中的下一个第一待处理数据块作为当前第一待处理数据块,并返回执行步骤S1021。

[0088] 在一些实施例中,待处理数据被分割为多个第一待处理数据块后,移动设备对该多个第一待处理数据块进行顺序处理,其中,当前第一待处理数据块是指多个第一待处理数据块中马上要被处理的数据块。

[0089] 在步骤S1021中,移动设备基于预设的第一命令格式,根据当前第一待处理数据块生成当前数据处理请求子命令,该当前数据处理请求子命令中包括当前第一待处理数据块;在步骤S1023中,当UICC接收到该当前数据处理请求子命令后,生成当前第一命令响应消息,并将该当前第一命令响应消息反馈至移动设备,移动设备在接收待该当前第一命令响应消息后,将多个第一待处理数据块中下一个第一待处理数据块作为当前第一待处理数据块,并返回执行步骤S1021,直至将全部第一待处理数据块均通过数据处理请求子命令的

方式成功发送至UICC。其中,下一个第一待处理数据块是指按照预设顺序排列的多个第一待处理数据中排在当前第一待处理数据块顺序之后的即将要被处理的第一待处理数据块,在实际应用中,为便于顺序提取第一待处理数据块,可在将待处理数据分割为多个第一待处理数据块后,对多个第一待处理数据块按顺序进行编号,在数据处理过程中按该编号的顺序提取第一待处理数据块。

[0090] 在一些实施例中,在UICC侧,UICC在接收到当前数据处理请求子命令后,基于当前数据处理请求子命令判断移动设备中当前是否还剩余有第一待处理数据块需要发送,该判断过程可通过识别当前数据处理请求子命令中的相关字段来确定,例如,在当前数据处理请求子命令中设置某一字段用来标识剩余数据块的数量,UICC检测该字段以确定出剩余数据块的数量。当UICC判断出移动设备中当前还剩余有第一待处理数据块需要发送时,UICC将生成第一命令响应消息,以使移动设备响应该第一命令响应消息而继续发送剩余第一待处理数据块,而当判断出移动设备中的第一待处理数据块已发送完时,UICC将不再生成第一命令响应消息返回至移动设备,而是执行对待处理数据进行处理的过程,此时,上述步骤S1021~S1023的循环结束。

[0091] 在一些实施例中,当待处理数据的数据量较小时,可不对待处理数据进行分割而直接根据待处理数据生成数据处理请求命令。即,步骤S102包括:根据完整的待处理数据生成数据处理请求命令,并向UICC发送包含完整的待处理数据的数据处理请求命令。本实施例中,根据完整的待处理数据生成数据处理请求命令的过程与上一实施例中基于第一待处理数据块生成数据处理请求子命令的过程相似,两种命令皆为基于预设的第一命令格式生成的命令。

[0092] 在一些实施例中,在移动设备将待处理数据分块传输至UICC的过程中,移动设备所发送的当前数据处理请求子命令可能发生异常,在此情况下,移动设备需要重新基于当前第一待处理数据块生成当前数据处理请求子命令并发送至UICC。具体的,如图4所示,图4为本发明实施例提供的又一种数据处理方法的流程图,本实施例在图3所示实施例的基础上,在步骤S1022之后,还包括:

[0093] 步骤S1022a、接收UICC针对当前数据处理请求子命令返回的当前第一命令响应消息。

[0094] 步骤S1022b、识别当前第一命令响应消息为指示重传当前第一待处理数据块或者指示传输下一个第一待处理数据块。

[0095] 当识别出当前第一命令响应消息为指示重传(重新传输)当前第一待处理数据块时,返回执行步骤S1021;当识别出当前第一命令响应消息为指示传输下一个第一待处理数据块时,则执行步骤S1023。

[0096] 本发明实施例中,数据处理请求子命令可能发生的异常包括命令中的数据格式错误和包含的第一待处理数据块不完整等等。数据处理请求子命令发生异常将导致UICC无法从数据处理请求子命令中获取到对应的完整的第一待处理数据块和/或UICC无法响应于该数据处理请求子命令而对对应的第一待处理数据块进行处理。因此,本发明实施例中,当移动设备将当前数据处理请求子命令发送至UICC后,UICC侧将对该当前数据处理请求子命令进行检测以确定该当前数据处理请求子命令是否存在异常,例如,UICC通过检测当前数据处理请求子命令的各字段是否符合预设规范来确定该当前数据处理请求子命令是否发生

格式错误,以及通过检测当前数据处理请求子命令中所包含的第一待处理数据块的大小是否等于预设大小来确定该第一待处理数据块是否完整,等等。

[0097] UICC在对当前数据处理请求子命令检测完成后,根据检测结果生成包含不同信息的当前第一命令响应消息,该当前第一命令响应消息所包含的信息可包括两种,一种用于指示移动设备重传当前第一待处理数据块,另一种用于指示移动设备传送下一个第一待处理数据块。在UICC检测出当前数据处理请求子命令存在异常时,则当前第一命令响应消息中包含用于指示移动设备重传当前第一待处理数据块的信息;在UICC检测出当前数据处理请求子命令不存在异常时,且UICC识别出移动设备当前还剩余有第一待处理数据块需要发送,则当前第一命令响应消息中包含用于指示移动设备传送下一个第一待处理数据块的信息。在实际应用中,当前第一命令响应消息所包含的不同信息可通过设置其对应的参数不同来实现。

[0098] 本发明实施例通过在数据处理请求子命令发生错误、异常时,重新生成数据处理请求子命令并发送至UICC,保证了传输至UICC的待处理数据的完整性,以及能够正确触发UICC对待处理数据进行处理。

[0099] 本发明实施例中,移动设备在将完整的待处理数据发送至UICC,且UICC接收到完整的待处理数据并完成处理后,移动设备将从UICC处获取处理后的待处理数据,如图2中的步骤S103。

[0100] 作为步骤S103的一种可选实施方式,步骤S103具体包括:接收UICC返回的数据处理响应消息,该数据处理响应消息包含处理后的待处理数据。即,UICC基于处理后的待处理数据生成数据处理响应消息,该数据处理响应消息包含处理后的待处理数据,UICC将该数据处理响应消息发送至移动设备,移动设备接收该数据处理响应消息,并从该数据处理响应消息中获取处理后的待处理数据。该实施方式适用于处理后的待处理数据的数据量不大的情况。

