(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 5 月 24 日 (24.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/090763 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2017/105732

(22) 国际申请日: 2017 年 10 月 11 日 (11.10.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611006175.9 2016年11月15日 (15.11.2016) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 王琪 (WANG, Qi); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。 刘国宝 (LIU, Guobao); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区宝盛南路1号院20号楼8层101-01, Beijing 100192 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) **Title:** METHOD AND DEVICE FOR CONFIGURING TERMINAL MASTER KEY

(54) 发明名称: 一种终端主密钥的设置方法和装置

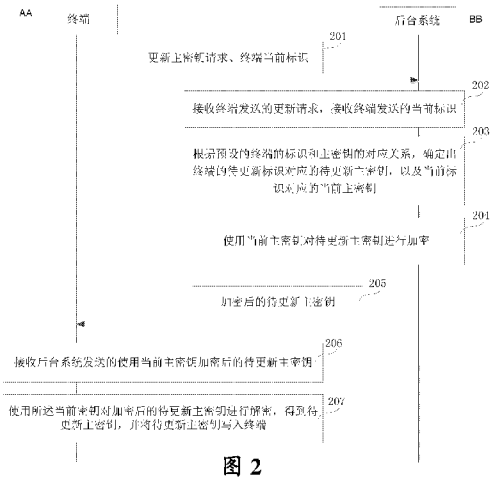

图 2

201 MASTER KEY UPDATE REQUEST, AND CURRENT TERMINAL IDENTIFIER
202 RECEIVE THE UPDATE REQUEST TRANSMITTED FROM TERMINAL, AND RECEIVE THE CURRENT IDENTIFIER TRANSMITTED FROM TERMINAL
203 DETERMINE, ACCORDING TO CORRESPONDENCES OF PRECONFIGURED TERMINAL IDENTIFIERS AND MASTER KEYS, A MASTER KEY TO BE UPDATED AND CORRESPONDING TO THE IDENTIFIER TO BE UPDATED OF THE TERMINAL, AND A CURRENT MASTER KEY CORRESPONDING TO THE CURRENT IDENTIFIER
204 EMPLOY THE CURRENT MASTER KEY TO ENCRYPT THE MASTER KEY TO BE UPDATED
205 THE ENCRYPTED MASTER KEY TO BE UPDATED
206 RECEIVE THE ENCRYPTED MASTER KEY TO BE UPDATED ENCRYPTED BY THE CURRENT MASTER KEY AND TRANSMITTED FROM BACKEND SYSTEM
207 EMPLOY THE CURRENT MASTER KEY TO DECRYPT THE ENCRYPTED MASTER KEY TO BE UPDATED TO OBTAIN THE MASTER KEY TO BE UPDATED, AND WRITE THE MASTER KEY TO BE UPDATED INTO TERMINAL
AA TERMINAL
BB BACKEND SYSTEM

(57) **Abstract:** A method and device for configuring a terminal master key. The method comprises: a backend system receives a master key update request transmitted from a terminal; and the backend system receives a current terminal identifier transmitted from the terminal; wherein the master key update request comprises an identifier to be updated of the terminal. The method further comprises: the backend system determines, according to correspondences of preconfigured terminal identifiers and master keys, a master key to be updated and corresponding to the identifier to be updated of the terminal, and a current master key corresponding to the current terminal identifier; and the backend system employs the current master key to encrypt the master key to be updated, and transmits to the terminal the encrypted master key to be updated; wherein the terminal employs the current master key to decrypt the encrypted master key to be updated to obtain the master key to be updated, and writes the master key to be updated into the terminal. The embodiment is used to enhance security of updating a master key of a terminal.

WO 2018/090763 A1

[见续页]

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种终端主密钥的设置方法和装置，后台系统接收终端发送的更新主密钥请求；接收终端发送的终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；后台系统根据预设的终端的标识和主密钥的对应关系，确定出终端的待更新标识对应的待更新主密钥，以及当前标识对应的当前主密钥；后台系统使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给终端；其中，加密后的待更新主密钥用于使终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥写入终端；提高了更新终端主密钥的安全性。

一种终端主密钥的设置方法和装置

本申请要求在2016年11月15日提交中国专利局、申请号为201611006175.9、发明名称为“一种终端主密钥的设置方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明实施例涉及网络认证领域，尤其涉及一种终端主密钥的设置方法和装置。

背景技术

在现有技术中，由于销售点（Point of sales，简称POS）终端安全、便捷的特点，受到用户、商家、银行的青睐，为了确保交易过程的安全性，每台POS终端拥有唯一的终端主密钥；当使用POS终端工作时，需要终端主密钥对工作密钥进行加密，确保信息交互过程信息的安全。因此，当POS终端在布放前，需要由专业化服务机构或收单机构需将每台POS终端对应的密码键盘拿到安全的区域，可以采用专用集成电路（Integrated Circuit，简称IC）芯片或使用母POS将终端主密钥灌入POS终端的密码键盘中；而且，当需要对POS 终端的终端主密钥进行更新时，也需要专业化服务机构或收单机构将该台POS终端对应的密码键盘拿到安全的区域，采用专用集成电路（Integrated Circuit，简称IC）芯片或使用母POS往待更新的POS终端的密码键盘中重新灌入待更新的终端主密钥。

由于在现有技术中POS终端主密钥的初始化和更新需要花费购买母POS的成本；且在POS终端布放前或POS终端需要更新终端主密钥时，需要由专业化服务机构或收单机构手动将密码键盘拿到安全的区域，使用母 POS 往POS 终端的密码键盘灌入终端主密钥，整个过程周期较长、增加运输成本、

并需要投入相应的人力。

综上，亟需一种终端主密钥的更新方案，用于安全、便捷地设置终端主密钥。

发明内容

本发明实施例提供了一种终端主密钥的设置方法和装置，用于提高设置终端主密钥的安全性和便捷性。

第一方面，本发明实施例提供一种终端主密钥的设置方法，该方法包括：后台系统接收终端发送的更新主密钥请求；接收终端发送的终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；后台系统根据预设的终端的标识和主密钥的对应关系，确定出终端的待更新标识对应的待更新主密钥，以及当前标识对应的当前主密钥；后台系统使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给终端；其中，加密后的待更新主密钥用于使终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥写入终端。

由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，也无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

