(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117714042 A
(43)申请公布日 2024.03.15

(21)申请号 202311707741.9

(22)申请日 2023.12.12

(71)申请人 上海商米科技集团股份有限公司
地址 200433 上海市杨浦区淞沪路388号创智天地7号楼605
申请人 深圳米开朗基罗科技有限公司

(72)发明人 万利强 林喆 曹亮

(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 骆希聪

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)

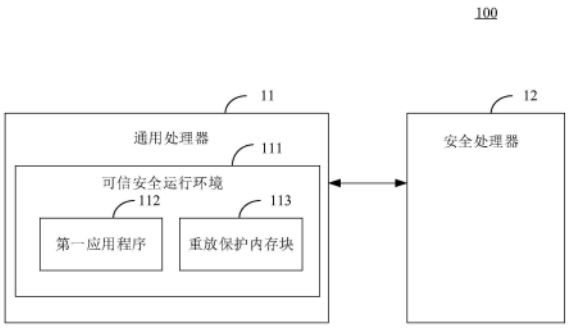
权利要求书3页 说明书8页 附图5页

(54)发明名称

密钥容量扩充系统及其密钥交互方法

(57)摘要

本发明提供了一种密钥容量扩充系统及其密钥交互方法,其中,密钥容量扩充系统包括:安全处理器和通用处理器,安全处理器与通用处理器通信连接,通用处理器包括可信安全运行环境、第一应用程序和重放保护内存块,第一应用程序和重放保护内存块位于安全运行环境中,其中,通用处理器存储有可信环境公钥,第一应用程序存储有可信环境私钥,可信环境公钥与可信环境私钥为非对称密钥对,重放保护内存块用于存储密文主密钥和安全处理器需要的目标密文传输密钥。本发明在保证了密钥的安全性符合要求同时,且不会对交易速度造成较大影响。



CN 117714042 A

1.一种密钥容量扩充系统,其特征在于,包括:安全处理器和通用处理器,所述安全处理器与所述通用处理器通信连接,所述通用处理器包括可信安全运行环境、第一应用程序和重放保护内存块,所述第一应用程序和所述重放保护内存块位于所述安全运行环境中,其中,所述通用处理器存储有可信环境公钥,所述第一应用程序存储有可信环境私钥,所述可信环境公钥与所述可信环境私钥为非对称密钥对,所述重放保护内存块用于存储密文主密钥和所述安全处理器需要的目标密文传输密钥;

所述通用处理器和所述安全处理器配置为采用如下交互方法进行交互:

所述通用处理器接收原始密文传输密钥,从所述重放保护内存块获取所述密文主密钥,将所述原始密文传输密钥和所述密文主密钥发送给所述安全处理器;

所述安全处理器根据所述原始密文传输密钥和所述密文主密钥生成所述目标密文传输密钥,将所述目标密文传输密钥发送给所述通用处理器;

所述通用处理器通过所述可信环境公钥对获取到的所述目标密文传输密钥进行加密,得到第一传输密钥,将所述第一传输密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一传输密钥解密,得到所述目标密文传输密钥,将所述目标密文传输密钥存储至所述重放保护内存块。

2.如权利要求1所述的密钥容量扩充系统,其特征在于,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:

所述安全处理器接收明文主密钥,在安全环境下生成随机密钥,通过所述随机密钥对所述明文主密钥进行加密,获得所述密文主密钥,将所述密文主密钥发送给所述通用处理器;

所述通用处理器接收所述密文主密钥,通过所述可信环境公钥对获取到的所述密文主密钥进行加密,得到第一主密钥,将所述第一主密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一主密钥解密,得到所述密文主密钥,将所述密文主密钥存储至所述重放保护内存块。

3.如权利要求2所述的密钥容量扩充系统,其特征在于,所述安全处理器还配置为采用如下方法生成所述目标密文传输密钥:

所述安全处理器通过所述随机密钥解密所述密文主密钥得到所述明文主密钥,通过所述明文主密钥对所述原始密文传输密钥进行解密,获得明文传输密钥,通过所述随机密钥对所述明文传输密钥进行加密,获得所述目标密文传输密钥。

4.如权利要求3所述的密钥容量扩充系统,其特征在于,所述安全处理器还配置为获得所述明文传输密钥之后,将所述明文传输密钥的标识号记录在本地密钥索引列表中。

5.如权利要求4所述的密钥容量扩充系统,其特征在于,所述通用处理器和所述安全处理器还配置为采用如下方法进行密钥自检:

所述通用处理器从所述重放保护内存块中读取所有的所述目标密文传输密钥,发送所述目标密文传输密钥给所述安全处理器;

所述安全处理器通过所述随机密钥每次对一条所述目标密文传输密钥进行解密,得到所述明文传输密钥,判断所述明文传输密钥的密钥检查值是否正确,如果是,则记录所述明文传输密钥的标识号,然后判断下一条所述明文传输密钥的密钥检查值是否正确,如果所有的明文传输密钥的标识号与所述本地密钥索引列表一致,则向所述通用处理器发送“自

检成功”信号。

6.如权利要求4所述的密钥容量扩充系统,其特征在于,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:

所述通用处理器从所述重放保护内存块中读取一条所述目标密文传输密钥,发送所述目标密文传输密钥给所述安全处理器;

所述安全处理器通过所述随机密钥对所述目标密文传输密钥进行解密,得到所述明文传输密钥,当接收到删除指令后,删除所述本地密钥索引列表中所述明文传输密钥的标识号,发送“删除成功信号”给所述通用处理器;

所述通用处理器中的所述第一应用程序根据所述“删除成功信号”删除所述重放保护内存块中所述明文传输密钥对应的所述目标密文传输密钥。

7.如权利要求3所述的密钥容量扩充系统,其特征在于,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:

所述通用处理器接收计算需求,从所述重放保护内存块读取所述计算需求对应的所述目标密文传输密钥,将所述目标密文传输密钥和所述计算需求发送给所述安全处理器;

所述安全处理器通过所述随机密钥解密所述目标密文传输密钥得到所述明文传输密钥,根据所述计算需求对所述明文传输密钥进行计算,将计算结果发送至所述通用处理器。

8.如权利要求3所述的密钥容量扩充系统,其特征在于,所述通用处理器和所述安全处理器还配置为采用如下方法进行相同密钥数据检测:

所述安全处理器获得待写入的所述明文传输密钥后,所述通用处理器将所述重放保护内存块中所有的所述目标密文传输密钥发送给所述安全处理器,所述安全处理器解密所有的所述目标密文传输密钥,将待写入的所述明文传输密钥与解密出的所有明文传输密钥进行对比,如果存在与待写入的所述明文传输密钥相同的明文传输密钥,则删除待写入的所述明文传输密钥。

9.如权利要求3所述的密钥容量扩充系统,其特征在于,所述安全处理器还配置为监测到攻击信号时,删除所述随机密钥。

10.如权利要求9所述的密钥容量扩充系统,其特征在于,所述安全处理器还配置为将所述攻击信号发送给所述通用处理器,所述通用处理器还配置为接收到所述攻击信号后通知所述第一应用程序删除所述重放保护内存块中的数据。

11.如权利要求1所述的密钥容量扩充系统,其特征在于,所述通用处理器还配置为接收到出厂设置命令时,删除所述可信环境公钥。

12.如权利要求1所述的密钥容量扩充系统,其特征在于,所述通用处理器还配置为接收到删除所述第一应用程序命令时,删除所述可信环境公钥。

13.一种密钥容量扩充系统的密钥交互方法,所述密钥容量扩充系统包括安全处理器和通用处理器,所述通用处理器包括可信安全运行环境、第一应用程序和重放保护内存块,所述通用处理器存储有可信环境公钥,所述第一应用程序存储有可信环境私钥,所述可信环境公钥与所述可信环境私钥为非对称密钥对,其特征在于,包括:

所述通用处理器接收原始密文传输密钥,从所述重放保护内存块获取密文主密钥,将所述原始密文传输密钥和所述密文主密钥发送给所述安全处理器;

所述安全处理器根据所述原始密文传输密钥和所述密文主密钥生成目标密文传输密

钥,将所述目标密文传输密钥发送给所述通用处理器;

所述通用处理器通过所述可信环境公钥对获取到的所述目标密文传输密钥进行加密,得到第一传输密钥,将所述第一传输密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一传输密钥解密,得到所述目标密文传输密钥,将所述目标密文传输密钥存储至所述重放保护内存块。

密钥容量扩充系统及其密钥交互方法

技术领域

[0001] 本发明主要涉及信息安全技术领域,尤其涉及一种密钥容量扩充系统及其密钥交互方法。

背景技术

[0002] 销售终端POS(Point of Sale)是可以通过与金融机构联网来实现非现金消费、预授权、查询余额、转账等功能的电子设备,通常会安装在商户端。而智能POS(Smart Point of Sale)对比于传统POS,不仅能实现传统POS的刷卡支付,而且还包括扫描二维码支付和验证会员卡券等功能。

[0003] 当前,智能POS的通用架构是采用通用处理器(Application Processor,AP)运行Android系统,采用安全处理器(Secure Processor,SP)运行金融系统。安全处理器需要的密钥通常存储于自身芯片的FLASH中,可以满足传统交易和绝大部分业务场景需求,但是如果想要扩充密钥容量,要么在SP外扩FLASH芯片,要么选用大容量的SP芯片。这两种方案都会导致成本会上升,并且涉及软硬件改造。

发明内容

[0004] 本发明要解决的技术问题是提供一种密钥容量扩充系统及其密钥交互方法,解决密钥容量受到SP端FLASH存储器限制的情况。

[0005] 为解决上述技术问题,本发明提供了一种密钥容量扩充系统,包括:安全处理器和通用处理器,所述安全处理器与所述通用处理器通信连接,所述通用处理器包括可信安全运行环境、第一应用程序和重放保护内存块,所述第一应用程序和所述重放保护内存块位于所述安全运行环境中,其中,所述通用处理器存储有可信环境公钥,所述第一应用程序存储有可信环境私钥,所述可信环境公钥与所述可信环境私钥为非对称密钥对,所述重放保护内存块用于存储密文主密钥和所述安全处理器需要的目标密文传输密钥;所述通用处理器和所述安全处理器配置为采用如下交互方法进行交互:所述通用处理器接收原始密文传输密钥,从所述重放保护内存块获取所述密文主密钥,将所述原始密文传输密钥和所述密文主密钥发送给所述安全处理器;所述安全处理器根据所述原始密文传输密钥和所述密文主密钥生成所述目标密文传输密钥,将所述目标密文传输密钥发送给所述通用处理器;所述通用处理器通过所述可信环境公钥对获取到的所述目标密文传输密钥进行加密,得到第一传输密钥,将所述第一传输密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一传输密钥解密,得到所述目标密文传输密钥,将所述目标密文传输密钥存储至所述重放保护内存块。

[0006] 可选地,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:所述安全处理器接收明文主密钥,在安全环境下生成随机密钥,通过所述随机密钥对所述明文主密钥进行加密,获得所述密文主密钥,将所述密文主密钥发送给所述通用处理器;所述通用处理器接收所述密文主密钥,通过所述可信环境公钥对获取到的所述密文主密钥

进行加密,得到第一主密钥,将所述第一主密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一主密钥解密,得到所述密文主密钥,将所述密文主密钥存储至所述重放保护内存块。

[0007] 可选地,所述安全处理器还配置为采用如下方法生成所述目标密文传输密钥:所述安全处理器通过所述随机密钥解密所述密文主密钥得到所述明文主密钥,通过所述明文主密钥对所述原始密文传输密钥进行解密,获得明文传输密钥,通过所述随机密钥对所述明文传输密钥进行加密,获得所述目标密文传输密钥。

[0008] 可选地,所述安全处理器还配置为获得所述明文传输密钥之后,将所述明文传输密钥的标识号记录在本地密钥索引列表中。

[0009] 可选地,所述通用处理器和所述安全处理器还配置为采用如下方法进行密钥自检:所述通用处理器从所述重放保护内存块中读取所有的所述目标密文传输密钥,发送所述目标密文传输密钥给所述安全处理器;所述安全处理器通过所述随机密钥每次对一条所述目标密文传输密钥进行解密,得到所述明文传输密钥,判断所述明文传输密钥的密钥检查值是否正确,如果是,则记录所述明文传输密钥的标识号,然后判断下一条所述明文传输密钥的密钥检查值是否正确,如果所有的明文传输密钥的标识号与所述本地密钥索引列表一致,则向所述通用处理器发送“自检成功”信号。