[0101] 作为步骤S103的另一种可选的实施方式,当处理后的待处理数据的数据量较大时,UICC可以将处理后的待处理数据分块返回给移动设备,即移动设备可分多次从UICC处获取处理后的待处理数据。具体的,如图5所示,图5为本发明实施例提供的再一种数据处理方法的流程图,本实施例中,处理后的待处理数据包括多个第二待处理数据块,即,UICC在对待处理数据完成处理后,将处理后的待处理数据分割为多个第二待处理数据块。本实施例在图2所示实施例的基础上,步骤S103具体包括:

[0102] 步骤S1031、接收UICC返回的当前数据处理响应消息。

[0103] 当前数据处理响应消息包含多个第二待处理数据块中的当前第二待处理数据块,其中,当前第二待处理数据块是指多个第二待处理数据块中马上要被传输的数据块;该数据处理响应消息用于指示移动设备通过发送命令获取下一个第二待处理数据块的信息,而当所有第二待处理数据块已发送完毕时,该数据处理响应消息还用于提示移动设备所有第二待处理数据块已发送完毕。

[0104] 步骤S1032、检测当前数据处理响应消息是否存在异常。

[0105] 在实际应用中,UICC在将第二待处理数据块返回至移动设备的过程中,UICC所发送的当前数据处理响应消息可能存在异常,在此情况下,移动设备需要生成重新获取当前第二待处理数据块的命令,以使UICC重传当前第二待处理数据块。其中,当前数据处理响应

消息可能存在的异常请参照上述图4所示实施例中对数据处理请求子命令的异常情况的描述,此处不再赘述。

[0106] 在步骤S1032中,当检测出当前数据处理响应消息存在异常时,则生成用于指示UICC重传当前第二待处理数据块的当前数据获取请求命令,并向UICC发送该当前数据获取请求命令,以供UICC响应于该当前数据获取请求命令,基于当前第二待处理数据块重新生成当前数据处理响应消息;而当检测出当前数据处理响应消息不存在异常时,则执行下述步骤S1033,以进行下一个第二待处理数据块的传输。

[0107] 步骤S1033、识别当前数据处理响应消息是指示通过发送命令获取下一个第二待处理数据块还是提示所有第二待处理数据块已发送完毕。

[0108] 当识别出当前数据处理响应消息为指示通过发送命令获取下一个第二待处理数据块时,执行步骤S1034,并顺序返回执行步骤S1031;而当识别出当前数据处理响应消息为提示所有第二待处理数据块已发送完毕时,则结束流程。

[0109] 步骤S1034、响应于当前数据处理响应消息,生成用于指示UICC传送下一个第二待处理数据块的当前数据获取请求命令,并向UICC发送当前数据获取请求命令。

[0110] UICC响应于当前数据获取请求命令,将下一个第二待处理数据块作为当前第二待处理数据块,并基于当前第二待处理数据块生成当前数据处理响应消息。

[0111] 本发明实施例中,移动设备在识别出当前数据处理响应消息为指示通过发送命令获取下一个第二待处理数据块时,基于预设的第一命令格式生成数据获取请求命令,并发送至UICC。

[0112] 在一些实施例中,UICC每次接收到数据获取请求命令后,均判断当前是否仅剩余一个第二待处理数据块未发送,当判断出当前仅剩余一个第二待处理数据块未发送时,则将下一个第二待处理数据块(最后一个待处理数据块)作为当前第二待处理数据块,并基于当前第二待处理数据块生成用于提示移动设备所有第二待处理数据块已发送完毕的当前数据处理响应消息,并发送至移动设备;而当判断出当前还剩余多个第二待处理数据块未发送时,则将下一个第二待处理数据块作为当前第二待处理数据块,并基于当前第二待处理数据块生成用于指示移动设备通过发送命令获取下一个第二待处理数据块的当前数据处理响应消息,并发送至移动设备。

[0113] 在一些实施例中,UICC每次接收到数据获取请求命令后,均判断当前是否还存在未发送的第二待处理数据块,若存在,则将下一个第二待处理数据块作为当前第二待处理数据块,并基于当前第二待处理数据块生成当前数据处理响应消息,该当前数据处理响应消息包含当前第二待处理数据块及用于指示移动设备通过发送命令获取下一个第二待处理数据块的信息;若不存在,则生成当前数据处理响应消息,该当前数据处理响应消息不包含任何第二待处理数据块,但包含用于提示移动设备所有第二待处理数据块已发送完毕的信息。

[0114] 在实际应用中,数据处理响应消息所包含的两种不同信息可通过设置预设第一命令格式中特定字段为不同值来实现。

[0115] 在上述实施例中,移动设备所发送的各种命令均可基于一种预设的第一命令格式并通过设置不同的字段值来实现,本发明实施例提供一种优选的第一命令格式,如下表所示:

[0116]

描述	内容		长度(字节)
CLA	命令类别: 00		1
INS	命令说明: 80		1
P1	命令参数1: b1b2:会话编号, 最大值为4 b3:-0: 不含数据 -1: 包含数据 b4:-0: 继续会话 -1: 中止会话 b5:-0: 下一数据块 -1: 重传最近的响应 其余保留		
P2	命令参数2: 剩余数据块数量		1
Lc	命令数据长度, b3=0时不存在,		1
NAF-ID	NAF-ID长度	X	X+1
	NAF-ID	NAF-ID值	
Data	数据长度	Y	Y+1

[0117]

	数据	数据值	
REQ	处理需求长度	Z	Z+1
	处理需求	处理需求	
Le	期望的响应长度, b3=1时不存在		

[0118] 该第一命令格式可同时适用于较大数据量的分块传输和较小数据量的整体传输, 并能够提供继续、中止、重传等基本管理。该第一命令格式的各参数说明如下:

[0119] P1为命令参数1, 表示本命令的管理要求, 其中b1b2字段表示本次数据传输处理的会话编号, 同时可以存在最多4个会话编号; b3字段表示本命令是否包含需传输的数据, 其可以有两个取值, 例如其取值为“0”时表示本命令不含需传输的数据, 其取值为“1”时表示本命令包含需传输的数据; b4字段表示对于会话继续还是中止的要求, 其可以有两个取值, 例如其取值为“0”时表示继续会话, 其取值为“1”时表示中止会话; b5字段表示对响应是否需要重传的要求, 其可以有两个取值, 例如其取值为“0”时表示本命令用于传输下一个数据块, 其取值为“1”时表示本命令用于重传最近的响应所指示的需要重传的数据块。P1的其余字段的定义可以保留, 具体各设置含义见上表。