可选地，终端的待更新标识包括终端待更新商户号和待更新终端号；终端的原始标识包括终端的原始商户号和原始终端号；其中，待更新商户号和

原始商户号相同或不同；待更新终端号和原始终端号相同或不同。

可选地，后台系统接收终端发送的更新主密钥请求之前，还包括：后台系统接收终端发送的初始化主密钥请求；接收终端发送的终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；后台系统根据预设的终端的标识和主密钥的对应关系，确定出终端的初始化标识对应的初始化主密钥；后台系统产生第一密钥；后台系统使用公钥对第一密钥进行加密，将得到的加密后的第一密钥发送给终端；后台系统使用第一密钥对初始化主密钥进行加密，将得到加密后的初始化主密钥发送给终端；其中，加密后的初始化主密钥用于使终端使用私钥对加密后的第一密钥进行解密得到第一密钥后，使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，后台系统接收终端发送的初始化主密钥请求之后，根据预设的终端的标识和主密钥的对应关系确定出终端的初始化标识对应的初始化主密钥之前，还包括：后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识。

第二方面，本发明实施例提供一种终端主密钥的设置方法，该方法包括：终端向后台系统发送更新主密钥请求；发送终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；终端接收后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，当前主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的当前标识对应的主密钥；待更新主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的待更新标识对应的主密钥；终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥替换当前主密钥。

由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，也无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

可选地，终端向后台系统发送更新主密钥请求后台系统之前，还包括：终端向后台系统发送初始化主密钥请求；发送终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；终端接收后台系统发送的使用公钥加密后的第一密钥；终端接收后台系统发送的使用第一密钥加密后的初始化主密钥；终端使用私钥对加密后的第一密钥进行解密得到第一密钥；终端使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，初始化主密钥为后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的初始化标识对应的主密钥。

第三方面，本发明实施例中提供可一种电子设备，包括：处理器、存储器、收发器和通信接口，其中，处理器、存储器、收发器和通信接口之间通过总线连接；

所述处理器，用于读取所述存储器中的程序，执行下列方法：接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识；根据预设的终端的标识

和主密钥的对应关系，确定出所述终端的待更新标识对应的待更新主密钥，以及所述当前标识对应的当前主密钥；使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给所述终端；其中，所述加密后的待更新主密钥用于使所述终端使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥写入所述终端。

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

所述收发器，用于在所述处理器的控制下接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识。

第四方面，本发明实施例中提供可一种电子设备，包括：处理器、存储器、收发器和通信接口，其中，处理器、存储器、收发器和通信接口之间通过总线连接；

所述处理器，用于读取所述存储器中的程序，执行下列方法使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥替换所述当前主密钥；

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

所述收发器，用于在所述处理器的控制下向后台系统发送更新主密钥请求；发送所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识；接收所述后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，所述当前主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述当前标识对应的主密钥；所述待更新主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述待更新标识对应的主密钥。

第五方面，本申请实施例提供一种后台系统，用于实现上述第一方面或第一方面中的任意一种方法，包括相应的功能模块，分别用于实现以上方法中的步骤。

第六方面，本申请实施例提供一种终端，用于实现上述第二方面或第二方面中的任意一种的方法，包括相应的功能模块，分别用于实现以上方法中的步骤。

第七方面，本申请实施例提供一种非暂态计算机可读存储介质，计算机存储介质中存储有指令，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法，或者使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法。

第八方面，本申请实施例提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法，或者使得计算机执行第二方面或第二方面的任意可能的实现方式中的方法。

由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，也无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，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获得其他的附图。

图 1 为本发明实施例提供的一种通信系统的架构示意图；

图 2 为本发明实施例提供的一种终端主密钥的设置方法流程示意图；

图 3 为本发明实施例提供的一种后台系统的结构示意图；

图 4 为本发明实施例提供的一种终端的结构示意图；

图 5 为本发明实施例提供的一种电子设备的结构示意图；

图 6 为本发明实施例提供的另一种电子设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案及有益效果更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。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。

图 1 示出了应用本发明实施例的一种通信系统的架构示意图。如图 1 所示，该系统架构可以包括后台系统 101、终端 102；其中，后台系统 101 可以包括服务器 103，加密机 104；终端 102 可以包括终端客户端 105，密码键盘 106；终端与后台系统之间可通过无线或有线的方式进行连接，进而实现了后台系统与终端之间的远程信息交互。终端中的终端客户端与密码键盘通过电路板连接，后台系统中的服务器与机密机通过局域网连接。

服务器 103 存储有终端需要访问的资源。服务器可以是用于与终端设备进行通信的网络设备，可以调用加密机进行加密、解密计算。

加密机 104 属于专用设备，用于对信息进行加密、解密计算；存储主密钥。终端 102 可以经无线接入网（Radio Access Network，简称 RAN）与一个或多个核心网进行通信，终端可以为智能 POS 终端。

终端客户端 105 运行与 POS 终端之上，能够调用密码接盘进行加密、解

密计算，可以更新终端主密钥，可以与后台系统建立通信。

密码键盘 106 通过电路板安装在 POS 终端上，用于保存终端主密钥；用来保护交易中的过程密钥；用于对 POS 终端接收到的终端主密钥进行解密，并用新的主密钥替换原来的主密钥；可以预装数据加密标准（Data Encryption Standard，简称 DES）算法、（Message Authentication Codes，简称 MAC）算法、PINBLOCK 运算，用户可选国家密码管理委员会加密芯片内含密钥管理程序，用最简单的终端实现密钥管理，防止密钥在设置过程中被窃取密钥在内部采用加密方式存放，不提供任何密钥问路径，强行拆卸时密钥和相关重要数据会自动销毁。保证了密码在线传输都是以密文的方式进行。

基于图 1 所示的系统架构，图 2 示例性示出了本发明实施例提供的一种终端主密钥的设置方法流程示意图，如图 2 所示，该终端主密钥的设置方法包括以下步骤：

步骤 201，终端向后台系统发送更新主密钥请求；发送终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；

步骤 202，后台系统接收终端发送的更新主密钥请求；接收终端发送的终端的当前标识；

步骤 203，后台系统根据预设的终端的标识和主密钥的对应关系，确定出终端的待更新标识对应的待更新主密钥，以及当前标识对应的当前主密钥；

步骤 204，后台系统使用当前主密钥对待更新主密钥进行加密；

步骤 205，将得到加密后的待更新主密钥发送给终端；其中，加密后的待更新主密钥用于使终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥替换当前主密钥；

