(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
2025 年 6 月 5 日 (05.06.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/112698 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01) *H04W 12/00* (2021.01)

(21) 国际申请号: PCT/CN2024/113795

(22) 国际申请日: 2024 年 8 月 21 日 (21.08.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311620399.9 2023年11月29日 (29.11.2023) CN

(71) 申请人: 中移物联网有限公司 (**CHINA MOBILE IOT COMPANY LIMITED**) [CN/CN]; 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 中国移动通信集团有限公司 (**CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.**) [CN/CN]; 中国北京市西城区金融大街29号 100032 (CN)。

(72) 发明人: 王鹏 (**WANG, Peng**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 林紫微 (**LIN, Ziwei**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 唐伟 (**TANG, Wei**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 曾云凤 (**ZENG, Yunfeng**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 施明瑞 (**SHI, Mingrui**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 张雄威 (**ZHANG, Xiongwei**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。 周豪 (**ZHOU, Hao**); 中国重庆市南岸区茶园新区玉马路8号 401336 (CN)。

(74) 代理人: 北京清亦华知识产权代理事务所（普通合伙） (**TSINGYIHUA INTELLECTUAL**

(54) **Title:** SECURITY MODULE, SECURE COMMUNICATION SYSTEM AND METHOD, STORAGE MEDIUM, AND PROGRAM PRODUCT

(54) 发明名称: 安全模组、安全通信系统及方法、存储介质和程序产品

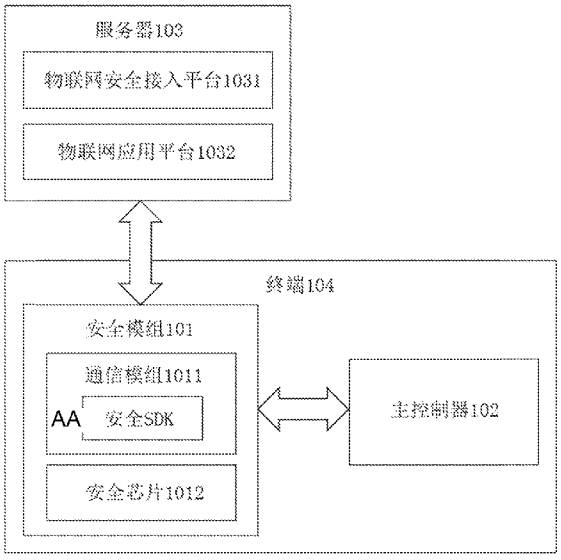

图 1

101 Security module
102 Main controller
103 Server
104 Terminal
1011 Communication module
1012 Security chip
1031 Internet of Things secure access platform
1032 Internet of Things application platform
AA Security SDK

(57) **Abstract:** The present disclosure provides a security module, a secure communication system and method, a storage medium, and a program product. The security module in the present disclosure comprises a communication module and a security chip. In a terminal device, the communication module performs encrypted data transmission with other modules in the terminal on the basis of a first encryption protocol. During external communication, the security chip performs encrypted data transmission with a device such as an external server on the basis of a security chip encryption protocol. According to the present solution, secure communication under multiple encryption methods is achieved by applying a security encryption function of a security chip and a customized encryption algorithm between modules in a terminal, thereby avoiding the risk of leakage of data during transmission between the modules in the terminal device while guaranteeing security of data transmission between the terminal and the external server.

WO 2025/112698 A1

[见续页]

PROPERTY LLC); 中国北京市海淀区悦秀路99号4层2单元417 100085 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, 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: 本公开提供了一种安全模组、安全通信系统及方法、存储介质和程序产品。本公开中的安全模组包括通信模组和安全芯片，在终端设备内部，该通信模组基于第一加密协议，与终端内的其他模组进行加密数据传输，在外部通信过程中，该安全芯片基于安全芯片加密协议与外部服务器等设备进行加密数据传输。在本方案中，通过应用安全芯片的安全加密功能，终端内部各模组之间的的自定义加密算法，实现多重加密方法下的安全通信，在保障终端和外部服务器之间数据传输安全性的同时，也避免了数据在终端设备内部模组之间传输过程中被泄露的风险。

安全模组、安全通信系统及方法、存储介质和程序产品

相关申请的交叉引用

本公开基于申请号为202311620399.9、申请日为2023年11月29日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本公开作为参考。

技术领域

本公开属于通信技术领域，尤其涉及一种安全模组、安全通信系统及方法、存储介质和程序产品。

背景技术

随着终端通信技术、物联网技术的快速发展，设备间的通信量大幅增长，也对通信安全提出了更高要求。目前的通信技术大多通过部署安全服务，来确保不同终端设备之间、终端设备与服务器之间的通信安全，但是在各个终端设备内部，缺少相应的安全机制，因为数据在终端设备内的各个模组之间传输时，存在泄漏风险，所以无法全面保障通信系统的数据安全。

发明内容

本公开实施例提供一种安全模组、安全通信系统及方法、存储介质和程序产品，能够实现多重加密方法下的安全通信，在保障终端设备和外部服务器之间数据传输安全性的同时，也避免了数据在终端设备内部的各个模组之间传输过程中被泄露的风险。

在第一方面，本公开实施例提供一种安全模组，该安全模组包括通信模组和安全芯片；该通信模组，用于基于第一加密协议进行数据加密或数据解密，其中该第一加密协议是该安全模组所在的终端内部的数据传输加密协议；该安全芯片，用于基于安全芯片加密协议进行数据加密或数据解密，其中该安全芯片加密协议是该安全模组所在的终端与外部设备之间的数据传输加密协议。

在第二方面，本公开实施例提供了一种安全通信系统，该安全通信系统包括上述第一方面提供的安全模组，以及主控制器、服务器；该安全模组与该主控制器部署在同一终端；该安全模组与该主控制器之间基于第一加密协议进行加密数据传输；该安全模组与该服务器之间基于安全芯片加密协议进行加密数据传输；该主控制器与该服务器之间基于第二加密协议进行数据传输。

在第三方面，本公开实施例提供了一种安全通信方法，该方法应用上述第二方面提供的安全通信系统，该方法包括：由该主控制器基于该第一加密协议进行数据加密，得到第一加密数据；由该主控制器将该第一加密数据发送至该安全模组中的该通信模组；以及由该通信模组接收该第一加密数据，基于该第一加密协议对该第一加密数据进行解密。

在第四方面，本公开实施例提供了一种计算机存储介质，其上存储有指令，所述指令被处理器执行时实现如上述第三方面所述的方法。

在第四方面，本公开实施例提供了一种包括指令的计算机程序产品，所述指令被处理器执行时，使得所述处理器执行如上述第三方面所述的方法。

本公开实施例提供了一种安全模组、安全通信系统及方法，所述安全模组包括通信模组和安全芯片，在终端设备内部，该通信模组基于第一加密协议，与终端内的其他模组进行加密数据传输，在外部通信过程中，该安全芯片基于安全芯片加密协议与外部服务器等设备进行加密数据传输。在本方案中，通过应用安全芯片的安全加密功能，终端内部各模组之间的的自定义加密算法，实现多重加密方法下的安全通信，在保障终端和外部服务器之间数据传输安全性的同时，也避免了数据在终端设备内部模组之间传输过程中被泄露的风险。

附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对本公开实施例中所需要使用的附图作简单的介绍，对于本领域普通技术人员来讲，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是本公开实施例提供的一种安全通信系统的示意图。

图2是本公开实施例提供的一种主控制器与安全模组之间的数据交互示意图。

图3是本公开实施例提供的一种安全模组与服务器之间的数据交互示意图。

图4是本公开实施例提供的一种主控制器与服务器之间的数据交互示意图。

图5是本公开实施例提供的另一种主控制器与服务器之间的数据交互示意图。

图6是本公开实施例提供的一种升级第一加密协议的流程图。

图7是本公开实施例提供的一种升级第二加密协议的流程图。

图 8 是本公开实施例提供的一种计算机设备的结构示意图。

具体实施方式

下面将详细描述本公开的各个方面的特征和示例性实施例，为了使本公开的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本公开进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本公开，而不是限定本公开。对于本领域技术人员来说，本公开可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本公开的示例来提供对本公开更好的理解。

需要说明的是，在本文中，诸如第一和第二等等术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

为了解决现有技术问题，本公开实施例提供了一种安全模组、安全通信系统及方法。下面结合附图进行详细说明。图 1 是本公开实施例提供的一种安全通信系统的示意图。如图 1 所示，该安全通信系统包括安全模组 101、主控制器 102 和服务器 103。在一个实施例中，该安全模组 101 与该主控制器 102 部署在同一终端 104，也即是，该安全模组与该主控制器是同一终端内部的不同硬件模块。该终端 104 可以是智能手机、平板电脑、便携型计算机、台式计算机等，本公开实施例对此不做限定。