[0120] P2为命令参数2, 表示移动设备到UICC的剩余的数据块的数量, 即未传输的数据块的数量。

[0121] Lc为命令中需传输的数据部分的长度, 可选, 当b3=0时不存在。

[0122] NAF-ID为命令数据的组成部分, 其是NAF (应用服务器) 的身份标识, 用于表示要求

本次数据传输处理对应的NAF (应用服务器),其包括NAF-ID的长度和NAF-ID值。

[0123] Data为命令数据的组成部分,表示本次传输的待处理数据或数据块,包括Data的长度和Data值,当b3=0时,Data的长度和Data值为空。

[0124] REQ为命令数据的组成部分,表示对待处理数据的处理需求,可包含终端应用可得到的本次数据处理的其它要求,如处理的类型、算法指示等。

[0125] Le是期望的响应长度,可选,当b3=1时不存在。

[0126] 上述各实施例中移动设备所发送的数据处理请求命令、数据处理请求子命令及数据获取请求命令等命令皆可基于该第一命令格式实现,其中各个字段的具体取值可根据实际情况设置。

[0127] 图6为本发明实施例提供的再一种数据处理方法的流程图,本实施例提供的数据处理方法基于用户终端中的UICC实现,如图6所示,该方法包括:

[0128] 步骤S201、接收移动设备发送的数据处理请求命令。

[0129] 数据处理请求命令为移动设备基于终端应用发送的基于GBA的待处理数据生成的命令。数据处理请求命令的生成过程与上述实施例中步骤S101中数据处理请求命令的生成过程相同,具体请参见步骤S101的描述,此处不再赘述。

[0130] 步骤S202、利用预设共享密钥对待处理数据进行处理。

[0131] 预设共享密钥为存储在UICC中的共享密钥,该共享密钥为GBA机制下生成的密钥,特别的,在GBA_U机制下,由UICC生成共享密钥,该共享密钥同时将被存储于应用服务器中,以供终端应用在与应用服务器进行通信时,使用该共享密钥进行数据处理(加解密处理、鉴权处理等)。

[0132] 在一些实施例中,UICC内的预设共享密钥为Ks_int_NAF密钥。

[0133] 步骤S203、将处理后的待处理数据发送至移动设备。

[0134] 本发明实施例中,UICC接收移动设备发送的数据处理请求命令,并从该数据处理请求命令中获取到待处理数据,基于预设共享密钥对该待处理数据进行处理,并将处理后的待处理数据返回至移动设备,以供终端应用使用,本发明实施例实现了利用UICC内存储的共享密钥来对安装于移动设备中的终端应用的通信数据进行处理的过程,相较于现有技术,避免了使用不同的共享密钥来对用户终端上安装于不同模块(移动设备和UICC)的应用的通信数据进行处理,从而降低了应用服务器管理共享密钥的复杂度,实现了密钥的统一管理。

[0135] 在一些实施例中,当终端应用的待处理数据的数据量较大时,移动设备将待处理数据分块传输至UICC,如图7所示,图7为本发明实施例提供的再一种数据处理方法的流程图,本实施例中,待处理数据包括多个第一待处理数据块,数据处理请求命令包括多个数据处理请求子命令,每个数据处理请求子命令对应包括一个第一待处理数据块,本实施例在图6所示实施例的基础上,步骤S201包括:

[0136] 步骤S2011、接收移动设备发送的当前数据处理请求子命令,当前数据处理请求子命令包括当前第一待处理数据块。

[0137] 步骤S2012、基于当前数据处理请求子命令判断移动设备中是否还剩余有第一待处理数据块需要发送。

[0138] UICC基于当前数据处理请求子命令判断移动设备中是否还剩余有第一待处理数

据块需要发送可通过识别数据处理请求子命令中的相关字段来确定,例如,在数据处理请求子命令中设置某一字段用来标识剩余数据块的数量,UICC通过检测该字段以确定出剩余数据块的数量。

[0139] 在步骤S2012中,当UICC判断出移动设备中还剩余有第一待处理数据块需要发送时,执行下述步骤S2013,以使移动设备响应该第一命令响应消息而继续发送剩余第一待处理数据块,并顺序返回步骤S2011,直至UICC成功接收到移动设备发送的全部的第一待处理数据块;而当判断出移动设备中没有第一待处理数据块需要发送时,UICC不再生成第一命令响应消息,而是直接执行步骤S202来对接收到的第一待处理数据块进行处理。

[0140] 步骤S2013、响应于当前数据处理请求子命令,生成用于指示移动设备传送下一个第一待处理数据块的当前第一命令响应消息,并将该当前第一命令响应消息发送至移动设备。

[0141] 移动设备在接收到当前第一命令响应消息后,针对该当前第一命令响应消息,将多个第一待处理数据块中的下一个第一待处理数据块作为当前第一待处理数据块,并根据当前第一待处理数据块生成当前数据处理请求子命令。

[0142] 本实施例中的步骤S2011~S2013与上述实施例中的步骤S1021~S1023对应,具体请见上述实施例中对对应步骤的描述,此处不再赘述。

[0143] 在一些实施例中,当待处理数据的数据量较小时,可不对待处理数据进行分割,此时,步骤S201的过程为:接收移动设备发送的数据处理请求命令,该数据处理请求命令为移动设备根据完整的待处理数据生成,该数据处理请求命令包含完整的待处理数据。

[0144] 在一些实施例中,在移动设备将待处理数据分块传输至UICC的过程中,移动设备所发送的数据处理请求子命令可能发生错误或异常,在此情况下,UICC需要指示移动设备重新发送包含当前第一待处理数据块的数据处理请求子命令。如图8所示,图8为本发明实施例提供的再一种数据处理方法的流程图,本实施例在图7所示实施例的基础上,在步骤S2011之后,还包括:

[0145] 步骤S2012a、检测当前数据处理请求子命令是否存在异常。

[0146] 若检测出当前数据处理请求子命令存在异常,则生成用于指示移动设备重传当前第一待处理数据块的当前第一命令响应消息,并发送至移动设备,以供移动设备根据当前第一待处理数据块生成当前数据处理请求子命令;若检测出当前数据处理请求子命令不存在异常,则执行步骤S2012。