步骤 206，终端接收后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，当前主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的当前标识对应的主密钥；待更新主密钥为后台系统根据预设的终

端的标识和主密钥的对应关系确定出的待更新标识对应的主密钥;

步骤 207，终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥写入终端。

由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，页无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

可选地，本发明实施例中，终端的标识包括终端号和商户号；终端号和商户号能唯一的标识该终端，一个终端号和一个商户号对应一个终端主密钥；终端的待更新标识包括待更新终端号和待更新商户号；终端的当前标识包括当前终端号和当前商户号；其中，待更新终端号和当前终端号相同或者不相同，待更新商户号和当前商户号可以相同或者不相同。

可选地，终端向后台系统发送更新主密钥请求之前，终端与后台系统建立双向安全认证通道。可选地，双向认证安全通道的建立过程：终端向后台系统发送安全认证请求，后台系统在接收到该安全认证请求后，向终端发送安全认证信息，其中，该安全真人信息包括后台系统标识；终端根据从后台系统接收的安全认证信息对后台系统进行安全认证；如果认证未通过，则断开终端和后台之间的连接；如果认证通过，则终端向后台系统发送安全认证信息，其中，该安全信息包括终端的标识，后台系统根据从终端接收的安全认证信息对终端进行安全认证；如果认证未通过，则断开终端和后台系统之

间的连接；如果通过，表明建立了安全双向认证通道。可选地，终端与客户端之间的双向安全认证通道连接，如安全套层协议(Secure Socket Layer，简称SSL)/安全传输层（Transport Layer Security Protocol，简称 TLS），进而确保在通信链路上保证传输的数据的完整性和安全性，进而，进一步提高了更新终端主密钥的安全性。

可选地，终端可置于后台系统的远程端，也可置于后台系统的近程端。后台系统可部署在可信的认证机构内，如金融 POS 收单服务的专业化服务机构或收单机构，如此，后台系统可远程更新终端主密钥，进而避免了通过手动的方式使用母 POS 终端更新终端主密钥，极大的缩短了终端的布放周期，降低了终端布放的人力成本，有利于智能 POS 终端的推广与发展，从而推动金融 POS 行业的发展。

可选地，终端向后台系统发送终端的当前标识，在建立双向安全认证通道的过程中发送；也可以将终端的当前的标识携带在更新主密钥请求中；所以后台系统获取当前标识可以通过双向安全认证通道获取，也可以通过接收到的更新主密钥的请求中获取。

可选地，后台系统接收到终端的当前标识和待更新标识后，根据预设的终端的标识与主密钥的对应的关系，确定出当前标识对应的当前主密钥，待更新标识对应的待更新主密钥。可选地，后台服务器在确定当前主密钥或待更新主密钥至少一个不存在，则后台服务器向终端发送不存在响应；在确定当前主密钥和待更新主密钥均存在的情况下，则后台服务器将当前主密钥和待更新主密钥发送到加密机中。

可选地，终端接收到后台系统发送的使用当前主密钥加密的待更新主密钥后，调用密码键盘解解密，即使用密码键盘中的当前主密钥解密用当前主

密钥加密的待更新主密钥，得到待更新主密钥，将待更新主密钥写入终端，替换当前主密钥；终端主密钥的明文包括：待更新主密钥和当前主密钥，均不出现在密码键盘和加密机外的的任何其他地方，进而提高了终端主密钥的更新方法安全性。

可选地，终端向后台系统发送更新主密钥请求后台系统之前，还包括：终端向后台系统发送初始化主密钥请求；发送终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；终端接收后台系统发送的使用公钥加密后的第一密钥；终端接收后台系统发送的使用第一密钥加密后的初始化主密钥；终端使用私钥对加密后的第一密钥进行解密得到第一密钥；终端使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

相应地，可选地，后台系统接收终端发送的更新主密钥请求之前，还包括：后台系统接收终端发送的初始化主密钥请求；接收终端发送的终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；后台系统根据预设的终端的标识和主密钥的对应关系，确定出终端的初始化标识对应的初始化主密钥；后台系统产生第一密钥；后台系统使用公钥对第一密钥进行加密，将得到的加密后的第一密钥发送给终端；后台系统使用第一密钥对初始化主密钥进行加密，将得到加密后的初始化主密钥发送给终端；其中，加密后的初始化主密钥用于使终端使用私钥对加密后的第一密钥进行解密得到第一密钥后，使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥，并将初始化主密钥写入终端。

可选地，终端向后台系统发送终端的原始标识，可以通过双向认证安全通道发送，也可以通过将原始标识携带在初始化请求中发送；所以，后台系统获取原始标识可以通过接收到的初始化请求，也可以通过建立双向安全认证通道获取。

可选地，终端与后台系统建立安全认证双向通道后，终端的客户端调用密码键盘接口产生非对称过程密钥，并将非对称过程密钥中的私钥保存在密码键盘中，终端客户端调用公钥，并将公钥携带在初始化的请求中；可选地，原始标识为生产商预置的标识，当后台系统确定获取到的原始标识为生产商预置的标识时，才执行对该终端进行主密钥初始化的过程。

可选地，第一密钥为随机密钥。

可选地，后台系统中的服务器在确定原始标识为生产商预置的标识的情况下，确定终端的初始化标识对应的终端主密钥，调用后台系统中的加密机产生随机密钥，其中，随机密钥可以为临时终端主密钥，该临时终端主密钥与主密钥使用相同的算法对随机信息加密获得，使用公钥对临时终端主密钥进行加密获得加密后的临时终端主密钥；使用临时终端主密钥对初始化终端主密钥进行加密，获得加密后的初始化终端主密钥。

可选地，终端接收到用公钥加密的临时终端主密钥和用临时终端主密钥加密的初始化主密钥之后，终端客户端调用密码键盘对其进行解密，在密码接盘中使用私钥对用公钥加密的临时终端主密钥进行解密，获得临时终端主密钥，使用临时终端主密钥对使用临时终端主密钥加密的初始化终端主密钥进行解密获得初始化终端主密钥，将获得的初始化终端主密钥写入密码键盘。通过非对称过程密钥进行加密解密极大的提高了初始终端主密钥的安全性。

通过上述初始化的方法，可以进一步提高初始化终端主密钥的安全性，使用临时终端主密钥加密初始化终端主密钥，公钥加密临时终端主密钥；而且，终端主密钥的明文不出现在密码键盘和加密机外的的任何其他地方，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都