[0010] 可选地,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:所述通用处理器从所述重放保护内存块中读取一条所述目标密文传输密钥,发送所述目标密文传输密钥给所述安全处理器;所述安全处理器通过所述随机密钥对所述目标密文传输密钥进行解密,得到所述明文传输密钥,当接收到删除指令后,删除所述本地密钥索引列表中所述明文传输密钥的标识号,发送“删除成功信号”给所述通用处理器;所述通用处理器中的所述第一应用程序根据所述“删除成功信号”删除所述重放保护内存块中所述明文传输密钥对应的所述目标密文传输密钥。

[0011] 可选地,所述通用处理器和所述安全处理器还配置为采用如下交互方法进行交互:所述通用处理器接收计算需求,从所述重放保护内存块读取所述计算需求对应的所述目标密文传输密钥,将所述目标密文传输密钥和所述计算需求发送给所述安全处理器;所述安全处理器通过所述随机密钥解密所述目标密文传输密钥得到所述明文传输密钥,根据所述计算需求对所述明文传输密钥进行计算,将计算结果发送至所述通用处理器。

[0012] 可选地,所述通用处理器和所述安全处理器还配置为采用如下方法进行相同密钥数据检测:所述安全处理器获得待写入的所述明文传输密钥后,所述通用处理器将所述重放保护内存块中所有的所述目标密文传输密钥发送给所述安全处理器,所述安全处理器解密所有的所述目标密文传输密钥,将待写入的所述明文传输密钥与解密出的所有明文传输密钥进行对比,如果存在与待写入的所述明文传输密钥相同的明文传输密钥,则删除待写入的所述明文传输密钥。

[0013] 可选地,所述安全处理器还配置为监测到攻击信号时,删除所述随机密钥。

[0014] 可选地,所述安全处理器还配置为将所述攻击信号发送给所述通用处理器,所述通用处理器还配置为接收到所述攻击信号后通知所述第一应用程序删除所述重放保护内存块中的数据。

[0015] 可选地,所述通用处理器还配置为接收到出厂设置命令时,删除所述可信环境公

钥。

[0016] 可选地,所述通用处理器还配置为接收到删除所述第一应用程序命令时,删除所述可信环境公钥。

[0017] 为解决上述技术问题,本发明提供了一种密钥容量扩充系统的密钥交互方法,所述密钥容量扩充系统包括安全处理器和通用处理器,所述通用处理器包括可信安全运行环境、第一应用程序和重放保护内存块,所述通用处理器存储有可信环境公钥,所述第一应用程序存储有可信环境私钥,所述可信环境公钥与所述可信环境私钥为非对称密钥对,包括:所述通用处理器接收原始密文传输密钥,从所述重放保护内存块获取密文主密钥,将所述原始密文传输密钥和所述密文主密钥发送给所述安全处理器;所述安全处理器根据所述原始密文传输密钥和所述密文主密钥生成目标密文传输密钥,将所述目标密文传输密钥发送给所述通用处理器;所述通用处理器通过所述可信环境公钥对获取到的所述目标密文传输密钥进行加密,得到第一传输密钥,将所述第一传输密钥传输至所述第一应用程序,所述第一应用程序通过所述可信环境私钥对所述第一传输密钥解密,得到所述目标密文传输密钥,将所述目标密文传输密钥存储至所述重放保护内存块。

[0018] 与现有技术相比,本发明具有以下优点:

[0019] 本发明的密钥容量扩充系统,第一应用程序和重放保护内存块位于安全运行环境中,且通用处理器存储可信环境公钥,第一应用程序存储可信环境私钥,将目标密文传输密钥存储在通用处理器的重放保护内存块中,保证了密钥的安全性符合要求,解决了密钥容量受到安全处理器的flash存储器限制的问题;本发明的密钥容量扩充系统的密钥交互方法,保证了密钥的安全性符合要求,且不会对交易速度造成较大影响。

附图说明

[0020] 包括附图是为提供对本申请进一步的理解,它们被收录并构成本申请的一部分,附图示出了本申请的实施例,并与本说明书一起起到解释本发明原理的作用。附图中:

[0021] 图1是根据本发明一实施例的密钥容量扩充系统的系统框图。

[0022] 图2是图1密钥容量扩充系统的一实施例的交互方法的流程图。

[0023] 图3是图2中步骤S22一实施例的流程图。

[0024] 图4是图2优化实施例的密钥容量扩充系统的交互方法的流程图。

[0025] 图5是图2优化实施例的密钥容量扩充系统的交互方法的流程图。

具体实施方式

[0026] 为了更清楚地说明本申请的实施例的技术方案,下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地,下面描述中的附图仅仅是本申请的一些示例或实施例,对于本领域的普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图将本申请应用于其他类似情景。除非从语言环境中显而易见或另做说明,图中相同标号代表相同结构或操作。

[0027] 当前,智能POS机的密钥通常支持几百个,存储在SP芯片的flash存储器中,可以满足绝大多数多应用需求,但是如果客户提出支持更多的密钥,那么就要扩展当前的密钥容量,由于SP内置flash存储器很小(常见的为512KB/1MKB),并且SP端没有外挂flash存储器

时,这个需求就无法满足。

[0028] 本发明的目的就是解决密钥容量受到SP端flash存储器容量限制的情况,本发明公开了一种密钥容量扩充系统,该系统将密钥加密存储在AP端的可信安全存储区域,彻底抛弃密钥存储在SP端的传统方式,从而空出了SP的更多flash存储器资源,并且满足安全要求,不会对交易速度造成较大影响。

[0029] 以下是本申请中一些专业术语的含义:

[0030] 工作秘钥(Terminal Transmit Key,TTK),又称为传输秘钥,在POS每次做签到交易时,由POS中心下发给POS机。在联机更新的报文中对工作密钥必须用主密钥加密,形成密文后进行传输。