[0147] 本发明实施例中,数据处理请求子命令可能发生的异常包括数据格式错误和包含的数据块不完整等等。数据处理请求子命令发生异常将导致UICC无法从数据处理请求子命令中获取到对应的完整的第一待处理数据块和/或UICC无法响应于该数据处理请求子命令而对对应的第一待处理数据块进行处理。因此,本发明实施例中,当移动设备将当前数据处理请求子命令发送至UICC后,UICC侧对该当前数据处理请求子命令进行检测以确定该当前数据处理请求子命令是否存在异常,例如,UICC通过检测当前数据处理请求子命令的各字段是否符合预设规范来确定该当前数据处理请求子命令是否发生格式错误,以及通过检测当前数据处理请求子命令中所包含的第一待处理数据块的大小是否等于预设大小来确定该第一待处理数据块是否完整,等等。

[0148] 本发明图8所示实施例与本发明图4所示实施例的方法步骤对应,具体请参见图4

所示实施例中对应方法步骤的描述,此处不再赘述。

[0149] 本发明中,UICC在对待处理数据完成处理后,可基于处理后待

[0150] 处理数据的数据量大小采用不同的方式将处理后的待处理数据返回至移动设备。

[0151] 在一些实施例中,当处理后的待处理数据的数据量较小时,可直接将处理后的待处理数据通过响应消息的形式返回至移动设备。对应的,步骤S203的过程为:根据处理后的待处理数据生成数据处理响应消息,该数据处理响应消息包括处理后的待处理数据,将数据处理响应消息发送至移动设备。

[0152] 在另一些实施例中,当处理后的待处理数据的数据量较大时,可基于数据分块传输的方式将处理后的待处理数据返回至移动设备。具体的,如图9所示,图9为本发明实施例提供的再一种数据处理方法的流程图,本实施例中,处理后的待处理数据被分割为多个第二待处理数据块,本实施例在图6所示实施例的基础上,步骤S203具体包括:

[0153] 步骤S2031、针对多个第二待处理数据块中的当前第二待处理数据块,根据当前第二待处理数据块生成用于指示移动设备获取下一个第二待处理数据块的当前数据处理响应消息,并将该当前数据处理响应消息发送至移动设备。

[0154] 当前数据处理响应消息包括当前第二待处理数据块。

[0155] 步骤S2032、响应于移动设备针对当前数据处理响应消息返回的当前数据获取请求命令,判断是否仅剩余一个第二待处理数据块未发送。

[0156] 当判断出仅剩余一个第二待处理数据块未发送时,执行步骤S2033;当判断出剩余多个第二待处理数据块未发送时,返回执行步骤S2031。

[0157] 步骤S2033、响应于移动设备针对当前数据处理响应消息返回的当前数据获取请求命令,将仅剩余的一个第二待处理数据块作为当前第二待处理数据块,根据当前第二待处理数据块生成用于提示移动设备第二待处理数据块已发送完毕的当前数据处理响应消息,并将该当前数据处理响应消息发送至移动设备。

[0158] 本实施例中的方法步骤与图5所示实施例的方法步骤对应,具体请参见图5所述实施例的方法步骤的描述,此处不再赘述。

[0159] 本发明实施例中,UICC所发送的各种响应消息可基于一种预设的第二命令格式并通过设置不同的字段值实现,本发明实施例提供一种优选的第二命令格式,如下表所示:

[0160]

描述	内容		长度(字节)
NAF-ID	NAF-ID长度	X	X+1
	NAF-ID	NAF-ID值	
Data	数据长度	Y	Y+1
	数据	数据值	
SW1	状态字1: 92-响应进行中 6A-响应中止		
SW2	状态字2: b1:-0: 无数据块待处理, 处理完成 -1: 有数据块待处理, 终端需发送命令取回 b2:-0: 发送下一数据块 -1: 重传前一数据块 b3b4:会话编号, 待处理数据块对应的会话编号 其余保留		

[0161] 该第二命令格式可同时适用于较大数据量的分块传输和较小数据量的整体传输, 并提供继续、中止、重传等基本管理。该第二命令格式的各参数说明如下:

[0162] NAF-ID和Data是UICC返回给移动设备的数据, 格式同表中要求。

[0163] SW1是命令处理状态字, 表示命令处理的基本结果, 例如, SW1=92表示响应进行中, SW1=6A表示响应终止。

[0164] SW2是命令处理状态字, 表示响应的管理要求, 其中b1字段表示是否还有待处理的数据块需要通过响应返回到移动设备, b2字段表示对命令是否需要重传的要求; b3b4字段表示处理的数据块对应的命令中的会话编号。SW2中其余字段的定义保留。

[0165] 本发明实施例中UICC所发送的第一命令响应消息、数据处理响应消息等消息皆可基于该第二命令格式实现。

[0166] 基于以上描述, 在一些实施例中, 提供一种数据处理方法, 其完整流程为:

[0167] 步骤1、响应于移动设备上的终端应用发送的基于GBA的数据处理请求, 移动设备获取终端应用的待处理数据。

[0168] 步骤2、移动设备将待处理数据分割为多个第一待处理数据块。

[0169] 步骤3、移动设备基于当前第一待处理数据块生成数据处理请求子命令, 并发送至UICC。

[0170] 步骤4、UICC接收到当前数据处理请求子命令, 存储当前第一待处理数据块, 并判断当前数据处理请求子命令是否异常, 若判断出异常, 则生成用于指示移动设备重新发送当前第一待处理数据块的第一命令响应消息并将该第一命令响应消息返回给移动设备, 并进入步骤6; 若判断出正常, 执行步骤5。

[0171] 步骤5、判断是否收到全部数据, 若判断出未收到全部数据, 则返回用于指示移动

设备发送下一个第一待处理数据块的第一命令响应消息;若判断出收到全部数据,则不返回第一命令响应消息,进入步骤7。

[0172] 步骤6、移动设备接收到第一命令响应消息,识别第一命令响应消息中的信息,若识别出第一命令响应消息为发送下一个第一待处理数据块,则将下一个第一待处理数据块作为当前第一待处理数据,并执行步骤3;若识别出第一命令响应消息为发送当前第一待处理数据块,则直接执行步骤3。