是密文，即使被窃取，也无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

可选地，后台系统接收终端发送的初始化主密钥请求之后，根据预设的终端的标识和主密钥的对应关系确定出终端的初始化标识对应的初始化主密钥之前，还包括：后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识。

相应地，可选地，初始化主密钥为后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的初始化标识对应的主密钥。

可选地，在终端初次布放前，生产商通常预置标识，默认终端主密钥写入密码键盘，初次进行密码键盘中终端主密钥的初始化使用该默认的终端主密钥进行初始化。可选地，终端的原始标识包括原始终端号和原始商户号。可选地，后台系统确定原始标识为生产商预置的标识的情况下，才允许对终端主密钥进行初始化操作，进而确保了终端的安全性，以及便于后续终端出现安全问题时进行追究责任。

需要说明的一点是：上述针对终端主密钥的设置的说明仅是示例性和解释性的，并不用于限定本发明。

从上述内容可以看出：由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前

终端主密钥和待更新终端主密钥都是密文，即使被窃取，页无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

图 3 示例性示出了本发明实施例提供的一种后台系统的结构示意图。

基于相同构思，本发明实施例提供一种后台系统，如图 3 所示，后台系统 300 包括接收单元 301、处理单元 302。其中：

接收单元，用于接收终端发送的更新主密钥请求；接收终端发送的终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；

处理单元，根据预设的终端的标识和主密钥的对应关系，确定出终端的待更新标识对应的待更新主密钥，以及当前标识对应的当前主密钥；使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给终端；其中，加密后的待更新主密钥用于使终端使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥写入终端。

可选地，接收单元，还用于：接收终端发送的初始化主密钥请求；接收终端发送的终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；

所述处理单元，用于：根据预设的终端的标识和主密钥的对应关系，确定出终端的初始化标识对应的初始化主密钥；产生第一密钥；使用公钥对第一密钥进行加密，将得到的加密后的第一密钥发送给终端；使用第一密钥对初始化主密钥进行加密，将得到加密后的初始化主密钥发送给终端；其中，加密后的初始化主密钥用于使终端使用私钥对加密后的第一密钥进行解密得到第一密钥后，使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，处理单元，还用于：根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识。

图 4 示例性示出了本发明实施例提供的一种终端的结构示意图。

基于相同构思，本发明实施例提供一种终端，如图 4 所示，终端 400 包括发送单元 401、接收单元 402 和处理单元 403。其中：

发送单元，用于向后台系统发送更新主密钥请求；发送终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；

接收单元，用于接收后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，当前主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的当前标识对应的主密钥；待更新主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的待更新标识对应的主密钥；

处理单元，用于使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥替换当前主密钥。

可选地，发送单元，还用于：向后台系统发送初始化主密钥请求；发送终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；

述接收单元，用于：接收后台系统发送的使用公钥加密后的第一密钥；接收后台系统发送的使用第一密钥加密后的初始化主密钥；

述处理单元，用于：使用私钥对加密后的第一密钥进行解密得到第一密钥；使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，初始化主密钥为后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的初始化标识对应的主密钥。

从上述内容可以看出：本发明实施例中，由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了

远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，页无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

基于相同构思，本申请提供一种电子设备，可用于执行上述后台系统侧的方法流程。图 5 为本申请提供的一种电子设备的结构示意图。该电子设备包括处理器 501、存储器 502、收发器 503 和通信接口 504; 其中，处理器 501、存储器 502、收发器 503 和通信接口 504 通过总线 505 相互连接。

总线 505 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 5 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 502 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，简称 RAM）; 存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，简称 HDD）或固态硬盘（solid-state drive，简称 SSD）; 存储器 502 还可以包括上述种类的存储器的组合。

通信接口 504 可以为有线通信接入口，无线通信接口或其组合，其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为 WLAN 接口。

处理器 501 可以是中央处理器（central processing unit，简称 CPU），网络处理器（network processor，简称 NP）或者 CPU 和 NP 的组合。

处理器 501 还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，简称 ASIC），可编程逻辑器件（programmable logic device，简称 PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device，简称 CPLD），现场可编程逻辑门阵列（field-programmable gate array，简称 FPGA），通用阵列逻辑（generic array logic，简称 GAL）或其任意组合。

所述处理器 501，用于读取所述存储器 502 中的程序，执行下列方法：接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识；根据预设的终端的标识和主密钥的对应关系，确定出所述终端的待更新标识对应的待更新主密钥，以及所述当前标识对应的当前主密钥；使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给所述终端；其中，所述加密后的待更新主密钥用于使所述终端使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥写入所述终端。

所述存储器 502，用于存储一个或多个可执行程序，可以存储所述处理器 501 在执行操作时所使用的数据；

所述收发器 503，用于在所述处理器 501 的控制下接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识。

可选地，所述收发器，还用于：接收终端发送的初始化主密钥请求；接收终端发送的终端的原始标识；其中，初始化主密钥请求中包括终端的初始化标识和公钥；

所述处理器，用于：根据预设的终端的标识和主密钥的对应关系，确定

出终端的初始化标识对应的初始化主密钥；产生第一密钥；使用公钥对第一密钥进行加密，将得到的加密后的第一密钥发送给终端；使用第一密钥对初始化主密钥进行加密，将得到加密后的初始化主密钥发送给终端；其中，加密后的初始化主密钥用于使终端使用私钥对加密后的第一密钥进行解密得到第一密钥后，使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，所述处理器，还用于：根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识。

应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，接收单元 301 可以由收发器实现，处理单元 302 可以由处理器实现。如图 5 所示，电子设备 500 可以包括处理器 501、收发器 503 和存储器 502。其中，存储器 502 可以用于存储电子设备 500 出厂时预装的程序/代码，也可以存储用于处理器 501 执行时的代码等。

基于相同构思，本申请提供一种电子设备，可用于执行上述终端侧的方法流程。图 6 为本申请提供的另一种电子设备的结构示意图。该电子设备包括处理器 601、存储器 602、收发器 603 和通信接口 604；其中，处理器 601、存储器 602、收发器 603 和通信接口 604 之间通过总线 605 相互连接。

总线 605 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 6 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 602 可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，简称 RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，简称 HDD）或固态硬盘（solid-state drive，简称 SSD）；存储器 602 还可以包括上述种类的存储器的组合。

通信接口 604 可以为有线通信接入口，无线通信接口或其组合，其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为 WLAN 接口。