[0031] 主密钥(Terminal Master Key,TMK)是用来加密、解密工作密钥,实现工作密钥联机传送。

[0032] P_TMK(Plain TMK):明文主密钥

[0033] C_TMK(Cipper TMK):密文主密钥

[0034] P_TTK(Plain TTK):明文传输秘钥

[0035] C_TTK(Ciper TTK):密文传输秘钥

[0036] A_C_TTK(AP Ciper TTK):存储在通用处理器中的目标密文传输密钥

[0037] teekeypub:可信环境公钥

[0038] teekeypri:可信环境私钥

[0039] 图1是根据本发明一实施例的密钥容量扩充系统的系统框图。如图1所示,密钥容量扩充系统100包括通用处理器11和安全处理器12。通用处理器11包括可信安全运行环境(Trusted execution environment,简称TEE)111、第一应用程序112和重放保护内存块(Replay Protected Memory Block,简称RPMB)113。TEE是一种具有运算和储存功能,能提供安全性和完整性保护的独立处理环境。其基本思想是在硬件中为敏感数据单独分配一块隔离的内存,所有敏感数据的计算均在这块内存中进行,并且除了经过授权的接口外,硬件中的其他部分不能访问这块隔离的内存中的信息。以此来实现敏感数据的隐私计算。重放保护内存块113可以读,可以写,但是读和写是受到访问控制和回放保护的。所述第一应用程序112和所述重放保护内存块113位于所述安全运行环境111中。通用处理器11和安全处理器12通信连接。可选地,通用处理器11和安全处理器12通过UART信号线连接。其中,通用处理器11与安全运行环境111中的第一应用程序112进行交互,安全运行环境111生成可信环境公钥teekeypub和可信环境私钥teekeypri,所述可信环境公钥与所述可信环境私钥为非对称密钥对。所述通用处理器11存储可信环境公钥teekeypub,所述第一应用程序112存储可信环境私钥teekeypri。所述重放保护内存块113用于存储密文主密钥C_TMK和所述安全处理器需要的目标密文传输密钥A_C_TTK。

[0040] 本发明的密钥容量扩充系统,第一应用程序和重放保护内存块位于安全运行环境中,且通用处理器存储可信环境公钥,第一应用程序存储可信环境私钥,将目标密文传输密钥存储在通用处理器的重放保护内存块中,保证了密钥的安全性符合要求,解决了密钥容量受到安全处理器的flash存储器限制的问题。

[0041] 图2是图1密钥容量扩充系统的一实施例的交互方法的流程图。其中,通用处理器(AP)和安全处理器(SP)配置为采用图2所示的交互方法进行交互:

[0042] 步骤S211:通用处理器接收原始密文传输密钥C_TTK;

[0043] 步骤S212:从可信安全运行环境(TEE)中的重放保护内存块获取密文主密钥C_TMK。示例性,第一应用程序从重放保护内存块读取密文主密钥C_TMK,第一应用程序通过可信环境私钥teekeypri对密文主密钥C_TMK进行加密,将经过可信环境私钥teekeypri加密的密文主密钥C_TMK发送给通用处理器的PayHardWareServiee,PayHardWareServiee通过可信环境公钥teekeypub解密得到密文主密钥C_TMK。其中,PayHardWareServiee为通用处理器的Android服务,负责管理安全处理器,抽象安全处理器功能,并为应用提供相关功能接口。

[0044] 步骤S213:将原始密文传输密钥C_TTK和密文主密钥C_TMK发送给安全处理器;

[0045] 可选地,在一些实施例中,在步骤S211之前还包括:

[0046] 步骤S201:安全处理器接收明文主密钥P_TMK,在安全环境下生成随机密钥aprootkey,通过随机密钥aprootkey对明文主密钥P_TMK进行加密,获得密文主密钥C_TMK,将密文主密钥C_TMK发送给通用处理器;

[0047] 步骤S202:通用处理器接收密文主密钥C_TMK,通过可信环境公钥teekeypub对获取到的密文主密钥C_TMK进行加密,得到第一主密钥,将第一主密钥传输至第一应用程序,第一应用程序通过可信环境私钥teekeypri对第一主密钥解密,得到密文主密钥C_TMK,将密文主密钥C_TMK存储至重放保护内存块。

[0048] 步骤S22:安全处理器根据原始密文传输密钥C_TTK和密文主密钥C_TMK生成目标密文传输密钥A_C_TTK,将目标密文传输密钥A_C_TTK发送给通用处理器。

[0049] 图3是图2中步骤S22一实施例的流程图。如图3所示,安全处理器根据原始密文传输密钥C_TTK和密文主密钥C_TMK生成目标密文传输密钥A_C_TTK包括:

[0050] 步骤S221:安全处理器通过随机密钥aprootkey解密密文主密钥C_TMK得到明文主密钥P_TMK;

[0051] 步骤S222:安全处理器通过明文主密钥P_TMK对原始密文传输密钥C_TTK进行解密,获得明文传输密钥P_TTK;

[0052] 步骤S223:通过随机密钥aprootkey对明文传输密钥P_TTK进行加密,获得目标密文传输密钥A_C_TTK。

[0053] 可选地,安全处理器还配置为获得明文传输密钥P_TTK之后,将明文传输密钥的标识号(明文传输密钥ID)记录在本地密钥索引列表中。

[0054] 步骤S231:通用处理器通过可信环境公钥teekeypub对获取到的目标密文传输密钥A_C_TTK进行加密,得到第一传输密钥,将第一传输密钥传输至第一应用程序;

[0055] 步骤S232:第一应用程序通过可信环境私钥teekeypri对第一传输密钥解密,得到目标密文传输密钥A_C_TTK,将目标密文传输密钥A_C_TTK存储至重放保护内存块。

[0056] 图4是图2优化实施例的密钥容量扩充系统的交互方法的流程图。如图3所示,密钥容量扩充系统的交互方法400还包括:

[0057] 步骤S411:通用处理器接收计算需求。在本实施例中,计算需求是计算目标密文传输密钥A_C_TTK的消息认证码(MAC)。MAC是将通信双方共享的密钥K和消息m作为输入,生成一个关于K和m的函数值。本申请对计算需求的类型不作限制。

[0058] 步骤S412:从重放保护内存块读取计算需求对应的目标密文传输密钥A_C_TTK。示

例性,第一应用程序从重放保护内存块读取目标密文传输密钥A_C_TTK,第一应用程序通过可信环境私钥teekeypri对目标密文传输密钥A_C_TTK进行加密,将经过可信环境私钥teekeypri加密的目标密文传输密钥A_C_TTK发送给通用处理器的PayHardWareServiee,PayHardWareServiee通过可信环境公钥teekeypub解密得到目标密文传输密钥A_C_TTK。其中,PayHardWareServiee为通用处理器的Android服务,负责管理安全处理器,抽象安全处理器功能,并为应用提供相关功能接口。

[0059] 步骤S413:将目标密文传输密钥A_C_TTK和计算需求发送给安全处理器。

[0060] 步骤S421:安全处理器通过随机密钥aprootkey解密目标密文传输密钥A_C_TTK得到明文传输密钥P_TTK;