[0173] 重复执行步骤3至步骤6,直到所有第一待处理数据块均成功且完整地发送至UICC。

[0174] 步骤7、UICC利用预设共享密钥对待处理数据进行处理。

[0175] 步骤8、UICC将处理后的待处理数据分割为多个第二待处理数据块。

[0176] 步骤9、UICC基于当前第二待处理数据块生成当前数据处理响应消息,并且,UICC基于第二待处理数据块的数量,在当前数据处理响应消息中添加信息,用于提示移动设备继续提取下一个第二待处理数据块或者提示移动设备所有第二待处理数据块已发送完毕。

[0177] 步骤10、移动设备接收到当前数据处理响应消息,存储当前第二待处理数据块,并识别当前数据处理响应消息中的信息,当识别出信息为提取下一个第二待处理数据块时,生成当前数据获取请求命令,并发送至UICC,当识别出信息为所有第二待处理数据块已发送完毕时,仅存储当前第二待处理数据块,不再生成当前数据获取请求命令。

[0178] 步骤11、UICC接收数据获取请求命令,将下一个第二待处理数据块作为当前第二待处理数据块,并执行步骤9。

[0179] 重复步骤9至步骤11,直到UICC将所有的第二待处理数据块成功且完整地返回至移动设备。

[0180] 本发明实施例还提供一种移动设备,包括:存储模块和至少一个处理器,该存储模块中存储有计算机程序,该计算机程序被至少一个处理器执行时实现本发明基于移动设备实现的数据处理方法。

[0181] 本发明实施例还提供一种UICC,包括:存储模块和至少一个处理器,该存储模块中存储有计算机程序,该计算机程序被至少一个处理器执行时实现本发明基于UICC实现的数据处理方法。

[0182] 本发明实施例还提供一种用户终端,如图1所示,该用户终端包括移动设备和UICC,其中,移动设备采用本发明实施例所提供的移动设备,UICC采用本发明实施例所提供的UICC。

[0183] 可以理解的是,以上实施方式仅仅是为了说明本发明的原理而采用的示例性实施方式,然而本发明并不局限于此。对于本领域内的普通技术人员而言,在不脱离本发明的精神和实质的情况下,可以做出各种变型和改进,这些变型和改进也视为本发明的保护范围。