处理器 601 可以是中央处理器（central processing unit，简称 CPU），网络处理器（network processor，简称 NP）或者 CPU 和 NP 的组合。

处理器 601 还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，简称 ASIC），可编程逻辑器件（programmable logic device，简称 PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device，简称 CPLD），现场可编程逻辑门阵列（field-programmable gate array，简称 FPGA），通用阵列逻辑（generic array logic，简称 GAL）或其任意组合。

所述处理器 601，用于使用当前主密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥替换当前主密钥。

所述存储器 602，用于存储一个或多个可执行程序，可以存储所述处理器 601 在执行操作时所使用的数据。

所述收发器 603，用于向后台系统发送更新主密钥请求；发送终端的当前标识；其中，更新主密钥请求中包括终端的待更新标识；接收后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，当前主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的当前标识对应的主密钥；

待更新主密钥为后台系统根据预设的终端的标识和主密钥的对应关系确定出的待更新标识对应的主密钥。

可选地，所述收发器，还用于：向后台系统发送初始化主密钥请求；发送终端的原始标识；接收后台系统发送的使用公钥加密后的第一密钥；接收后台系统发送的使用第一密钥加密后的初始化主密钥；其中，初始化主密钥请求中包括终端的初始化标识和公钥；所述处理器，用于：使用私钥对加密后的第一密钥进行解密得到第一密钥；使用第一密钥对加密后的初始化主密钥进行解密，得到初始化主密钥。

可选地，第一密钥为随机密钥。

可选地，初始化主密钥为后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的初始化标识对应的主密钥。

应理解，以上各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，发送单元 401 和接收单元 402 均可以由收发器 603 实现，处理单元 403 可以由处理器 601 实现。如图 6 所示，电子设备 600 可以包括处理器 601、存储器 602 和收发器 603。其中，存储器 602 可以用于存储处理器 601 执行方案时的代码，该代码可为电子设备 600 出厂时预装的程序/代码。

从上述内容可以看出：本发明实施例中，由于本发明实施例中后台系统根据终端的发送的更新主密钥请求，对终端的主密钥进行更新，从而实现了远程更新终端主主密钥，使更新主密钥快捷、方便；而且，在更新过程中后台系统使用当前主密钥对待更新主密钥进行加密，防止后台系统在向服务器发送终端主密钥时时待更新主密钥被泄露，提高了更新终端主密钥的安全性；

而且，由于当前终端主密钥和待更新终端主密钥都是密文，即使被窃取，页无法获得真实的终端主密钥，无法进行窃取或破坏，进一步提高了更新终端主密钥的安全性。

本领域内的技术人员应明白，本发明的实施例可提供为方法、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包括有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权

利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包括这些改动和变型在内。

权 利 要 求

1、一种终端主密钥的设置方法，其特征在于，包括:

后台系统接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识;

所述后台系统根据预设的终端的标识和主密钥的对应关系，确定出所述终端的待更新标识对应的待更新主密钥，以及所述当前标识对应的当前主密钥;

所述后台系统使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给所述终端；其中，所述加密后的待更新主密钥用于使所述终端使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥写入所述终端。

2、如权利要求 1 所述的方法，其特征在于，所述后台系统接收终端发送的更新主密钥请求之前，还包括:

所述后台系统接收终端发送的初始化主密钥请求；接收所述终端发送的所述终端的原始标识；其中，所述初始化主密钥请求中包括所述终端的初始化标识和公钥;

所述后台系统根据所述预设的终端的标识和主密钥的对应关系，确定出所述终端的所述初始化标识对应的初始化主密钥;

所述后台系统产生第一密钥;

所述后台系统使用公钥对所述第一密钥进行加密，将得到的加密后的第一密钥发送给所述终端;

所述后台系统使用所述第一密钥对所述初始化主密钥进行加密，将得到加密后的初始化主密钥发送给所述终端;

其中，所述加密后的初始化主密钥用于使所述终端使用私钥对加密后的第一密钥进行解密得到所述第一密钥后，使用所述第一密钥对加密后的初始化主密钥进行解密，得到所述初始化主密钥。

3、如权利要求 2 所述的方法，其特征在于，所述第一密钥为随机密钥。

4、如权利要求 2 所述的方法，其特征在于，所述后台系统接收终端发送的初始化主密钥请求之后，根据预设的终端的标识和主密钥的对应关系确定出所述终端的所述初始化标识对应的初始化主密钥之前，还包括:

所述后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在所述终端的原始标识对应的生产商预置标识。

5、一种终端主密钥的设置方法，其特征在于，包括:

终端向后台系统发送更新主密钥请求; 发送所述终端的当前标识; 其中，所述更新主密钥请求中包括所述终端的待更新标识;

所述终端接收所述后台系统发送的使用当前主密钥加密后的待更新主密钥; 其中，所述当前主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述当前标识对应的主密钥; 所述待更新主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述待更新标识对应的主密钥;

所述终端使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥替换所述当前主密钥。

6、如权利要求 5 所述的方法，其特征在于，所述终端向后台系统发送更新主密钥请求后台系统之前，还包括:

终端向所述后台系统发送初始化主密钥请求; 发送所述终端的原始标识; 其中，所述初始化主密钥请求中包括所述终端的初始化标识和公钥;

所述终端接收所述后台系统发送的使用所述公钥加密后的第一密钥; 所述终端接收所述后台系统发送的使用所述第一密钥加密后的所述初始化主密钥;

所述终端使用私钥对加密后的第一密钥进行解密得到所述第一密钥;

所述终端使用所述第一密钥对加密后的初始化主密钥进行解密，得到所述初始化主密钥。

7、如权利要求 5 所述的方法，其特征在于，所述第一密钥为随机密钥。

8、如权利要求 5 所述的方法，其特征在于，所述初始化主密钥为所述后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在所述终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的所述初始化标识对应的主密钥。

9、一种电子设备，其特征在于，包括处理器、存储器、收发器、通信接口，其中处理器、存储器与收发器之间通过总线连接;

所述处理器，用于读取所述存储器中的程序，执行下列方法：根据预设的终端的标识和主密钥的对应关系，确定出所述终端的待更新标识对应的待更新主密钥，以及所述当前标识对应的当前主密钥；使用当前主密钥对待更新主密钥进行加密，将得到加密后的待更新主密钥发送给所述终端；其中，所述加密后的待更新主密钥用于使所述终端使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥写入所述终端;

所述收发器，用于接收终端发送的更新主密钥请求；接收所述终端发送的所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识;