在一个实施例中，该安全模组 101 属于终端 104 的通信单元。示例性的，该安全模组 101 外观上与传统通信模组一致，是具有安全加密能力和网络通信能力的通信模组，用于实现终端 104 与服务器 103 之间的通信。在一个实施例中，该安全模组 101 包括通信模组 1011 和安全芯片 1012，该通信模组 1011 与安全芯片 1012 之间可以进行数据交互。示例性的，该通信模组 1011 和安全芯片 1012 可以通过物理接口连接，该物理接口可以是串口、I2C、SPI 等接口，本公开实施例对此不做限定。可选地，该通信模组 1011 上可以集成有与安全芯片 1012 适配的安全软件开发工具包（Software Development Kit，SDK），调用该安全 SDK 提供的 API 接口能够驱动安全芯片 1012 提供安全通信服务。

在一个实施例中，该主控制器 102 是终端设备的控制单元，该主控制器 102 可以通过安全模组 101 与服务器 103 进行数据交互。在一个实施例中，该主控制器 102 属于终端 104 的控制单元，可以用于接收安全模组 101 发送的控制指令，并完成该控制指令所指示的操作以及回复操作结果。在一个实施例中，该主控制器 102 可以实现为单片机 MCU（Microcontroller Unit，微控单元），本公开实施例对此不做限定。

在一个实施例中，服务器 103 部署在云端，该服务器 103 可以是一台服务器、多台服务器、云计算平台等，本公开实施例对服务器 103 的设备类型不做限定。该服务器 103 可以通过无线网络或有线网络与终端 104 相连，实现对终端 104 的通信和控制。在一个实施例中，服务器 103 可以向安全模组 101 中的通信模组 1011 和主控制器 1012 提供远程升级服务，安全模组 101 中的通信模组 1011 和主控制器 1012 支持远程升级功能。

在一个实施例中，该服务器 103 包括物联网安全接入平台 1031 和物联网应用平台 1032。示例性的，该物联网安全接入平台 1031 可以和终端 104 进行通信，可以对传输的数据进行加密、解密和数据签名等操作。该物联网应用平台 1032 可以提供设备接入、数据采集、数据处理、应用管理等功能。

下面结合附图对上述安全通信系统中终端内部的各硬件之间的通信流程进行详细说明。在本公开实施例中，安全模组与主控制器之间可以基于第一加密协议进行加密数据传输。其中，该第一加密协议是该安全模组所在的终端内部的数据传输加密协议。示例性的，在本公开实施例中，该第一加密协议可以是安全模组和主控制器之间的自定义加密协议，该主控制器和该安全模组中的通信模组均可以基于第一加密协议进行数据加密或数据解密。图 2 是本公开实施例提供的一种主控制器与安全模组之间的数据交互示意图。如图 2 中的图（a）所示，在一个实施例中，该主控制器可以基于该第一加密协议进行数据加密，得到第一加密数据，再将该第一加密数据发送至该安全模组中的通信模组。也即是，执行步骤 201，发送基于第一加密协议加密后的数据。在该通信模组接收该第一加密数据之后，基于该第一加密协议对该第一加密数据进行解密，得到该主控制器发送的原始数据。在这一场景中，仅调用安全模组中的通信模组，由该主控制器和通信模组分别提供数据加密或解密功能，无需调用安全芯片，该主控制器与该安全模组中的通信模组之间可以直接传输加密数据。在一个实施例中，该通信模组也可以执行步骤 202，向主控制器发送基于第一加密协议加密后的数据，主控制器基于第一加密协议对收到的数据进行解密。需要说明的是，本公开实施例中，对步骤 201 和步骤 202 的执行顺序不做限定。在本公开实施例中，通过该第一加密协议对主控制器和安全模组之间的数据传输进行加密，能够避免出现终端内部数据泄密的情况。

在本公开实施例中，终端内的各个模组之间也可以传输未加密的明文数据。如图 2 中的图（b）所示，在一个实施例中，该主控制器与安全模组之间可以传输未加密的明文数据。示例性的，主控制器可以执行步骤 203，向通信模组发送未加密的明文数据，通信模组可以执行步骤 204，向主控制器发送未加密的明文数据。本公开实施例中，对步骤 203 和步骤 204 的执行顺序不做限定。在这一场景中，仅需调用安全模组中的通信模组，无需安全芯片进行数据加密，该主控制器与该安全模组中的通信模组之间直接传输未加密的明文数据。

在一个实施例中，主控制器发给安全模组的数据可以携带有第一数据接收方标识、第一加密标识中的至少一项。其中，该第一数据接收方标识用于指示数据接收设备，例如，该第一数据接收方标识可以是安全模组的标识或服务器的标识。安全模组接收到主控制器发送的数据后，可以基于该第一数据接收方标识判断接收到的数据是由该安全模组进行数据处理还是转发给服务器。在一个实施例中，这一判断过程可以由安全模组中的通信模组执行。该第一加密标识用于指示数据是否采用第一加密协议进行加密，安全模组可以基于该第一加密标识，判断是否需要基于第一加密协议对接收到的数据进行解密。例如，在本公开实施例中，该通信模组接收第一加密数据后，响应于该第一加密数据携带该第一加密标识，执行基于该第一加密协议对该第一加密数据进行解密的步骤。该主控制器发送的数据还可以携带其他信息，本公开实施例对此不做限定。在一个实施例中，该主控制器发送的数据所携带的信息可以是未加密的明文数据，也可以是采用第一加密协议加密后的数据，本公开实施例对此不做限定。

下面结合附图对上述安全通信系统中各个设备之间的通信流程进行详细说明。在本公开实施例中，该安全模组与服务器之间可以基于安全芯片加密协议进行加密数据传输。其中，该安全芯片加密协议是安全模组所在的终端与外部设备之间的数据传输加密协议。示例性的，该安全芯片加密协议可以由物联网安全厂家提供，集成在安全芯片和物联网安全接入平台中，该安全模组中的安全芯片和服务器中的物联网安全接入平台均可以基于该安全芯片加密协议进行数据加密或数据解密。也即是，终端侧由安全芯片提供数据加密和数据解密功能，服务器侧由物联网安全接入平台提供数据加密和数据解密功能。在一个实施例中，由于该安全芯片加密协议、设备和服务均由物联网安全厂家提供，其他用户不可修改其内容，在该安全通信系统运行后，安全芯片加密协议不支持更改。

图 3 是本公开实施例提供的一种安全模组与服务器之间的数据交互示意图。如图 3 所示，在一个实施例中，该安全模组和服务器之间可以基于安全芯片加密协议进行加密数据传输。示例性的，该安全模组中的通信模组可以执行步骤 301，调用内部集成的安全 SDK 的 API 接口，将待加密的数据发送至安全芯片。该安全芯片执行步骤 302，基于该安全芯片加密协议对待加密的数据进行加密，将加密后的数据发送至通信模组。该通信模组执行步骤 303，将加密后的数据发送至服务器中的物联网安全接入平台。该物联网安全接入平台执行步骤 304，基于安全芯片加密协议进行数据解密，将解密后的数据发送至物联网应用平台。该服务器向安全模组发送加密数据的过程同理。示例性的，该服务器中的物联网应用平台执行步骤 305，将待加密的数据发送至物联网安全接入平台。该物联网安全接入平台执行步骤 306，基于该安全芯片加密协议对待加密的数据进行加密，将加密后的数据发送至该安全模组中的通信模组。该通信模组执行步骤 307，将该加密后的数据发送至安全芯片。由该安全芯片执行步骤 308，基于安全芯片加密协议进行数据解密，将解密后的数据发回至该通信模组。在本公开实施例中，通过应用安全芯片加密协议，能够提高终端中安全模组与服务器之间数据传输的安全性。