[0061] 步骤S422:根据计算需求对明文传输密钥P_TTK进行计算,例如,使用明文传输密钥P_TTK计算MAC数据,将计算结果发送至通用处理器。

[0062] 图5是图2优化实施例的密钥容量扩充系统的交互方法的流程图。如图5所示,密钥容量扩充系统的交互方法还包括通用处理器(AP)和安全处理器(SP)之间进行密钥自检,通用处理器(AP)和安全处理器(SP)之间进行密钥自检包括:

[0063] 步骤51:AP通过申请从TEE中取出一条密钥A_C_TTK,输送一条密钥A_C_TTK至SP;

[0064] 步骤52:SP检查密钥A_C_TTK的密钥检查值(Key Check Value,KCV)是否正确,并且将检查结果输送至AP;

[0065] 步骤53:AP判断自检结果,若A_C_TTK的KCV为正确,进一步判断密钥密文列表是否全部发送;若未发送,重新发送新的密钥密文至SP,若发送完全,进入下一步:

[0066] 步骤54:SP判断自检密钥ID列表和本地密钥索引列表是否一致,并且将自检结果输出至AP。

[0067] 可选地,密钥容量扩充系统的交互方法还包括密钥删除操作,包括:

[0068] 1)通用处理器从重放保护内存块中读取一条目标密文传输密钥A_C_TTK,发送目标密文传输密钥A_C_TTK给安全处理器;

[0069] 2)安全处理器通过随机密钥aprootkey对目标密文传输密钥A_C_TTK进行解密,得到明文传输密钥P_TTK,当接收到删除指令后,删除本地密钥索引列表中明文传输密钥的标识号,发送“删除成功信号”给通用处理器;

[0070] 3)通用处理器中的第一应用程序根据“删除成功信号”删除重放保护内存块中明文传输密钥P_TTK对应的目标密文传输密钥A_C_TTK。

[0071] 可选地,密钥容量扩充系统的交互方法还包括相同密钥数据检测,相同密钥数据检测包括:安全处理器获得待写入的明文传输密钥后,通用处理器将重放保护内存块中所有的目标密文传输密钥发送给安全处理器,安全处理器解密所有的目标密文传输密钥,将待写入的明文传输密钥与解密出的所有明文传输密钥进行对比,如果存在与待写入的明文传输密钥相同的明文传输密钥,则删除待写入的明文传输密钥。其中判断是否存在与待写入的明文传输密钥相同的明文传输密钥包括判断算法类型、密钥长度、密钥数据是否完全相同,如果全部相同,则判断存在相同密钥。换而言之,待写入的明文传输密钥已经存在重放保护内存块中了,不需要重复写入。

[0072] 可选地,密钥容量扩充系统的交互方法还包括异常处理,异常处理包括:

[0073] (1)安全处理器还配置为监测到攻击信号时,删除随机密钥,通用处理器存储的密

文密钥失去解密密钥(随机密钥),等同于失效。

[0074] (2)安全处理器还配置为将攻击信号发送给通用处理器,通用处理器还配置为接收到攻击信号后通知第一应用程序删除重放保护内存块中的数据。

[0075] (3)通用处理器还配置为接收到出厂设置命令时,删除可信环境公钥。

[0076] 通用丢失可信环境公钥teerkeypub后,无法获取到正确的A_C_TTK密钥数据。

[0077] (4)通用处理器还配置为接收到删除第一应用程序命令时,删除可信环境公钥。

[0078] 本发明的密钥容量扩充系统的密钥交互方法,保证了密钥的安全性符合要求,且不会对交易速度造成较大影响。

[0079] 上文已对基本概念做了描述,显然,对于本领域技术人员来说,上述发明披露仅仅作为示例,而并不构成对本申请的限定。虽然此处并没有明确说明,本领域技术人员可能会对本申请进行各种修改、改进和修正。该类修改、改进和修正在本申请中被建议,所以该类修改、改进、修正仍属于本申请示范实施例的精神和范围。

[0080] 同时,本申请使用了特定词语来描述本申请的实施例。如“一个实施例”、“一实施例”、和/或“一些实施例”意指与本申请至少一个实施例相关的某一特征、结构或特点。因此,应强调并注意的是,本说明书中在不同位置两次或多次提及的“一实施例”或“一个实施例”或“一替代性实施例”并不一定是指同一实施例。此外,本申请的一个或多个实施例中的某些特征、结构或特点可以进行适当的组合。

[0081] 本申请的一些方面可以完全由硬件执行、可以完全由软件(包括固件、常驻软件、微码等)执行、也可以由硬件和软件组合执行。以上硬件或软件均可被称为“数据块”、“模块”、“引擎”、“单元”、“组件”或“系统”。处理器可以是一个或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理器件(DAPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器或者其组合。此外,本申请的各方面可能表现为位于一个或多个计算机可读介质中的计算机产品,该产品包括计算机可读程序编码。例如,计算机可读介质可包括,但不限于,磁性存储设备(例如,硬盘、软盘、磁带……)、光盘(例如,压缩盘CD、数字多功能盘DVD……)、智能卡以及闪存设备(例如,卡、棒、键驱动器……)。

[0082] 计算机可读介质可能包含一个内含有计算机程序编码的传播数据信号,例如在基带上或作为载波的一部分。该传播信号可能有多种表现形式,包括电磁形式、光形式等等、或合适的组合形式。计算机可读介质可以是除计算机可读存储介质之外的任何计算机可读介质,该介质可以通过连接至一个指令执行系统、装置或设备以实现通讯、传播或传输供使用的程序。位于计算机可读介质上的程序编码可以通过任何合适的介质进行传播,包括无线电、电缆、光纤电缆、射频信号、或类似介质、或任何上述介质的组合。

[0083] 同理,应当注意的是,为了简化本申请披露的表述,从而帮助对一个或多个发明实施例的理解,前文对本申请实施例的描述中,有时会将多种特征归并至一个实施例、附图或对其的描述中。但是,这种披露方法并不意味着本申请对象所需要的特征比权利要求中提及的特征多。实际上,实施例的特征要少于上述披露的单个实施例的全部特征。

[0084] 如本申请和权利要求书中所示,除非上下文明确提示例外情形,“一”、“一个”、“一种”和/或“该”等词并非特指单数,也可包括复数。一般说来,术语“包括”与“包含”仅提示包括已明确标识的步骤和元素,而这些步骤和元素不构成一个排它性的罗列,方法或者设备