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据。

10、如权利要求 9 所述的电子设备，其特征在于，所述收发器，还用于:

接收终端发送的初始化主密钥请求；接收所述终端发送的所述终端的原始标识；其中，所述初始化主密钥请求中包括所述终端的初始化标识和公钥;

所述处理器，用于:

根据所述预设的终端的标识和主密钥的对应关系，确定出所述终端的所述初始化标识对应的初始化主密钥；产生第一密钥；使用公钥对所述第一密钥进行加密，将得到的加密后的第一密钥发送给所述终端；使用所述第一密钥对所述初始化主密钥进行加密，将得到加密后的初始化主密钥发送给所述终端；其中，所述加密后的初始化主密钥用于使所述终端使用私钥对加密后

的第一密钥进行解密得到所述第一密钥后，使用所述第一密钥对加密后的初始化主密钥进行解密，得到所述初始化主密钥。

11、如权利要求 9 所述的电子设备，其特征在于，所述第一密钥为随机密钥。

12、如权利要求 9~11 所述的电子设备，其特征在于，所述处理器，还用于：根据预设的终端标识和生产商预置标识的对应关系，确定存在所述终端的原始标识对应的生产商预置标识。

13、一种电子设备，其特征在于，包括：处理器、存储器、收发器和通信接口，其中，处理器、存储器、收发器和通信接口之间通过总线连接；

所述收发器，用于向后台系统发送更新主密钥请求；发送所述终端的当前标识；其中，所述更新主密钥请求中包括所述终端的待更新标识；

接收所述后台系统发送的使用当前主密钥加密后的待更新主密钥；其中，所述当前主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述当前标识对应的主密钥；所述待更新主密钥为所述后台系统根据预设的终端的标识和主密钥的对应关系确定出的所述待更新标识对应的主密钥；

所述处理器，用于使用所述当前主密钥对所述加密后的待更新主密钥进行解密，得到所述待更新主密钥，并将所述待更新主密钥替换所述当前主密钥。

14、如权利要求 13 所述的电子设备，其特征在于，所述收发器，还用于：

向所述后台系统发送初始化主密钥请求；发送所述终端的原始标识；其中，所述初始化主密钥请求中包括所述终端的初始化标识和公钥；

接收所述后台系统发送的使用所述公钥加密后的第一密钥；接收所述后台系统发送的使用所述第一密钥加密后的所述初始化主密钥；

所述处理器，用于：

使用私钥对加密后的第一密钥进行解密得到所述第一密钥；使用所述第一密钥对加密后的初始化主密钥进行解密，得到所述初始化主密钥。

15、如权利要求 13 所述的电子设备，其特征在于，所述第一密钥为随机密钥。

16、如权利要求 13 所述的电子设备，其特征在于，所述初始化主密钥为所述后台系统根据预设的终端标识和生产商预置标识的对应关系，确定存在所述终端的原始标识对应的生产商预置标识的情况下，根据预设的终端的标识和主密钥的对应关系确定出的所述初始化标识对应的主密钥。

17、一种非暂态计算机可读存储介质，其特征在于，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行权利要求 1~4 任一所述方法，或者所述计算机指令用于使所述计算机执行权利要求 5~8 任一所述方法。

18、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行权利要求 1~4 任一所述方法；或者使所述计算机执行权利要求 5~8 任一所述方法。