在本公开实施例中，主控制器可以通过安全模组与服务器进行加密数据传输。在一个实施例中，主控制器可以将未加密的明文数据发送给安全模组，由安全模组基于安全芯片加密协议加密后转发至服务器。图 4 是本公开实施例提供的一种主控制器与服务器之间的数据交互示意图。如图 4 所示，主控制器执行步骤 401，将未加密的明文数据发送给安全模组中的通信模组。该通信模组执行步骤 402，调用内部集成的安全 SDK 的 API 接口，将主控制器发送的数据转发给安全芯片。由安全芯片执行步骤 403，基于安全芯片加密协议进行数据加密，并将加密后的数据发回至通信模组。该通信模组执行步骤 404 将加密后的数据发送给服务器中的物联网安全接入平台。该物联网安全接入平台执行步骤 405，基于安全芯片加密协议进行数据解密，得到该主控器发送的明文数据，并将解密后得到的该明文数据发送给物联网应用平台。该服务器向主控制器发送数据的过程同理。示例性的，物联网应用平台执行步骤 406 将未加密的明文数据发送至物联网安全接入平台。由该物联网安全接入平台执行步骤 407 应用安全芯片加密协议进行数据加密，并将加密后的数据发送个安全模组中的通信模组。该通信模组执行步骤 408 将接收到的加密后的数据转发给安全芯片。由该安全芯片执行步骤 409 基于安全芯片加密协议进行数据解密，并将解密后的数据发回至通信模组。再由通信模组将解密后的数据转发给主控制器。在本公开实施例中，主控制器与服务器进行通信过程中，通过安全模组进行转发和数据加密，能够确保设备间通信的安全性。

在一个实施例中，该主控制器与该服务器之间可以基于第二加密协议进行加密数据传输，也即是主控制器与服务器之间可以传输对安全模组保密的数据。其中，该第二加密协议是主控制器与物联网应用平台之间的自定义加密协议，主控制器和物联网应用平台均可以基于该第二加密协议进行数据加密或数

据解密。图 5 是本公开实施例提供的另一种主控制器与服务器之间的数据交互示意图。如图 5 所示，该主控制器执行步骤 501 基于第二加密协议进行数据加密，得到第二加密数据，将该第二加密数据发送至安全模组中的通信模组。该通信模组执行步骤 502，调用内部集成的安全 SDK 的 API 接口，发送待加密的数据，即该第二加密数据。该安全芯片执行步骤 503 接收通信模组转发的第二加密数据，基该安全芯片加密协议对该第二加密数据进行加密，得到第三加密数据。该通信模组在接收到该安全芯片发送的第三加密数据后，执行步骤 504 将该第三加密数据转发至该服务器。该服务器接收第三加密数据，基于该安全芯片协议和该第二加密协议对该第三加密数据进行解密。在一个实施例中，由该服务器中的物联网安全接入平台接收该第三加密数据，执行步骤 505 基于安全芯片加密协议对该第三加密数据进行解密，得到该第二加密数据，将解密出的第二加密数据转发至该物联网应用平台。该物联网应用平台执行步骤 506 接收该第二加密数据，基于第二加密协议对该第二加密数据进行解密，得到该主控制器发送的原始数据。该服务器向主控制器发送加密数据的过程同理。示例性的，该物联网应用平台执行步骤 507 基于第二加密协议对待发送的明文数据进行数据加密，得到加密后的中间数据，再执行步骤 508 将该中间数据发送至物联网安全接入平台。该物联网安全接入平台执行步骤 509 基于安全芯片加密协议对该中间数据进行加密，再执行步骤 510 将加密后的数据发送至通信模组。由通信模组转发给安全芯片进行解密。安全芯片执行步骤 511 基于安全芯片加密协议对接收到的数据进行解密，得到中间数据，将该中间数据发回至通信模组。该通信模组执行步骤 512 转发解密后的数据，即将该中间数据转发给主控制器。由主控制器执行步骤 513 基于第二加密协议进行数据解密，得到该物联网应用平台发送的原始的明文数据。

本公开实施例中，通过应用该第二加密协议，主控制器与服务器之间传输的数据对终端中的其他模块保密，能够保障数据在主控制器与物联网应用平台间之间传输的过程中不会被传输中间设备解析和窃取。示例性的，该传输中间设备可以是安全模组、物联网安全接入平台等。

在一个实施例中，上述安全模组与主控制器之间的通信可以通过 AT（Attention）指令实现，也可以通过用户自定义的协议和通道实现，本公开实施例对此不做限定。

在一个实施例中，服务器发送给安全模组的数据可以携带有第二数据接收方标识、第二加密标识中的至少一项。其中该第二数据接收方标识用于指示数据接收设备，例如，该第二数据接收方标识可以是安全模组的标识或主控制器的标识。在安全模组接收到接收到服务器发送的数据后，可以基于该第二数据接收方标识判断接收到的数据是由该安全模组进行数据处理还是转发给主控制器。可选地，这一判断过程可以由安全模组中的通信模组执行。该第二加密标识用于指示数据是否采用第二加密协议进行加密，主控制器可以基于该第二加密标识，判断是否需要基于第二加密协议对接收到的数据进行解密。例如在本公开实施例中，该主控制器接收到通信模组转发的该中间数据后，响应于该中间数据携带该第二加密标识，执行基于第二加密协议对该中间数据进行解密的步骤；响应于该中间数据不携带该第二加密标识，则将该中间数据作为服务器发送的原始的明文数据。当然，该服务器发送的数据还可以携带其他信息，本公开实施例对此不做限定。在一个实施例中，该服务器发送的数据所携带的信息可以是采用第二加密协议或安全芯片加密协议加密后数据，本公开实施例对此不做限定。

在一个实施例中，该第一加密协议和第二加密协议可以由开发人员进行设置。示例性的，该第一加密协议和第二加密协议均可以实现为“算法”+“key”的形式，该第一加密协议部署在通信模组所运行的软件中和主控制器所运行的软件中，该第二加密协议部署在主控制器所运行软件中和物联网应用平台上。在一个实施例中，该第一加密协议支持更改，例如，可以通过远程升级 OTA（Over-the-Air Technology，空中下载技术）的方式，分别对主控制器和安全模组中该第一加密协议相关的软件固件进行升级。在一个实施例中，该第二加密协议协议支持更改，例如，可以对物联网应用平台上该第二加密协议相关的软件固件进行升级。通过远程升级 OTA 的方式，对主控制器中该第二加密协议相关的软件固件进行升级。

下面结合附图对上述第一安全协议和第二安全协议的升级流程进行详细说明。在一个实施例中，该通信模组和主控制器可以用于对该第一加密协议的运行软件进行升级。图 6 是本公开实施例提供的一种升级第一加密协议的流程图。如图 6 所示，首先，可以由开发人员制作支持升级后的第一加密协议在主控制器上运行的第一软件固件升级包，以及支持升级后的第一加密协议在通信模组上运行的第二软件固件升级包，并将该第一软件固件升级包和第二软件固件升级包添加至服务器中的物联网应用平台，也即是执行步骤 601 的过程。然后，对主控制器中第一加密协议的运行软件进行升级。示例性的，该过程可以实现为，服务器执行步骤 602 发送第一升级指令给安全模组，然后通过安全模组将该第一升级指令转发给主控制器，该第一升级指令携带该第一软件固件升级包。该主控制器在接收到服务器发送的第一升级指令之后，执行步骤 603 基于该第一升级指令对该主控制器中第一加密协议的运行软件进行升级，即该主控制器可以通过对该第一软件固件升级包进行烧录来完成对第一加密协议的升级。该主控制器完成对第一加密协议的升级后，将升级后的第一加密协议的版本号、主控制器标识发送至服务器中的物联网应用平台。物联网应用平台执行步骤 604，接收并检测升级后的第一加密协议的版本号、主控制器标识的正确性。若升级后的第一加密协议的版本号、主控制器标识是正确的，则升级成功。若升级后的第一加

密协议的版本号、主控制器标识是不正确的，则升级失败。响应于升级失败，服务器重新下发该第一升级指令给主控制器，即重新执行上述步骤602。响应于升级成功，继续执行后续对通信模组中第一加密协议的运行软件进行升级的步骤。最后，对通信模组中第一加密协议的运行软件进行升级。示例性的，该过程可以实现为，服务器执行步骤605，发送第二升级指令给该安全模组中的通信模组，该第二升级指令携带该第二软件固件升级包。该通信模组在接收到该服务器发送的第二升级指令后，执行步骤606基于该第二升级指令对该通信模组中第一加密协议的运行软件进行升级，即该通信模组可以通过对该第二软件固件升级包进行烧录来完成对第一加密协议的升级。该通信模组完成对第一加密协议的升级后，将升级后的第一加密协议的版本号、主控制器标识发送至服务器中的物联网应用平台。物联网应用平台执行步骤607接收并检测升级后的第一加密协议的版本号、主控制器标识的正确性。若升级后的第一加密协议的版本号、主控制器标识是正确的，则升级成功。若升级后的第一加密协议的版本号、主控制器标识是不正确的，则升级失败。响应于升级失败，服务器重新下发该第二升级指令给通信模组，即重新执行上述步骤605。响应于升级成功，则确定第一加密协议升级完成。在本公开实施例中，通过对第一加密协议进行升级，确保数据加密效果，进一步提高数据在终端设备内部各个模组之间传输的安全性。