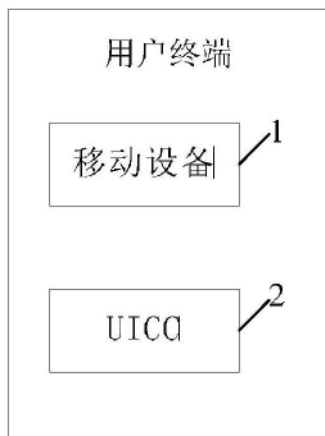


图1

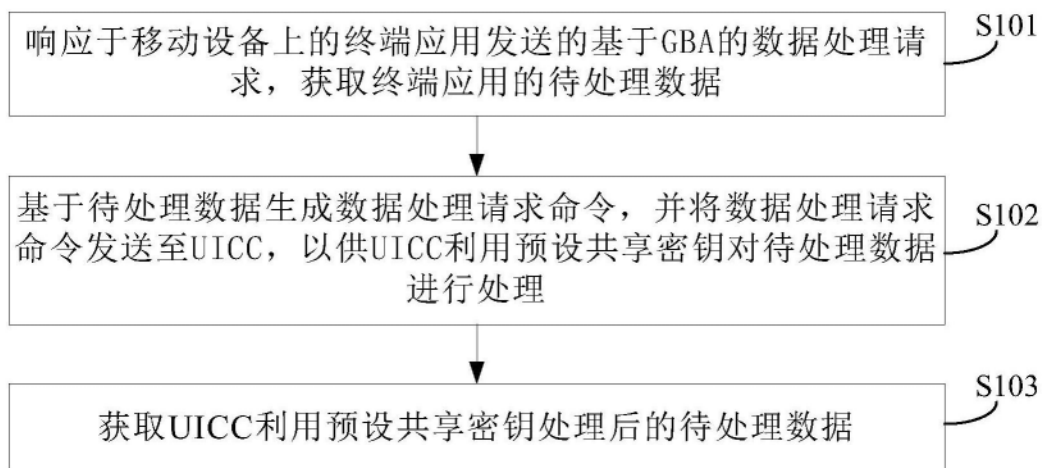


图2

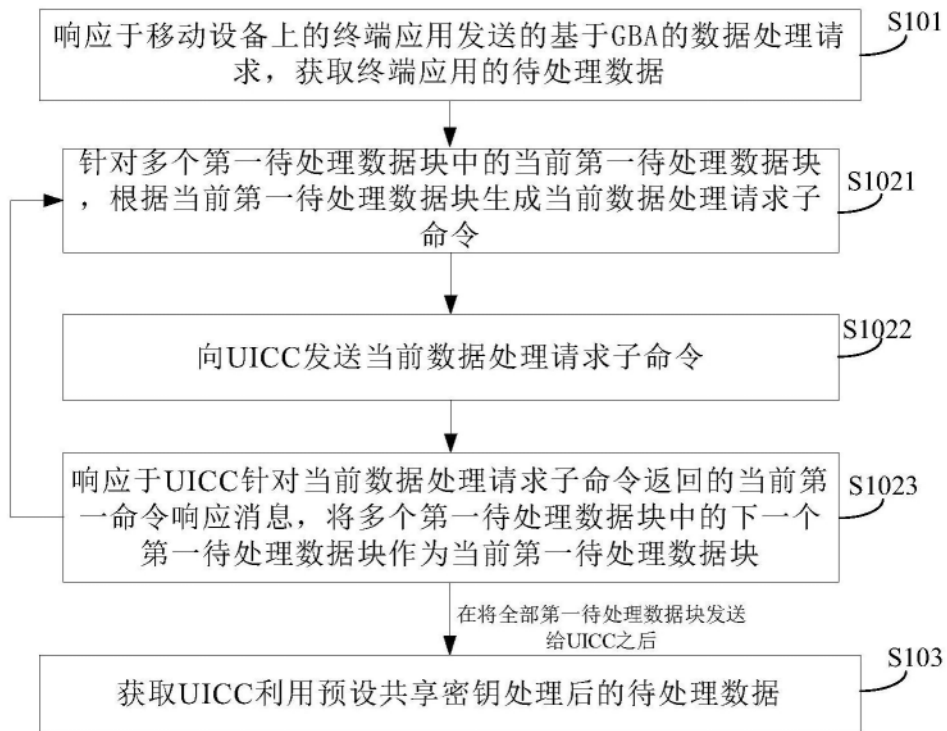


图3