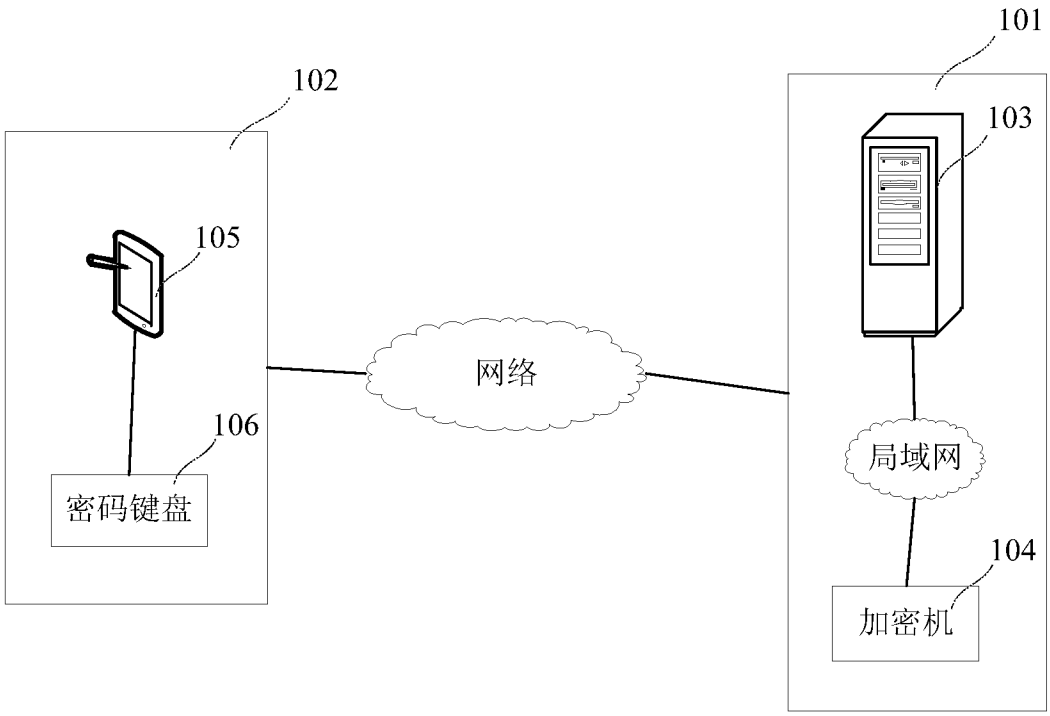

图 1

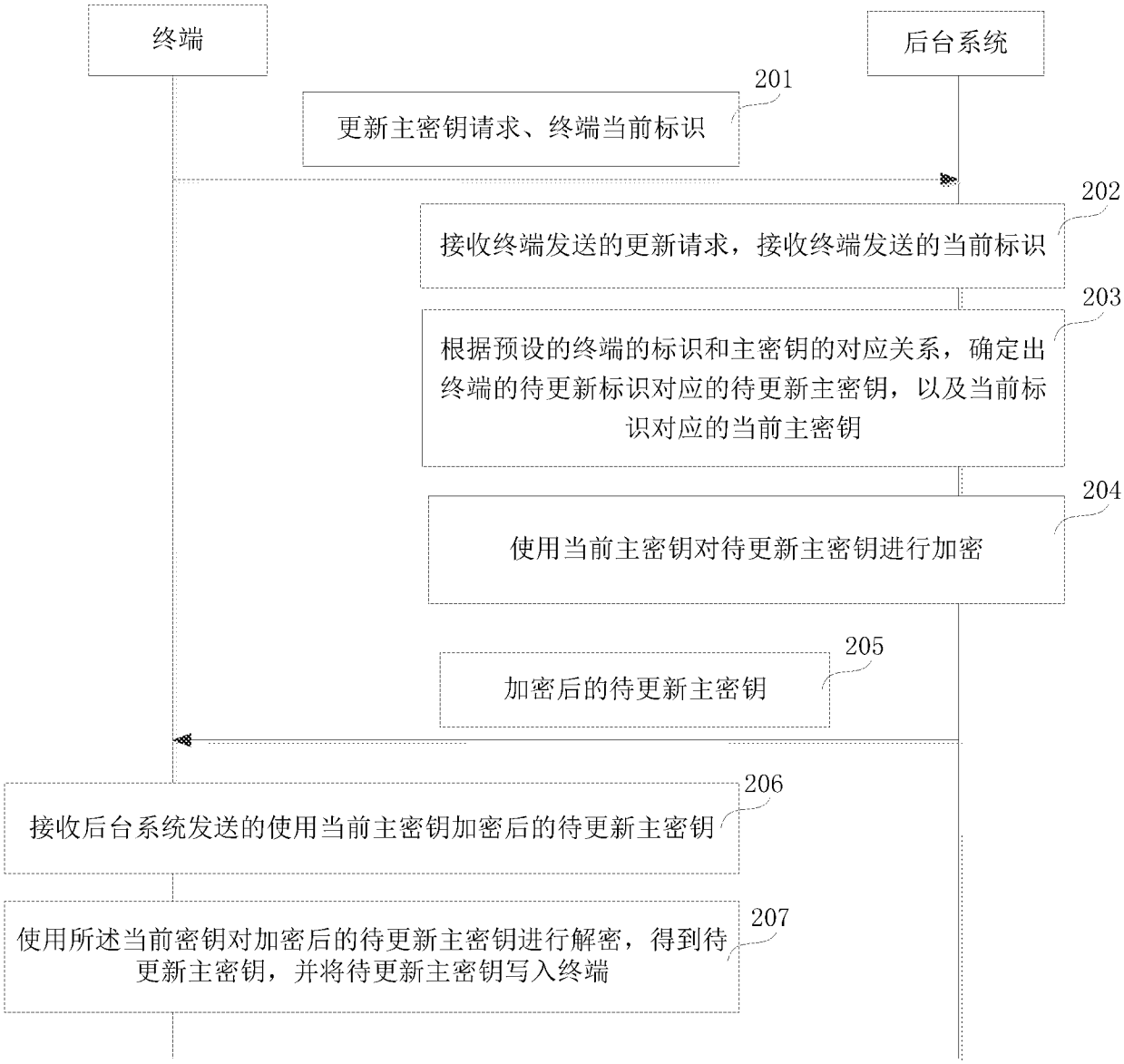
终端
后台系统
201
更新主密钥请求、终端当前标识
202
接收终端发送的更新请求，接收终端发送的当前标识
203
根据预设的终端的标识和主密钥的对应关系，确定出终端的待更新标识对应的待更新主密钥，以及当前标识对应的当前主密钥
204
使用当前主密钥对待更新主密钥进行加密
205
加密后的待更新主密钥
206
接收后台系统发送的使用当前主密钥加密后的待更新主密钥
207
使用所述当前密钥对加密后的待更新主密钥进行解密，得到待更新主密钥，并将待更新主密钥写入终端

图 2

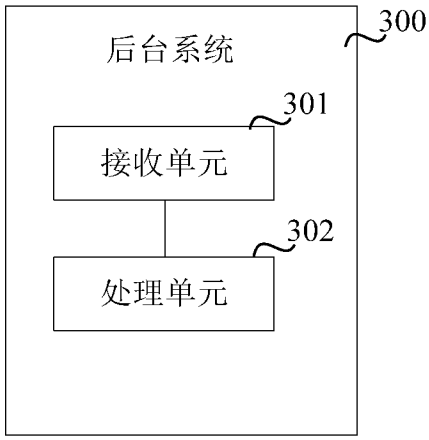

图 3

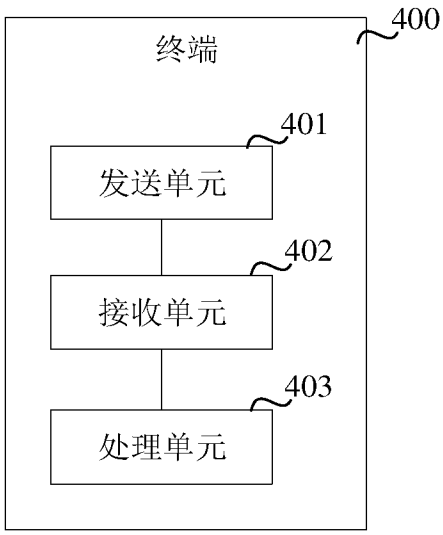

图 4

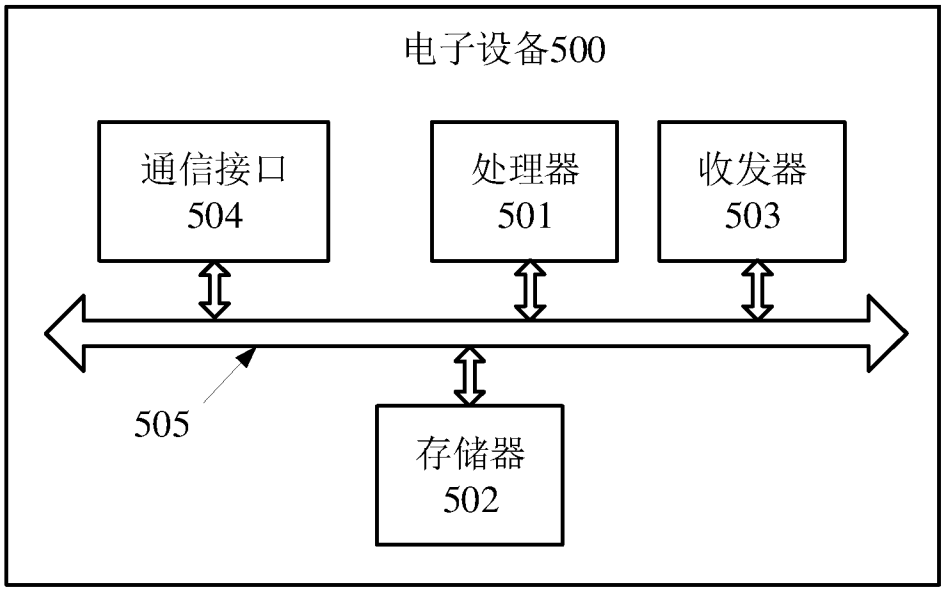
电子设备500
通信接口
504
处理器
501
收发器
503
505
存储器
502