图7是本公开实施例提供的一种升级第二加密协议的流程图。如图7所示，首先，开发人员可以在服务器中的物联网应用平台集成、部署升级后的第二加密协议，即执行步骤701的过程，完成对服务器中第二加密协议的运行软件的升级。部署后该物联网应用平台支持基于升级后的第二加密协议进行数据加密和数据解密。开发人员还可以制作支持升级后的第二加密协议在主控制器上运行的第三软件固件升级包，并添加到服务器的物联网应用平台中，即执行步骤702的过程。然后，对主控制器中第二加密协议的运行软件进行升级。示例性的，该过程可以实现为，服务器执行步骤703发送第三升级指令给安全模组，然后通过安全模组将该第三升级指令转发给主控制器，该第三升级指令携带该第三软件固件升级包。该主控制器在执行步骤704接收到服务器发送的第三升级指令后，基于该第三升级指令对该主控制器中第二加密协议的运行软件进行升级，即该主控制器可以通过对该第三软件固件升级包进行烧录来完成对第二加密协议的升级。主控制器将升级后的第二加密协议的版本号、主控制器标识发送至服务器中的物联网应用平台。物联网应用平台执行步骤705接收并检测升级后的第二加密协议的版本号、主控制器标识的正确性。若升级后的第二加密协议的版本号、主控制器标识是正确的，则升级成功。若升级后的第二加密协议的版本号、主控制器标识是错误的，则升级失败。响应于升级失败，服务器重新下发该第三升级指令给主控制器，即重新执行步骤703。响应于升级成功，则确定第二加密协议升级完成。在本公开实施例中，通过对第二加密协议进行升级，确保数据加密效果，进一步提高数据在主控制器和服务器之间传输的安全性。

在一个实施例中，上述第一加密协议的版本号、第二加密协议的版本号可以用于进行软件版本的管理，升级前后版本号不同，可以用于判断加密协议的运行软件是否升级成功。上述通信模组标识、主控制器标识可以用于进行设备管理，标识可以为设备的IMEI（International Mobile Equipment Identity）号、SN（serial number）号、硬件版本号等。在本公开实施例中，对上述软件固件升级包的传输方式不做限定，例如，可以应用第二加密协议和安全芯片加密协议进行加密后传输，也可以仅应用安全芯片加密协议加密后进行传输。

本公开实施例中的安全模组包括通信模组和安全芯片，在终端设备内部，该通信模组基于第一加密协议，与终端内的其他模组进行加密数据传输，在外部通信过程中，该安全芯片基于安全芯片加密协议与外部服务器等设备进行加密数据传输。在本方案中，通过应用安全芯片的安全加密功能，终端内部各模组之间的的自定义加密算法，实现多重加密方法下的安全通信，在保障终端和外部服务器之间数据传输安全性的同时，也避免了数据在终端设备内部模组之间传输过程中被泄露的风险。

上述所有可选技术方案，可以采用任意结合形成本申请的可选实施例，在此不再一一赘述。

图8是本公开实施例提供的一种计算机设备的硬件结构示意图。在本公开实施例中，上述终端和服务器均可以视为一种计算机设备。

该计算机设备设备可以包括处理器801以及存储有计算机程序指令的存储器802。

具体地，上述处理器801可以包括中央处理器（Central Processing Unit，CPU），或者特定集成电路（Application Specific Integrated Circuit ，ASIC），或者可以被配置成实施本公开实施例的一个或多个集成电路。

存储器802可以包括用于数据或指令的大容量存储器。举例来说而非限制，存储器802可包括硬盘驱动器（Hard Disk Drive，HDD）、软盘驱动器、闪存、光盘、磁光盘、磁带或通用串行总线（Universal Serial Bus，USB）驱动器或者两个或更多个以上这些的组合。在一个实例中，存储器802可以包括可移除或不可移除(或固定)的介质，或者存储器802是非易失性固态存储器。存储器802可在计算设备的内部或外部。

在一个实例中，存储器802可以包括只读存储器（ROM），随机存取存储器（RAM），磁盘存储介质

设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本公开的一方面的方法所描述的操作。

处理器 801 通过读取并执行存储器 802 中存储的计算机程序指令，以实现图 2 至图 7 所示的安全通信方法。

在一个示例中，计算机设备还可包括通信接口 803 和总线 804。如图 8 所示，处理器 801、存储器 802、通信接口 803 通过总线 804 连接并完成相互间的通信。

通信接口 803，主要用于实现本公开实施例中各模块、装置、单元和/或设备之间的通信。

总线 804 包括硬件、软件或两者，将在线数据流量计费设备的部件彼此耦接在一起。举例来说而非限制，总线可包括加速图形端口（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Extended Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（Hyper Transport，HT）互连、工业标准架构（Industry Standard Architecture，ISA）总线、无限带宽互连、低引脚数（LPC）总线、存储器总线、微信道架构（MCA）总线、外围组件互连（PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（SATA）总线、视频电子标准协会局部（VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 304 可包括一个或多个总线。尽管本公开实施例描述和示出了特定的总线，但本公开考虑任何合适的总线或互连。

另外，结合上述实施例中的安全通信方法，本公开实施例可提供一种计算机存储介质来实现。该计算机存储介质上存储有计算机程序指令；该计算机程序指令被处理器执行时实现上述实施例中的任意一种安全通信方法。示例性的，该计算机存储介质可以是非暂时性计算机可读存储介质。

需要明确的是，本公开并不局限于上文所描述并在图中示出的特定配置和处理。为了简明起见，这里省略了对已知方法的详细描述。在上述实施例中，描述和示出了若干具体的步骤作为示例。但是，本公开的方法过程并不限于所描述和示出的具体步骤，本领域的技术人员可以在领会本公开的精神后，作出各种改变、修改和添加，或者改变步骤之间的顺序。

以上所述的结构框图中所示的功能块（模块）可以实现为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路（Application Specific Integrated Circuit，ASIC）、适当的固件、插件、功能卡等等。当以软件方式实现时，本公开的组件/元件是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、只读存储器（Read-Only Memory，ROM）、闪存、可擦除只读存储器（Erasable Read Only Memory，EROM）、软盘、只读光盘（Compact Disc Read-Only Memory，CD-ROM）、光盘、硬盘、光纤介质、射频（Radio Frequency，RF）链路，等等。代码段可以经由诸如因特网、内联网等的计算机网络被下载。

还需要说明的是，本公开中提及的示例性实施例，基于一系列的步骤或者装置描述一些方法或系统。但是，本公开不局限于上述步骤的顺序，也就是说，可以按照实施例中提及的顺序执行步骤，也可以不同于实施例中的顺序，或者若干步骤同时执行。

上面参考根据本公开的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本公开的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

以上所述，仅为本公开的具体实施方式，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。应理解，本公开的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本公开的保护范围之内。

权利要求书

1、一种安全模组，所述安全模组包括通信模组和安全芯片；

所述通信模组，用于基于第一加密协议进行数据加密或数据解密，其中所述第一加密协议是所述安全模组所在的终端内部的数据传输加密协议；

所述安全芯片，用于基于安全芯片加密协议进行数据加密或数据解密，其中所述安全芯片加密协议是所述安全模组所在的终端与外部设备之间的数据传输加密协议。

2、根据权利要求 1 所述的安全模组，其中，所述通信模组还用于对所述第一加密协议的运行软件进行升级。

3、一种安全通信系统，所述安全通信系统包括权利要求 1 或 2 所述的安全模组，以及主控制器、服务器；

所述安全模组与所述主控制器部署在同一终端；

所述安全模组与所述主控制器之间基于第一加密协议进行加密数据传输；

所述安全模组与所述服务器之间基于安全芯片加密协议进行加密数据传输；

所述主控制器与所述服务器之间基于第二加密协议进行数据传输。

4、根据权利要求 3 所述的安全通信系统，其中，所述主控制器用于基于所述第一加密协议进行数据加密，得到第一加密数据，以及将所述第一加密数据发送至所述安全模组中的所述通信模组；

所述通信模组，用于接收所述第一加密数据，以及基于所述第一加密协议对所述第一加密数据进行解密。

5、根据权利要求 3 所述的安全通信系统，其中，所述主控制器用于基于所述第二加密协议进行数据加密，得到第二加密数据，以及将所述第二加密数据转发至所述安全模组中的所述通信模组；

所述安全芯片，用于接收所述第二加密数据，以及基于所述安全芯片加密协议对所述第二加密数据进行加密，得到第三加密数据；

所述通信模组，用于接收所述安全芯片发送的所述第三加密数据，以及将所述第三加密数据转发至所述服务器；

所述服务器，用于接收所述第三加密数据，以及基于所述安全芯片协议和所述第二加密协议对所述第三加密数据进行解密。

6、根据权利要求 5 所述的安全通信系统，其中，所述服务器包括物联网安全接入平台和物联网应用平台；

所述物联网安全接入平台，用于接收所述第三加密数据，基于所述安全芯片加密协议对所述第三加密数据进行解密，得到所述第二加密数据，以及将所述第二加密数据转发至所述物联网应用平台；