也可能包含其他的步骤或元素。

[0085] 除非另外具体说明,否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本申请的范围。同时,应当明白,为了便于描述,附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论,但在适当情况下,所述技术、方法和设备应当被视为授权说明书的一部分。在这里示出和讨论的所有示例中,任何具体值应被解释为仅仅是示例性的,而不是作为限制。因此,示例性实施例的其它示例可以具有不同的值。应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步讨论。

[0086] 此外,需要说明的是,使用“第一”、“第二”等词语来限定零部件,仅仅是为了便于对相应零部件进行区别,如没有另行声明,上述词语并没有特殊含义,因此不能理解为对本申请保护范围的限制。此外,尽管本申请中所使用的术语是从公知公用的术语中选择的,但是本申请说明书中所提及的一些术语可能是申请人按他或她的判断来选择的,其详细含义在本文的描述的相关部分中说明。此外,要求不仅仅通过所使用的实际术语,而是还要通过每个术语所蕴含的意义来理解本申请。

[0087] 本申请中使用了流程图用来说明根据本申请的实施例的系统所执行的操作。应当理解的是,前面或下面操作不一定按照顺序来精确地执行。相反,可以按照倒序或同时处理各种步骤。同时,或将其他操作添加到这些过程中,或从这些过程移除某一步或数步操作。

[0088] 虽然本申请已参照当前的具体实施例来描述,但是本技术领域中的普通技术人员应当认识到,以上的实施例仅是用来说明本申请,在没有脱离本申请精神的情况下还可作出各种等效的变化或替换,因此,只要在本申请的实质精神范围内对上述实施例的变化、变型都将落在本申请的权利要求书的范围内。