图 5

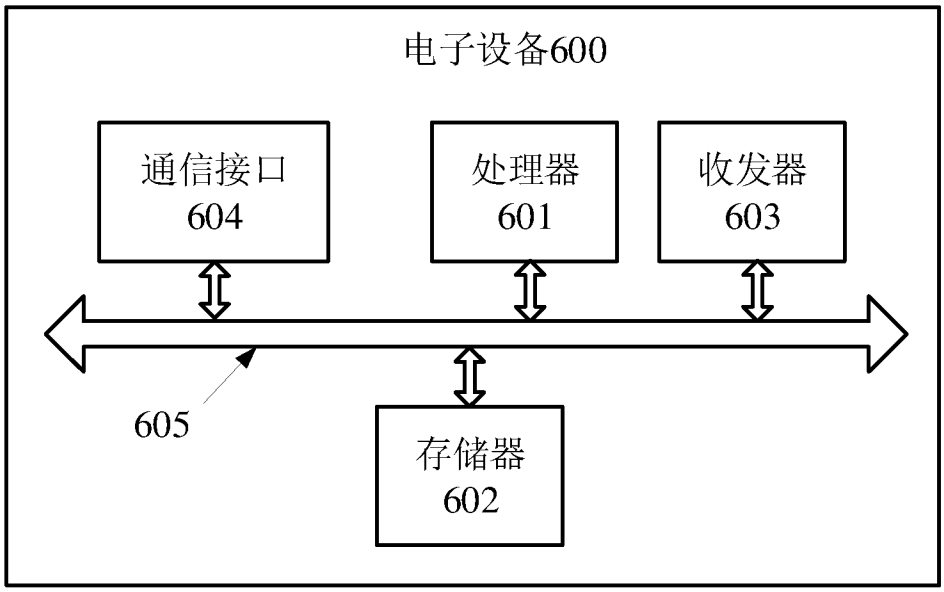
电子设备600
通信接口
604
处理器
601
收发器
603
605
存储器
602

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/105732

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, GOOGLE, CNPAT, CNKI: 密钥, 更新, 当前, 标识, 识别, 加密, 解密, 初始化, 随机, 终端, 远程, key, updat+, current+, identif+, encrypt+, decrypt+, initializat+, random, device?, terminal?, remote, long, distance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106571915 A (CHINA UNIONPAY CO., LTD.), 19 April 2017 (19.04.2017), claims 1-16, and description, paragraphs [0074]-[0098]	1-18
A	CN 104954123 A (CHINA UNIONPAY CO., LTD.), 30 September 2015 (30.09.2015), claims 1-12, figure 1, and description, paragraphs [0027]-[0036]	1-18
A	CN 105743654 A (DYNAMICODE COMPANY LIMITED), 06 July 2016 (06.07.2016), entire document	1-18
A	CN 101370248 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 18 February 2009 (18.02.2009), entire document	1-18
A	CN 102118385 A (WATCHDATA SYSTEM CO., LTD.), 06 July 2011 (06.07.2011), entire document	1-18
A	US 2003219129 A1 (WHELM, R. et al.), 27 November 2003 (27.11.2003), entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 December 2017	28 December 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer JIA, Yu Telephone No. (86-10) 61648539

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/105732

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106571915 A	19 April 2017	None	
CN 104954123 A	30 September 2015	None	
CN 105743654 A	06 July 2016	None	
CN 101370248 A	18 February 2009	None	
CN 102118385 A	06 July 2011	None	
US 2003219129 A1	27 November 2003	US 2006078124 A1	13 April 2006
		WO 03100561 A2	04 December 2003
		EP 1512244 A2	09 March 2005
		AU 2003241543 A1	12 December 2003

国际检索报告

国际申请号 PCT/CN2017/105732

A. 主题的分类

H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,EPODOC,GOOGLE,CNPAT,CNKI：密钥，更新，当前，标识，识别，加密，解密，初始化，随机，终端，远程，key，updat+，current+，identif+，encrypt+，decrypt+，initializat+，random，device?，terminal?，remote，long，distance

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 106571915 A (中国银联股份有限公司) 2017年 4月 19日 (2017-04-19) 权利要求1-16，说明书第[0074]-[0098]段	1-18
A	CN 104954123 A (中国银联股份有限公司) 2015年 9月 30日 (2015-09-30) 权利要求1-12，附图1，说明书第[0027]-[0036]段	1-18
A	CN 105743654 A (上海动联信息技术股份有限公司) 2016年 7月 6日 (2016-07-06) 全文	1-18
A	CN 101370248 A (中国移动通信集团公司) 2009年 2月 18日 (2009-02-18) 全文	1-18
A	CN 102118385 A (北京握奇数据系统有限公司) 2011年 7月 6日 (2011-07-06) 全文	1-18
A	US 2003219129 A1 (WHELAN, ROBERT 等) 2003年 11月 27日 (2003-11-27) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 12月 13日	2017年 12月 28日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 加玉 电话号码 (86-10)61648539

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/105732

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	106571915	A	2017年 4月 19日	无			
CN	104954123	A	2015年 9月 30日	无			
CN	105743654	A	2016年 7月 6日	无			
CN	101370248	A	2009年 2月 18日	无			
CN	102118385	A	2011年 7月 6日	无			
US	2003219129	A1	2003年 11月 27日	US	2006078124	A1	2006年 4月 13日
				WO	03100561	A2	2003年 12月 4日
				EP	1512244	A2	2005年 3月 9日
				AU	2003241543	A1	2003年 12月 12日