所述物联网应用平台，用于接收所述第二加密数据，以及基于所述第二加密协议对所述第二加密数据进行解密。

7、根据权利要求 3 所述的安全通信系统，其中，所述主控制器还用于接收所述服务器发送的第一升级指令，基于所述第一升级指令对所述主控制器中第一加密协议的运行软件进行升级；

所述通信模组，还用于接收所述服务器发送的第二升级指令，以及基于所述第二升级指令对所述通信模组中第一加密协议的运行软件进行升级。

8、根据权利要求 3 所述的安全通信系统，其中，所述主控制器还用于接收所述服务器发送的第三升级指令，以及基于所述第三升级指令对所述主控制器中第二加密协议的运行软件进行升级。

9、一种安全通信方法，所述方法应用于权利要求 3-8 任一项所述的安全通信系统，所述方法包括：

由所述主控制器基于所述第一加密协议进行数据加密，得到第一加密数据；

由所述主控制器将所述第一加密数据发送至所述安全模组中的所述通信模组；以及

由所述通信模组接收所述第一加密数据，并基于所述第一加密协议对所述第一加密数据进行解密。

10、根据权利要求 9 所述的方法，其中，所述主控制器基于所述第一加密协议进行数据加密，得到第一加密数据之前，所述方法还包括：

由所述主控制器基于所述第二加密协议进行数据加密，得到第二加密数据，以及将所述第二加密数据发送至所述安全模组中的所述通信模组；

由所述安全芯片接收所述第二加密数据，以及基于所述安全芯片加密协议对所述第二加密数据进行加密，得到第三加密数据；

由所述通信模组接收所述第三加密数据，以及将所述第三加密数据转发至所述服务器；以及

由所述服务器接收所述第三加密数据，以及基于所述安全芯片协议和所述第二加密协议对所述第三加密数据进行解密。

11、根据权利要求 10 所述的方法，其中，所述服务器包括物联网安全接入平台和物联网应用平台，所述服务器接收所述第三加密数据，以及基于所述安全芯片协议和所述第二加密协议对所述第三加密数

据进行解密包括：

由所述物联网安全接入平台接收所述第三加密数据，基于所述安全芯片加密协议对所述第三加密数据进行解密，得到所述第二加密数据，以及将所述第二加密数据转发至所述物联网应用平台；

由所述物联网应用平台接收所述第二加密数据，以及基于所述第二加密协议对所述第二加密数据进行解密。

12、根据权利要求 9 所述的方法，其中，所述主控制器基于所述第一加密协议进行数据加密，得到第一加密数据之前，所述方法还包括：

由所述主控制器接收所述服务器发送的第一升级指令，以及基于所述第一升级指令对所述主控制器中第一加密协议的运行软件进行升级；以及

由所述通信模组接收所述服务器发送的第二升级指令，以及基于所述第二升级指令对所述通信模组中第一加密协议的运行软件进行升级。

13、根据权利要求 12 所述的方法，其中，所述主控制器接收所述服务器发送的第一升级指令，基于所述第一升级指令对所述主控制器中第一加密协议的运行软件进行升级之后，所述方法还包括：

由所述主控制器将所述第一加密协议的运行软件的升级结果发送至所述服务器；

响应于升级成功，由所述服务器向所述通信模组发送所述第二升级指令；以及

响应于升级失败，由所述服务器重新向所述主控制器发送所述第一升级指令。

14、根据权利要求 10 所述的方法，其中，所述主控制器基于所述第二加密协议进行数据加密，得到第二加密数据，将所述第二加密数据发送至所述安全模组中的所述通信模组之前，所述方法还包括：

由所述主控制器接收所述服务器发送的第三升级指令，以及基于所述第三升级指令对所述主控制器中第二加密协议的运行软件进行升级。

15. 一种计算机存储介质，其上存储有指令，所述指令被处理器执行时实现如权利要求 9 至 14 中任一项所述的方法。

16. 一种包括指令的计算机程序产品，其中所述指令被处理器执行时，使得所述处理器执行如权利要求 9 至 14 中任一项所述的方法。

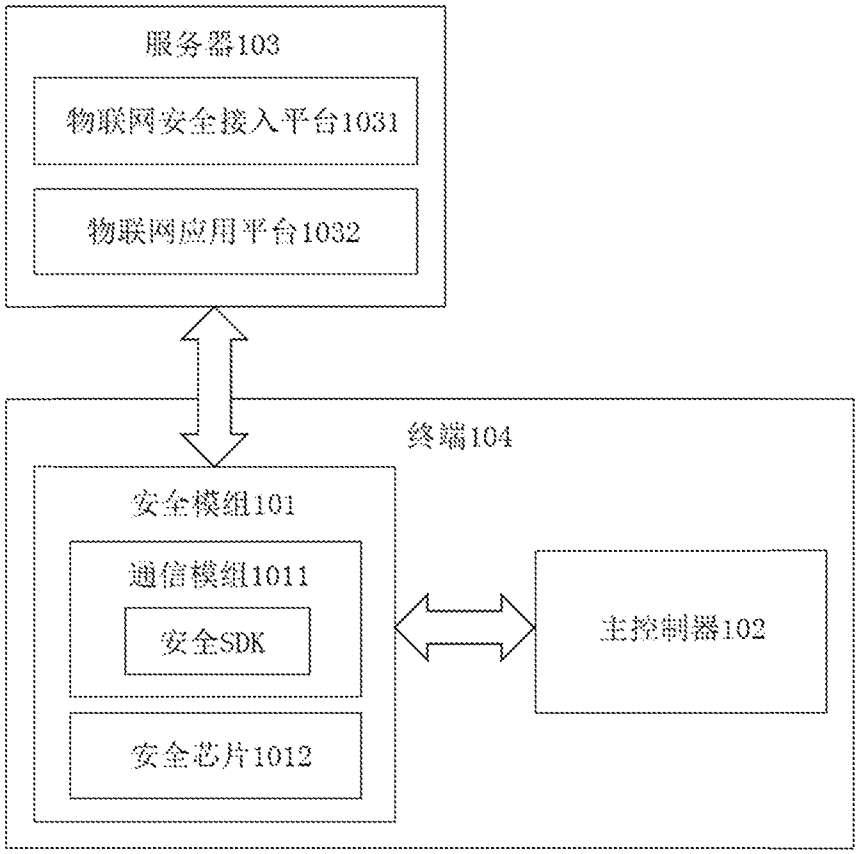
服务器103
物联网安全接入平台1031
物联网应用平台1032
终端104
安全模组101
通信模组1011
安全SDK
安全芯片1012
主控制器102

图 1

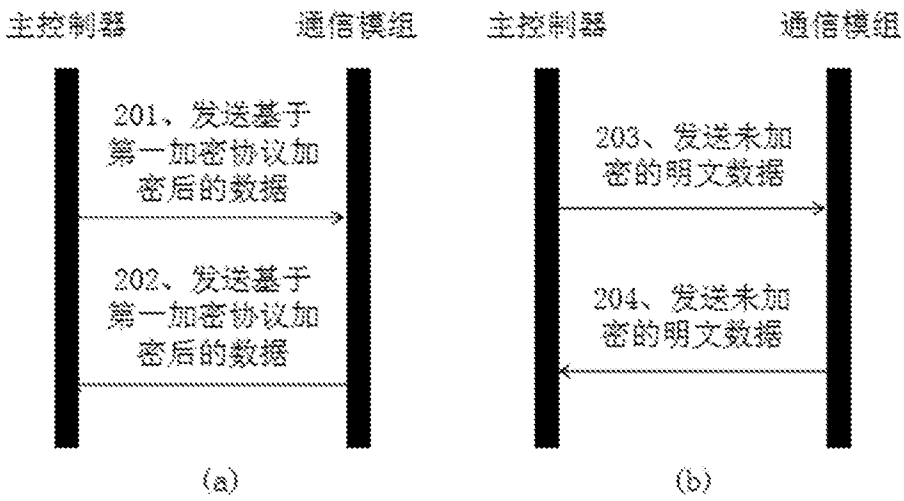
主控制器
通信模组
201、发送基于第一加密协议加密后的数据
202、发送基于第一加密协议加密后的数据
(a)
主控制器
通信模组
203、发送未加密的明文数据
204、发送未加密的明文数据
(b)