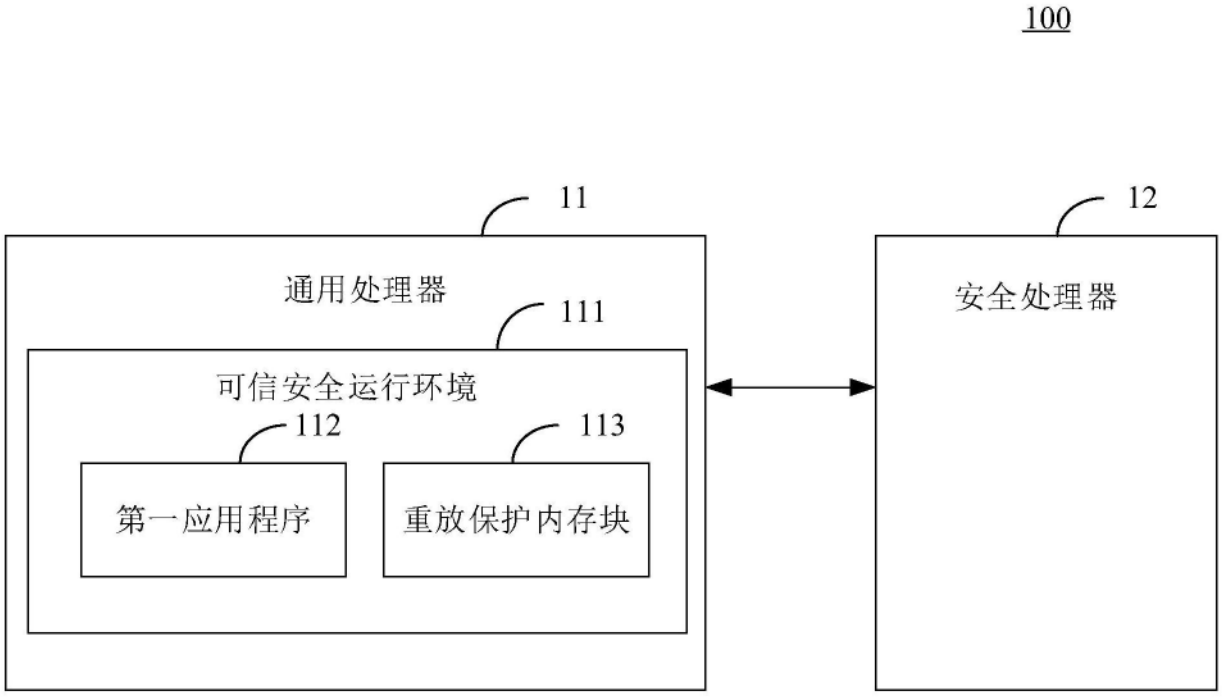


图1

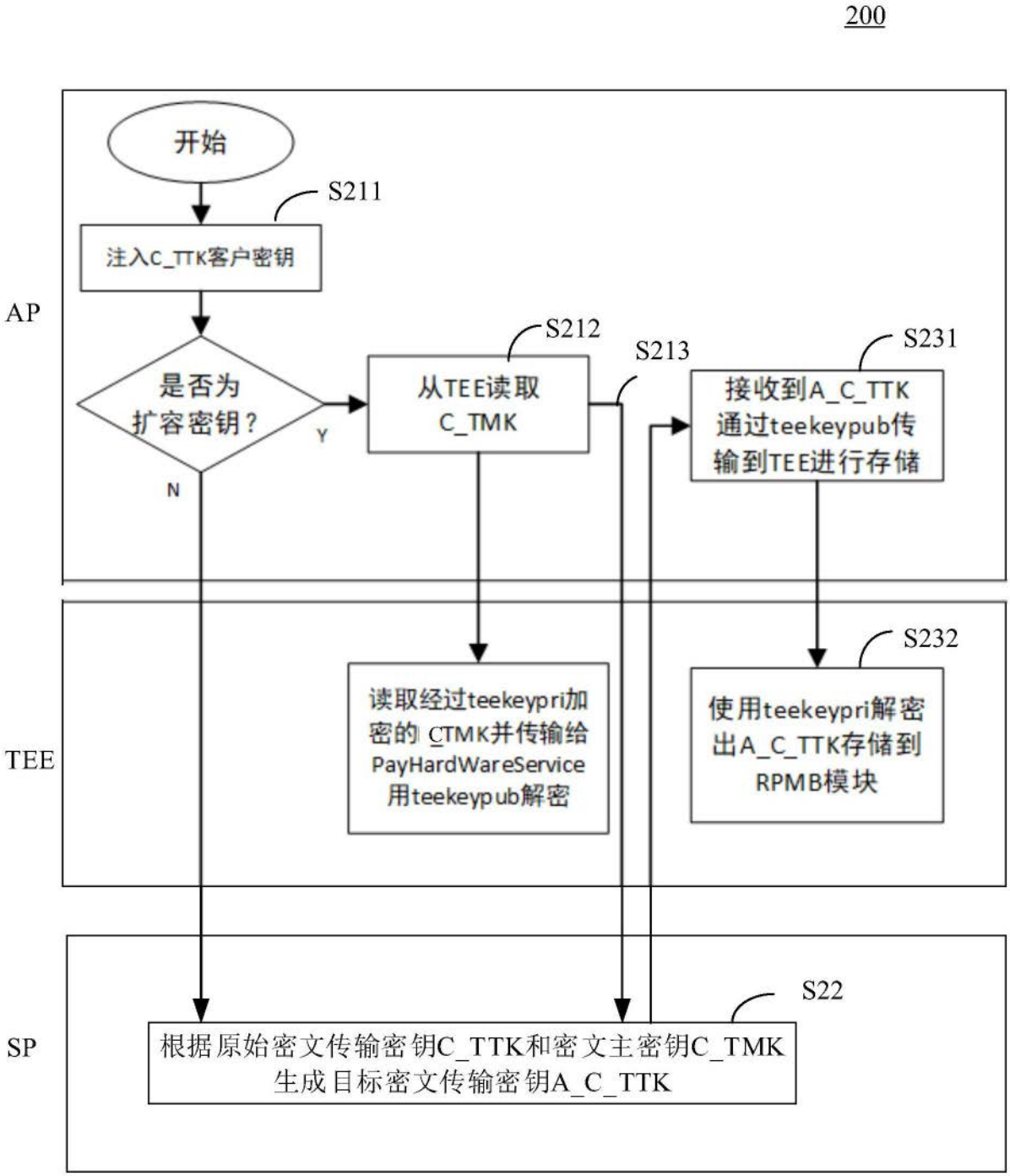

200
开始
S211
注入C_TTK客户密钥
AP
是否为
扩容密钥？
Y
N
S212
从TEE读取
C_TMK
S213
S231
接收到A_C_TTK
通过teekeypub传
输到TEE进行存储
TEE
读取经过teekeypri加
密的 CTMK并传输给
PayHardWareService
用teekeypub解密
S232
使用teekeypri解密
出A_C_TTK存储到
RPMB模块
SP
S22
根据原始密文传输密钥C_TTK和密文主密钥C_TMK
生成目标密文传输密钥A_C_TTK

图2

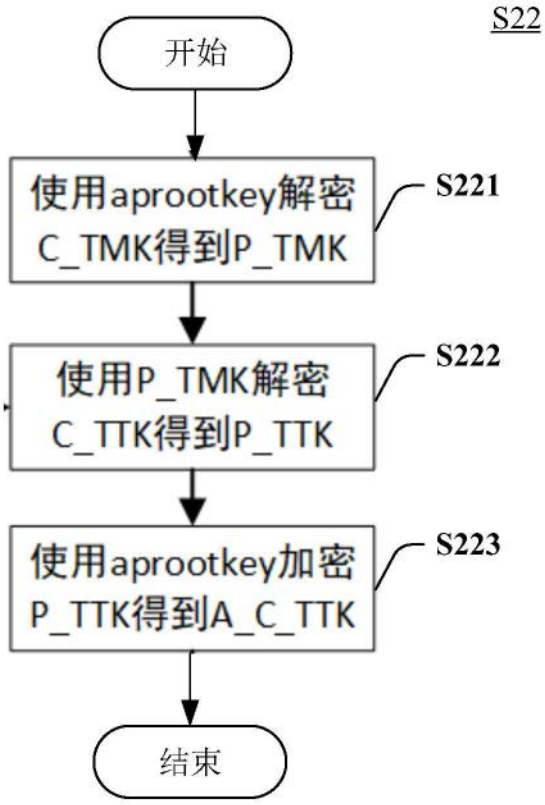

S22
开始
使用aprootkey解密
C_TMK得到P_TMK
S221
使用P_TMK解密
C_TTK得到P_TTK
S222
使用aprootkey加密
P_TTK得到A_C_TTK
S223
结束