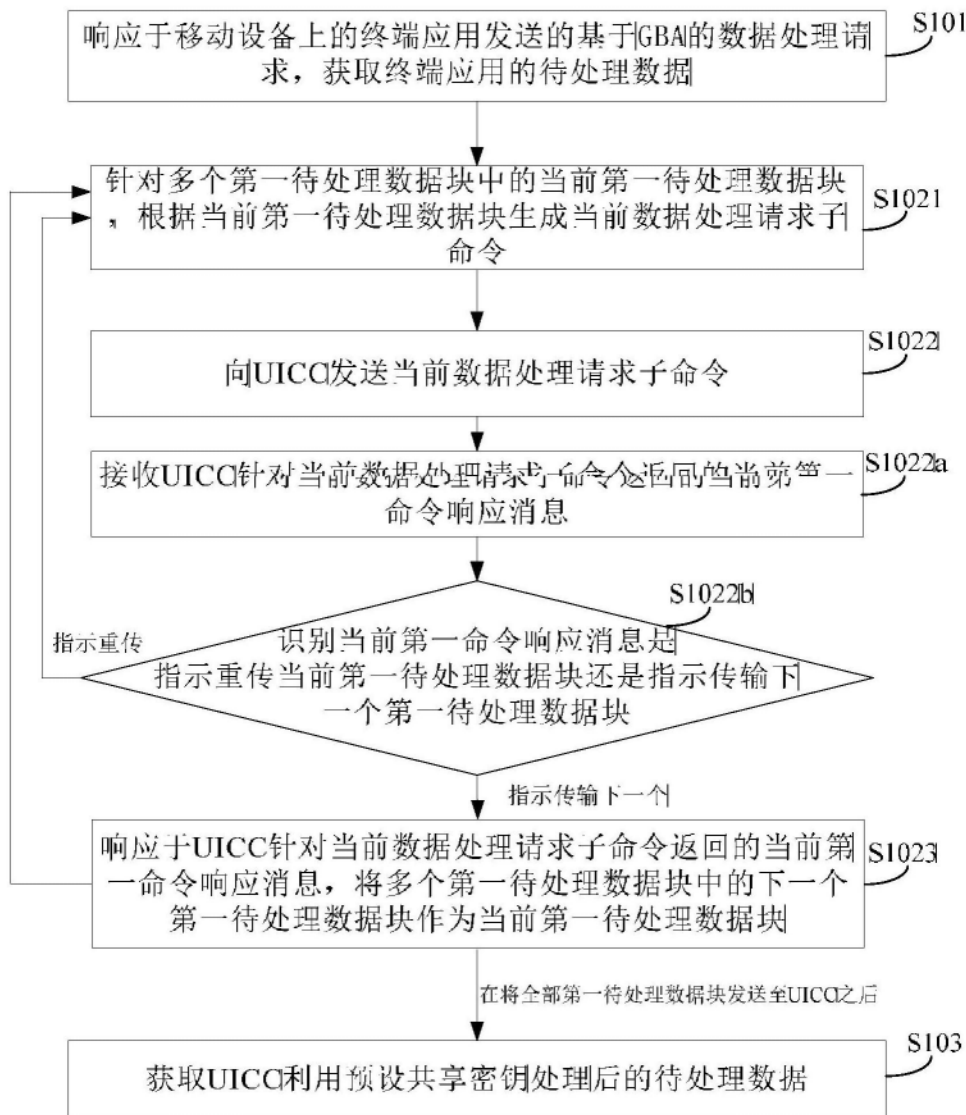


图4

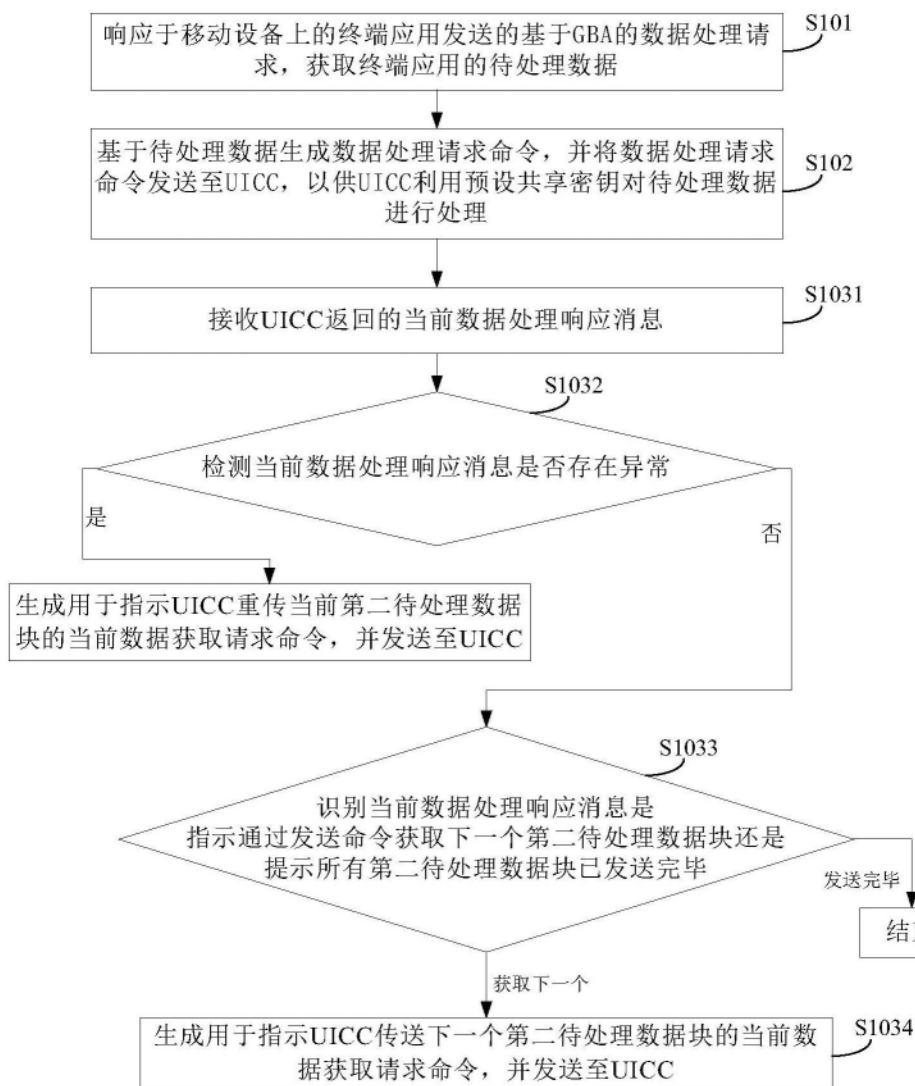


图5

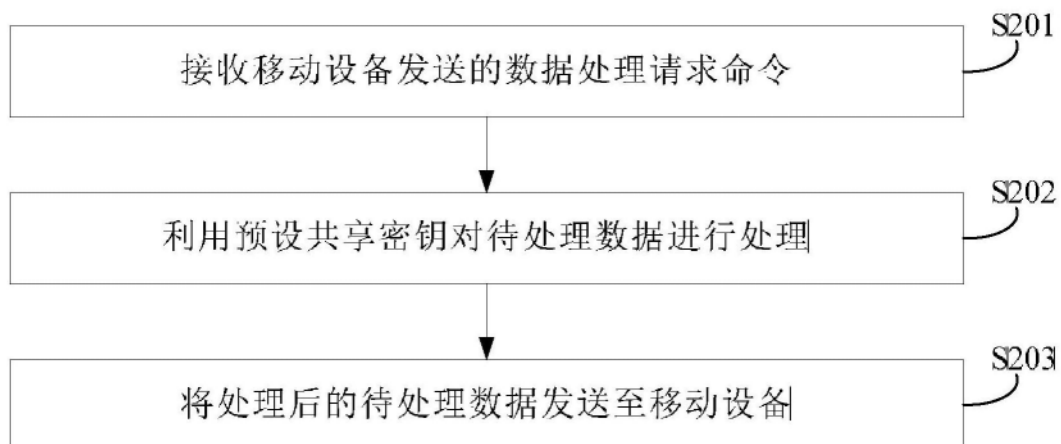


图6