图 2

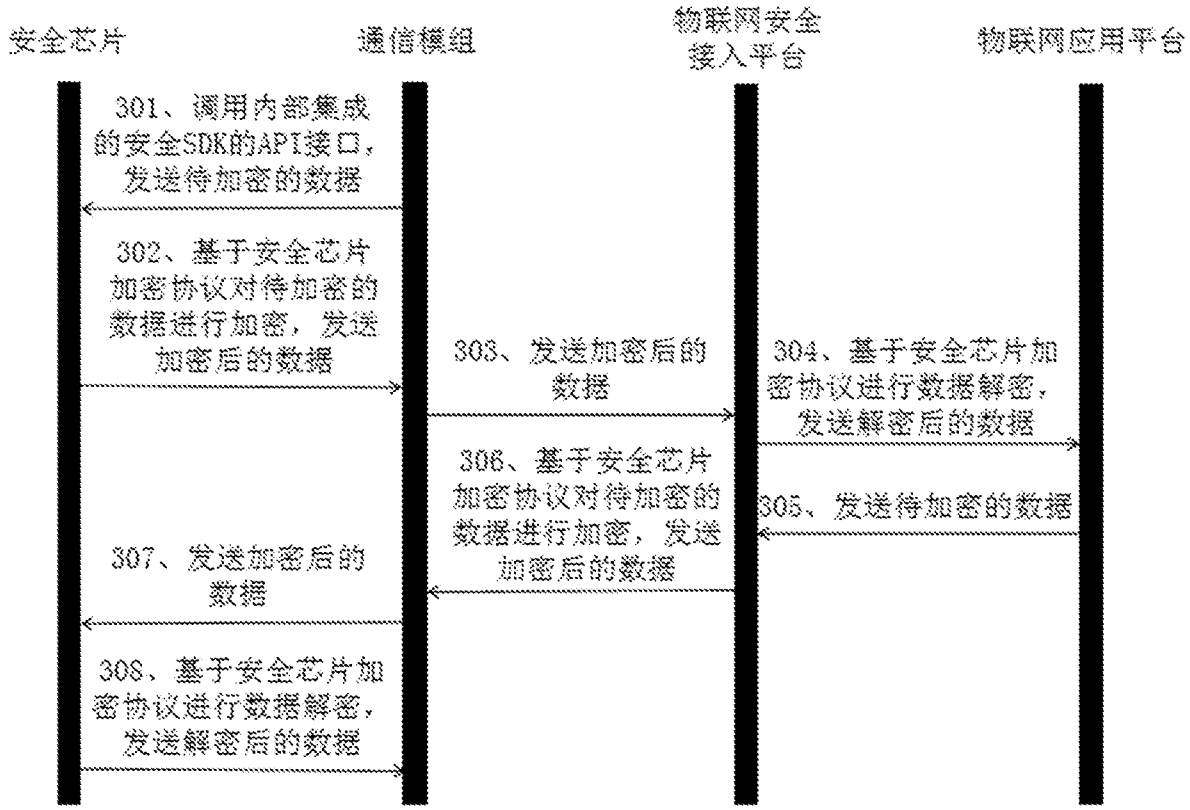
安全芯片
通信模组
物联网安全接入平台
物联网应用平台
301、调用内部集成的安全SDK的API接口，发送待加密的数据
302、基于安全芯片加密协议对待加密的数据进行加密，发送加密后的数据
303、发送加密后的数据
304、基于安全芯片加密协议进行数据解密，发送解密后的数据
305、发送待加密的数据
306、基于安全芯片加密协议对待加密的数据进行加密，发送加密后的数据
307、发送加密后的数据
308、基于安全芯片加密协议进行数据解密，发送解密后的数据

图 3

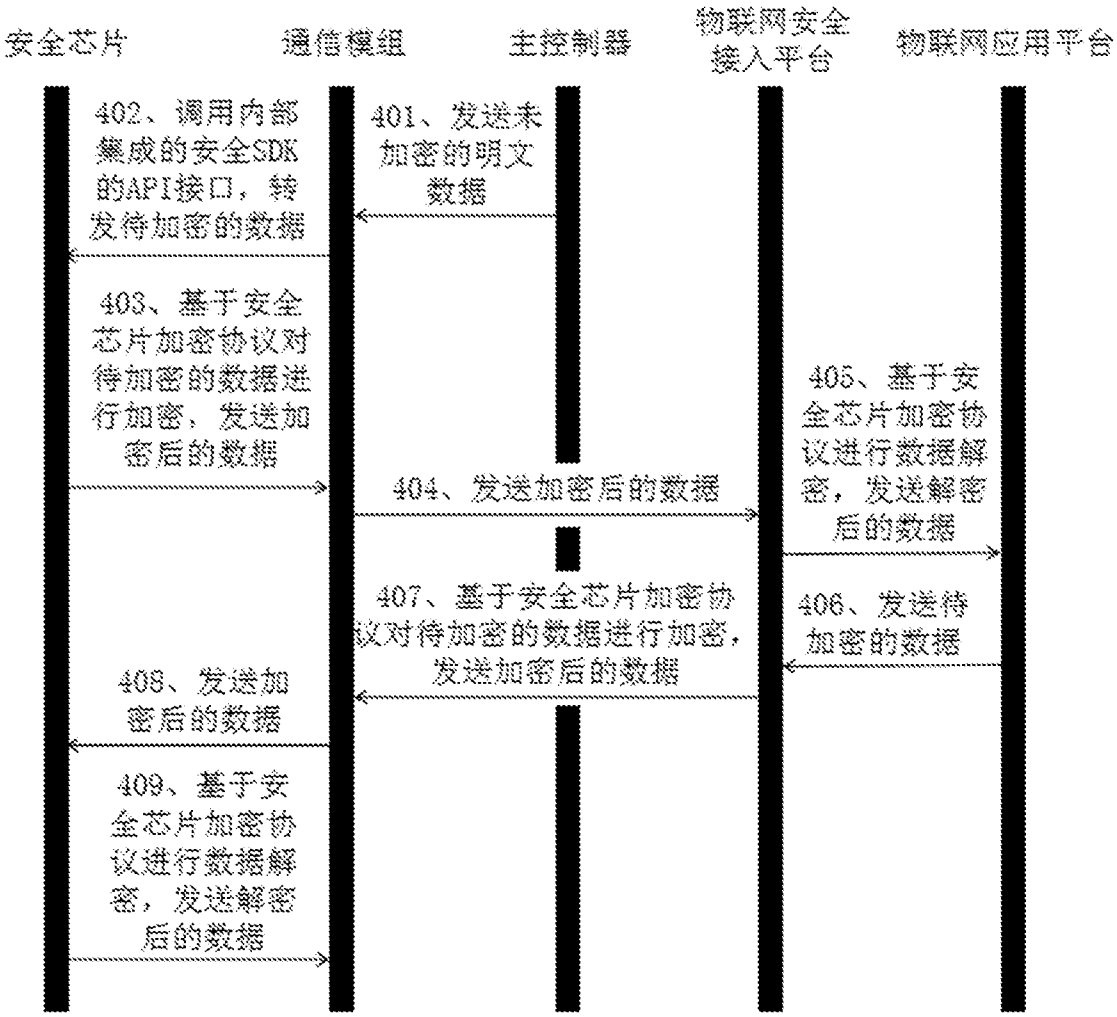
安全芯片
通信模组
主控制器
物联网安全接入平台
物联网应用平台
401、发送未加密的明文数据
402、调用内部集成的安全SDK的API接口，转发待加密的数据
403、基于安全芯片加密协议对待加密的数据进行加密，发送加密后的数据
404、发送加密后的数据
405、基于安全芯片加密协议进行数据解密，发送解密后的数据
406、发送待加密的数据
407、基于安全芯片加密协议对待加密的数据进行加密，发送加密后的数据
408、发送加密后的数据
409、基于安全芯片加密协议进行数据解密，发送解密后的数据