图3

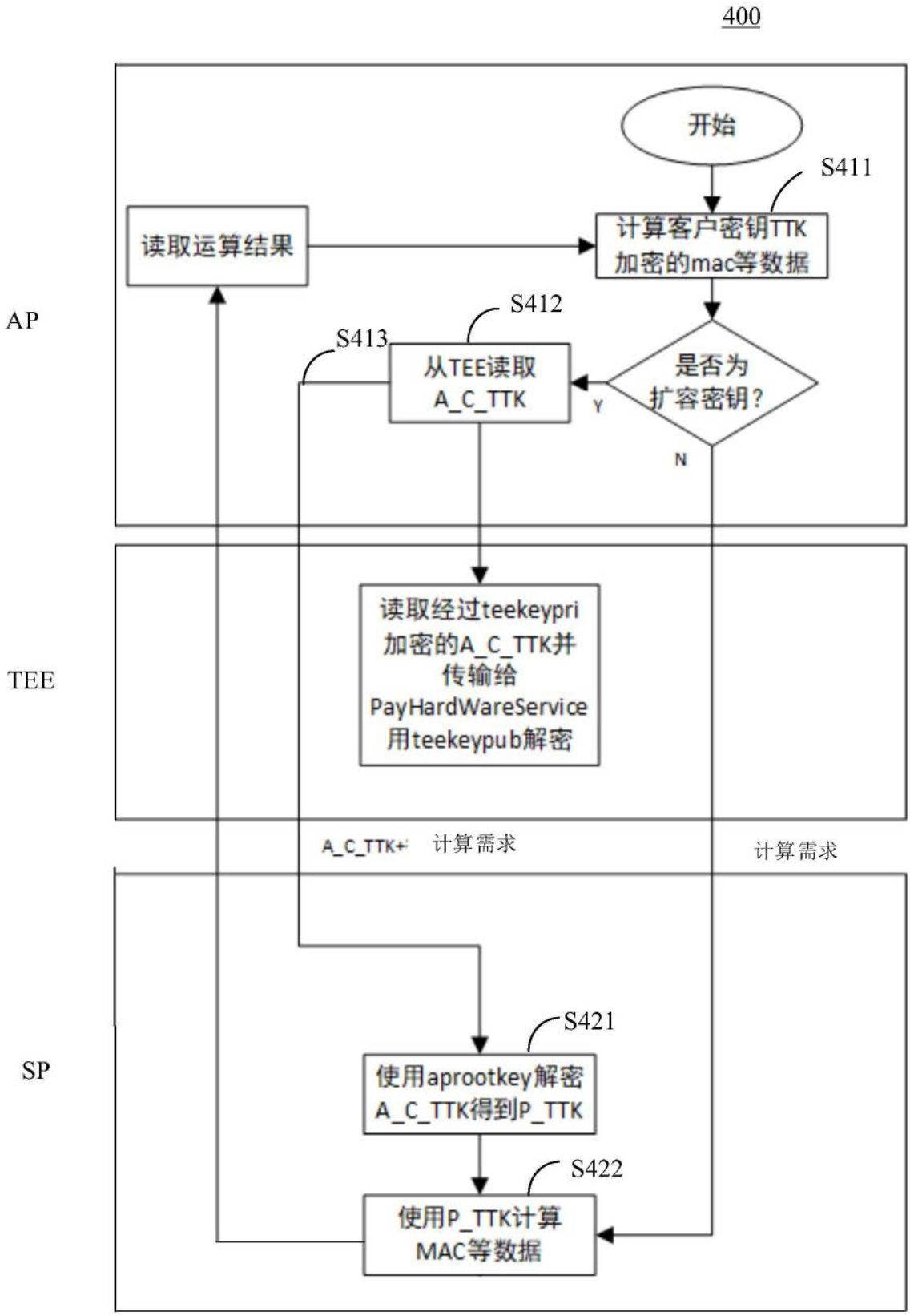

400
AP
TEE
SP
开始
S411
计算客户密钥TTK
加密的mac等数据
读取运算结果
S412
S413
从TEE读取
A_C_TTK
是否为
扩容密钥?
Y
N
读取经过teekeypri
加密的A_C_TTK并
传输给
PayHardWareService
用teekeypub解密
A_C_TTK+
计算需求
计算需求
S421
使用aprootkey解密
A_C_TTK得到P_TTK
S422
使用P_TTK计算
MAC等数据

图4

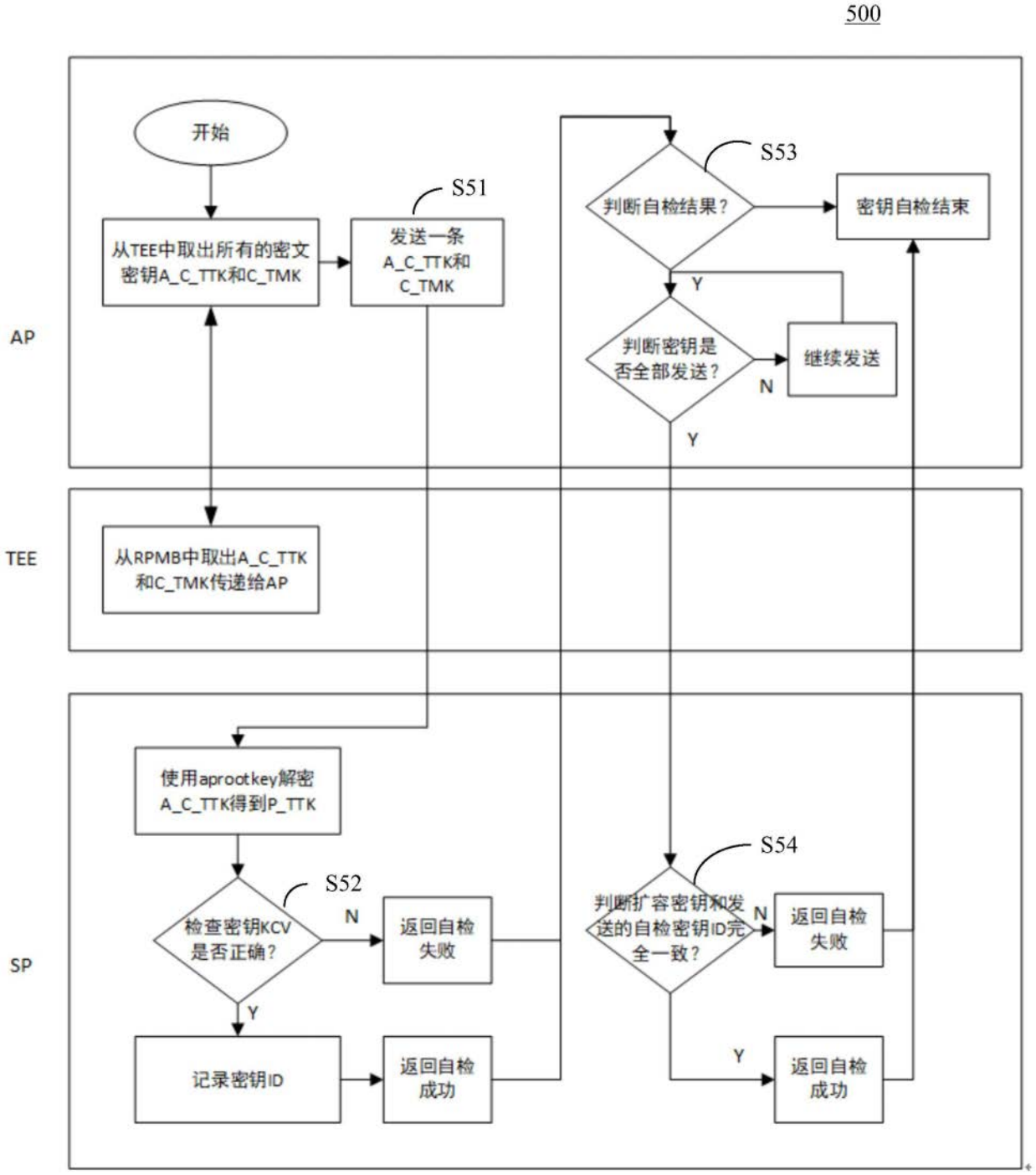

500
AP
TEE
SP
开始
从TEE中取出所有的密文密钥A_C_TTK和C_TMK
S51
发送一条A_C_TTK和C_TMK
从RPMB中取出A_C_TTK和C_TMK传递给AP
使用aprootkey解密A_C_TTK得到P_TTK
S52
检查密钥KCV是否正确?
N
返回自检失败
Y
记录密钥ID
返回自检成功
S53
判断自检结果?
密钥自检结束
Y
判断密钥是否全部发送?
N
继续发送
Y
S54
判断扩容密钥和发送的自检密钥ID完全一致?
N
返回自检失败
Y
返回自检成功

图5