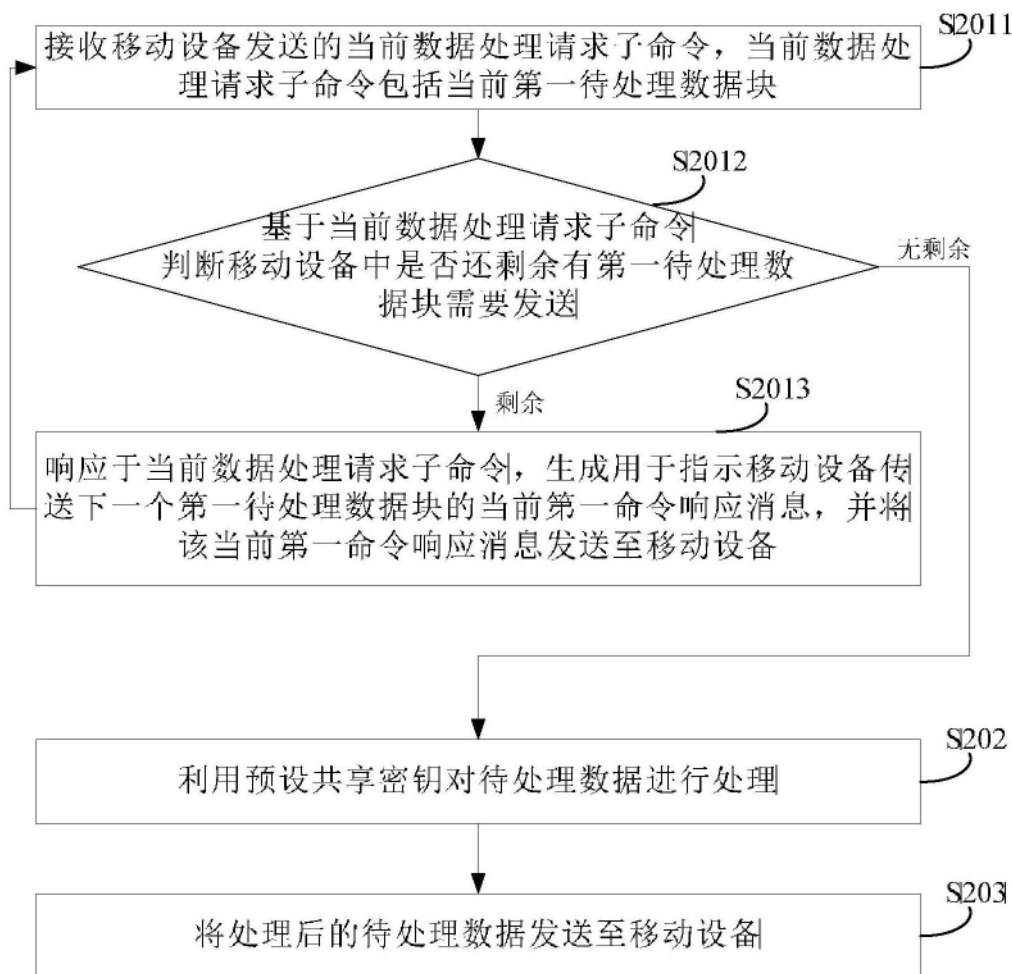


图7

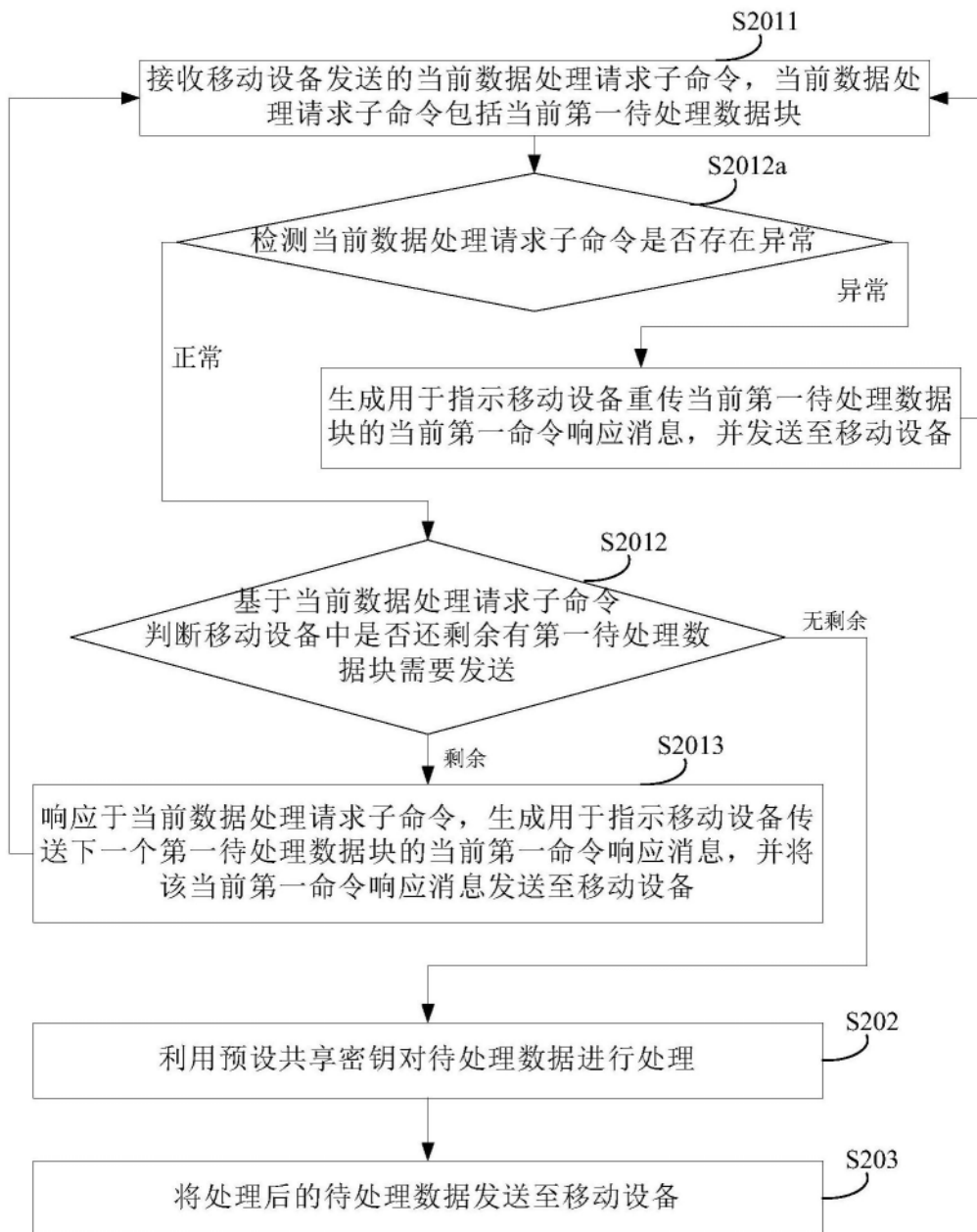


图8

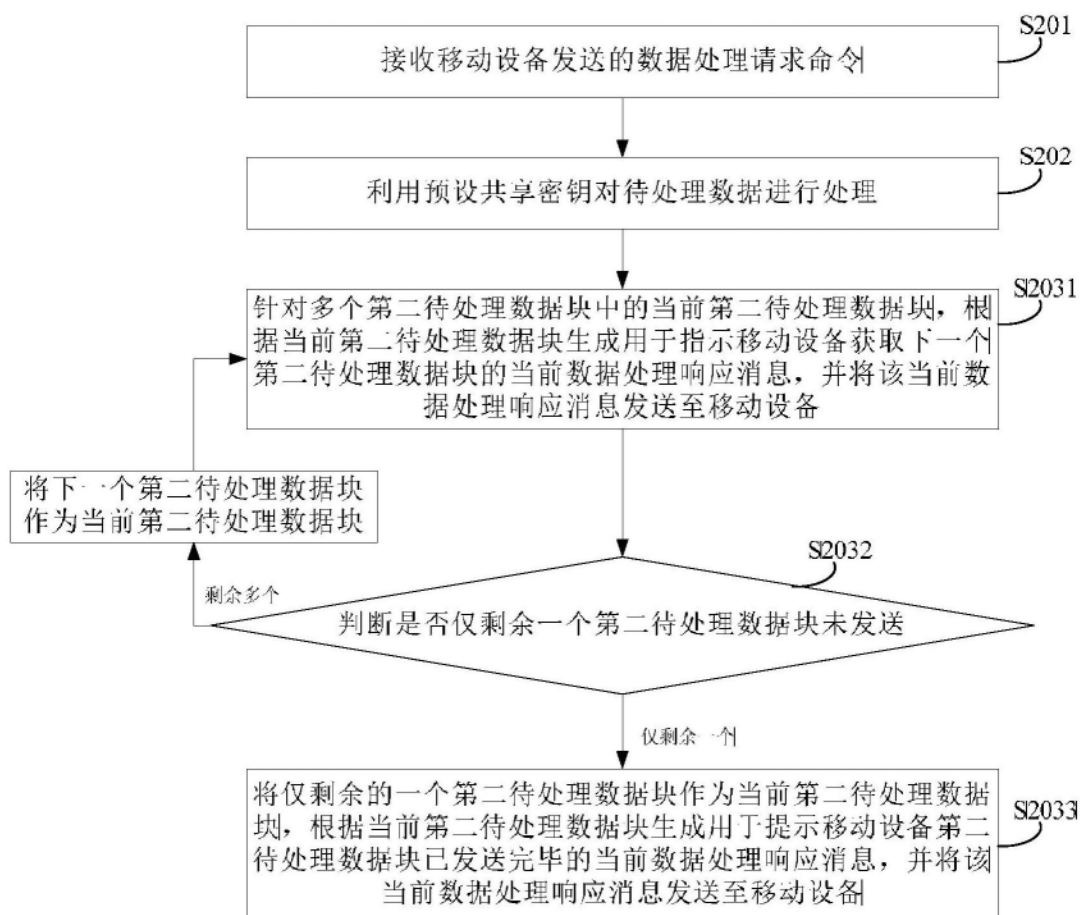


图9