图 4

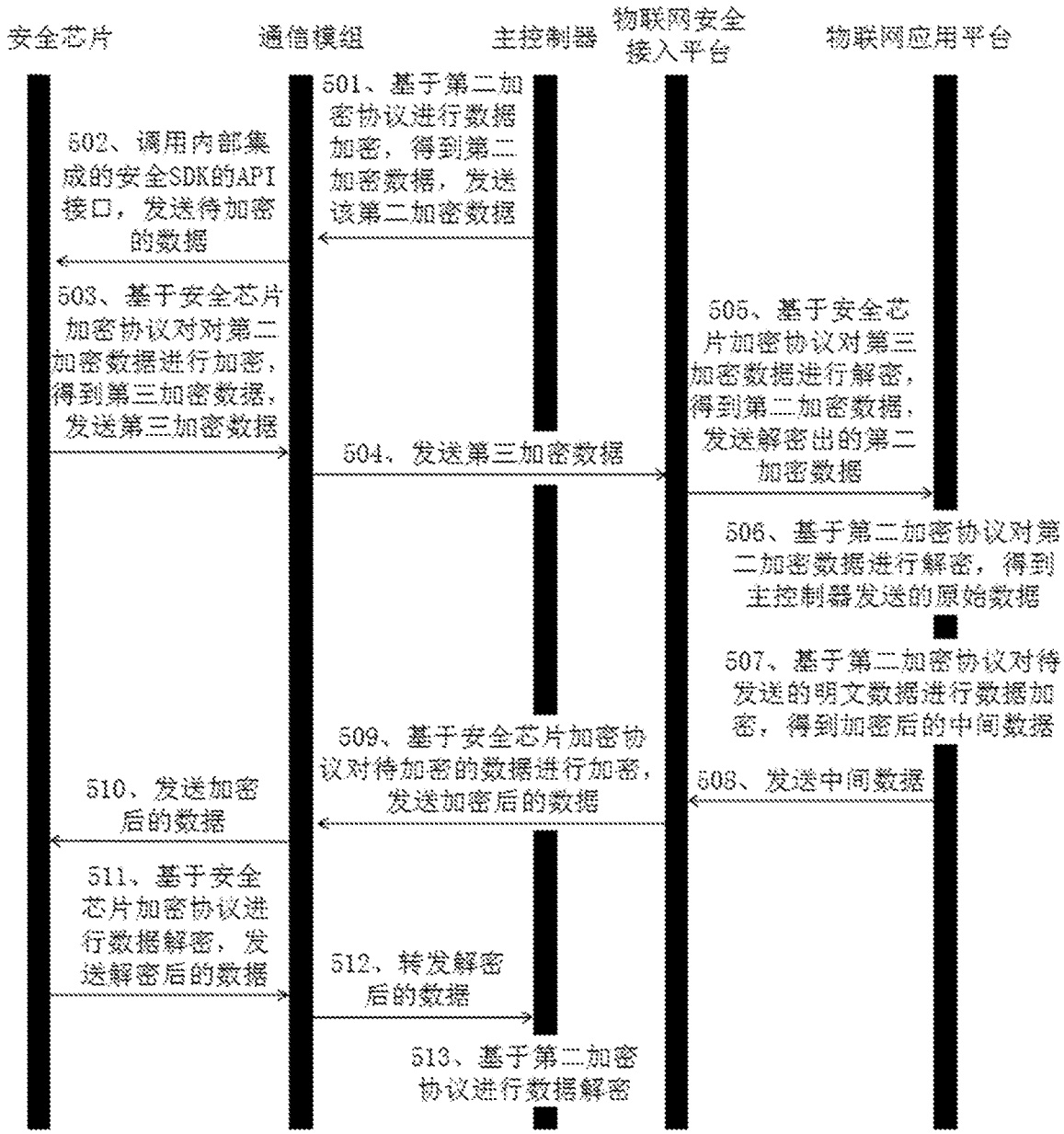
安全芯片
通信模组
主控制器
物联网安全接入平台
物联网应用平台
501、基于第二加密协议进行数据加密，得到第二加密数据，发送该第二加密数据
502、调用内部集成的安全SDK的API接口，发送待加密的数据
503、基于安全芯片加密协议对对第二加密数据进行加密，得到第三加密数据，发送第三加密数据
504、发送第三加密数据
505、基于安全芯片加密协议对第三加密数据进行解密，得到第二加密数据，发送解密出的第二加密数据
506、基于第二加密协议对第二加密数据进行解密，得到主控制器发送的原始数据
507、基于第二加密协议对待发送的明文数据进行数据加密，得到加密后的中间数据
508、发送中间数据
509、基于安全芯片加密协议对待加密的数据进行加密，发送加密后的数据
510、发送加密后的数据
511、基于安全芯片加密协议进行数据解密，发送解密后的数据
512、转发解密后的数据
513、基于第二加密协议进行数据解密

图 5

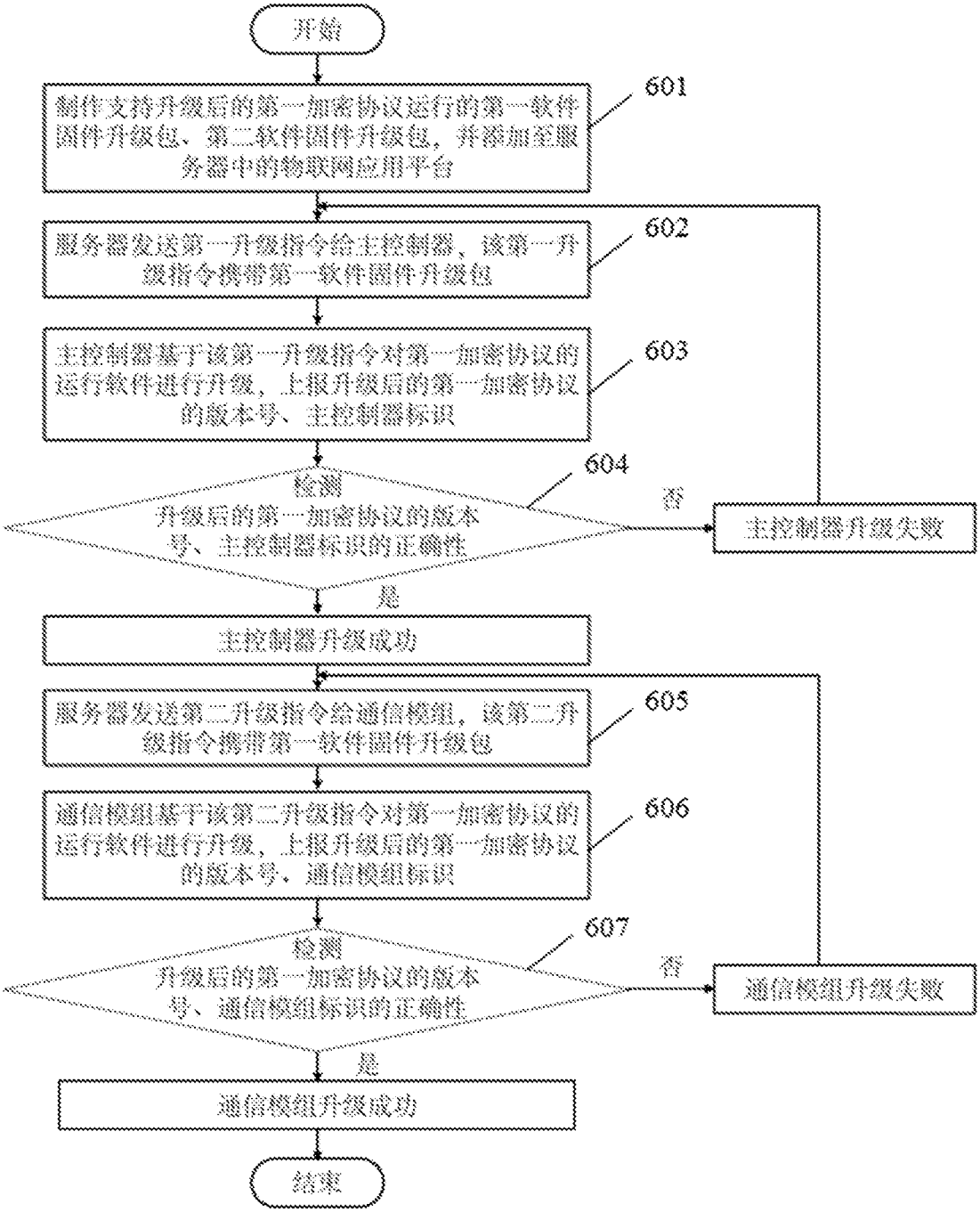
开始
制作支持升级后的第一加密协议运行的第一软件固件升级包、第二软件固件升级包，并部署至服务器中的物联网应用平台
601
服务器发送第一升级指令给主控制器，该第一升级指令携带第一软件固件升级包
602
主控制器基于该第一升级指令对第一加密协议的运行软件进行升级，上报升级后的第一加密协议的版本号、主控制器标识
603
检测升级后的第一加密协议的版本号、主控制器标识的正确性
604
否
主控制器升级失败
是
主控制器升级成功
服务器发送第二升级指令给通信模组，该第二升级指令携带第一软件固件升级包
605
通信模组基于该第二升级指令对第一加密协议的运行软件进行升级，上报升级后的第一加密协议的版本号、通信模组标识
606
检测升级后的第一加密协议的版本号、通信模组标识的正确性
607
否
通信模组升级失败
是
通信模组升级成功
结束

图 6

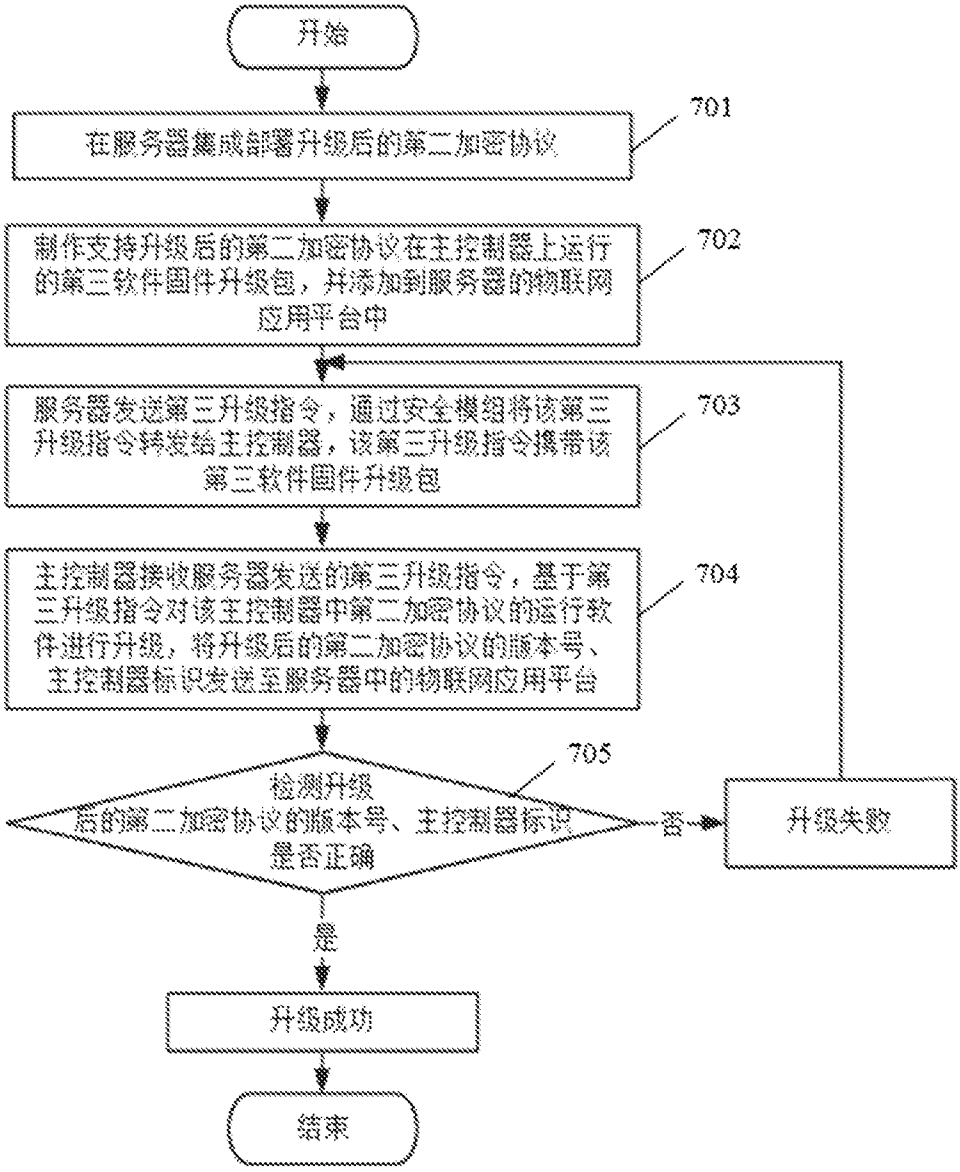
开始
在服务器集成部署升级后的第二加密协议
701
制作支持升级后的第二加密协议在主控制器上运行的第三软件固件升级包，并添加到服务器的物联网应用平台中
702
服务器发送第三升级指令，通过安全模组将该第三升级指令转发给主控制器，该第三升级指令携带该第三软件固件升级包
703
主控制器接收服务器发送的第三升级指令，基于第三升级指令对该主控制器中第二加密协议的运行软件进行升级，将升级后的第二加密协议的版本号、主控制器标识发送至服务器中的物联网应用平台
704
检测升级后的第二加密协议的版本号、主控制器标识是否正确
705
否
升级失败
是
升级成功
结束

图 7

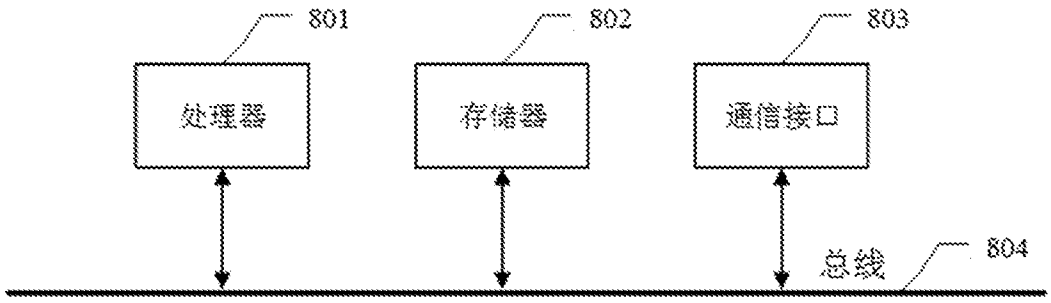
801
处理器
802
存储器
803
通信接口
总线
804

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/113795

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01)i; H04W12/00(2021.01)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)

IPC: H04L、H04W

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)

CNABS, CNTXT, VEN, USTXT, WOTXT, EPTXT, CNKI, IEEE: 终端, 设备, 内部, 外部, 安全, 加密, 协议, 算法, 不同, 多个, 模组, 组件, 芯片, terminal, internal, inside, external, outside, security, encrypt, security, protocol, chip

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 112887263 A (MIDEA GROUP CO., LTD. et al.) 01 June 2021 (2021-06-01) description, paragraphs [0043]-[0057], and figures 1-4	1-2
Y	CN 107277320 A (BEIJING SHIBO FUSION TECHNOLOGY CO., LTD.) 20 October 2017 (2017-10-20) description, paragraphs [0044]-[0059]	1-2
Y	US 2016196437 A1 (DONGGUAN LEVETOP TECHNOLOGY CO., LTD.) 07 July 2016 (2016-07-07) description, paragraphs [0027]-[0054], and figures 1-2	1-2
A	CN 111683367 A (ZHENGZHOU XINDA JIEAN INFORMATION TECHNOLOGY CO., LTD.) 18 September 2020 (2020-09-18) entire document	1-16

☐ 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
"D" document cited by the applicant in the international application
"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
04 November 2024	**07 November 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/113795

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112887263 A	01 June 2021	None	
CN 107277320 A	20 October 2017	None	
US 2016196437 A1	07 July 2016	WO 2015032063 A1	12 March 2015
CN 111683367 A	18 September 2020	CN 111683367 B	11 February 2022

国际检索报告

国际申请号
PCT/CN2024/113795

A. 主题的分类

H04L9/40(2022.01)i；H04W12/00(2021.01)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)

IPC：H04L、H04W

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））

CNABS,CNTXT,VEN,USTXT,WOTXT,EPTXT,CNKI,IEEE:终端，设备，内部，外部，安全，加密，协议，算法，不同，多个，模组，组件，芯片；terminal, internal, inside, external, outside, security, encrypt, security, protocol, chip

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
Y	CN 112887263 A (美的集团股份有限公司等) 2021年6月1日 (2021 - 06 - 01) 说明书第[0043]-[0057]段，图1-4	1-2
Y	CN 107277320 A (北京视博融合科技有限公司) 2017年10月20日 (2017 - 10 - 20) 说明书第[0044]-[0059]段	1-2
Y	US 2016196437 A1 (DONGGUAN LEVETOP TECHNOLOGY CO LTD) 2016年7月7日 (2016 - 07 - 07) 说明书第[0027]-[0054]段，图1-2	1-2
A	CN 111683367 A (郑州信大捷安信息技术股份有限公司) 2020年9月18日 (2020 - 09 - 18) 全文	1-16

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2024年11月4日	2024年11月7日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 朱丹丹 电话号码 (+86) 020-28950440

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/113795

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 112887263 A	2021年6月1日	无	
CN 107277320 A	2017年10月20日	无	
US 2016196437 A1	2016年7月7日	WO 2015032063 A1	2015年3月12日
CN 111683367 A	2020年9月18日	CN 111683367 B	2022年2月11日