

(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 26 日 (26.06.2025)



(10) 国际公布号
WO 2025/130622 A1

(51) 国际专利分类号:

H04L 9/40 (2022.01)

北京市朝阳区农展馆南路 13 号 瑞辰国际中心 509 室 100125 (CN)。

(21) 国际申请号:

PCT/CN2024/136887

(22) 国际申请日:

2024 年 12 月 4 日 (04.12.2024)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202311775094.5 2023 年 12 月 21 日 (21.12.2023) CN

(71) 申请人: 长城汽车股份有限公司 (**GREAT WALL MOTOR COMPANY LIMITED**) [CN/CN]; 中国河北省保定市朝阳南大街 2266 号 071000 (CN)。

(72) 发明人: 郭阳 (**GUO, Yang**); 中国河北省保定市朝阳南大街 2266 号 071000 (CN)。董凯歌 (**DONG, Kaige**); 中国河北省保定市朝阳南大街 2266 号 071000 (CN)。

(74) 代理人: 北京风雅颂专利代理有限公司 (**BEIJING FORESTSONG PATENT AGENCY CO., LTD**); 中国

(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,

(54) **Title:** DATA SECURITY VERIFICATION METHOD, RELATED DEVICE AND VEHICLE

(54) 发明名称: 数据安全验证方法、相关设备及车辆

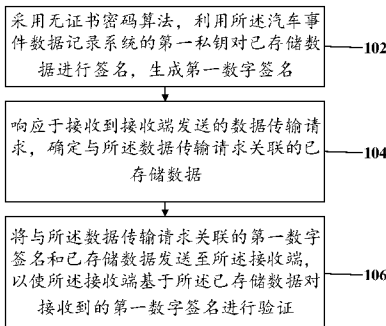


图 2

102 Use a certificateless cryptographic algorithm, and use a first private key of a vehicle event data recorder to sign stored data to generate a first digital signature
104 In response to receiving a data transmission request sent by a receiving end, determine the stored data associated with the data transmission request
106 Send to the receiving end the first digital signature and the stored data, which are associated with the data transmission request, so that the receiving end verifies the received first digital signature on the basis of the stored data

(57) **Abstract:** The present application provides a data security verification method, a related device and a vehicle. The method comprises: using a certificateless cryptographic algorithm, and using a first private key of a vehicle event data recorder (EDR) to sign stored data to generate a first digital signature; in response to receiving a data transmission request sent by a receiving end, determining the stored data associated with the data transmission request; and sending the first digital signature and the stored data to the receiving end, so that the receiving end verifies the received first digital signature on the basis of the stored data. By means of the data security verification method provided in the present application, the integrity and authenticity of the stored data can be verified, and the certificateless cryptographic algorithm used in the data security verification method can also improve the data verification rate, thus improving the EDR data reading rate.

[见续页]

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: 本申请提供一种数据安全验证方法、相关设备及车辆, 包括采用无证书密码算法, 利用汽车事件数据记录系统的第一私钥对已存储数据进行签名, 生成第一数字签名。响应于接收到接收端发送的数据传输请求, 确定与数据传输请求关联的已存储数据。将第一数字签名和已存储数据发送至接收端, 以使接收端基于已存储数据对接收到的第一数字签名进行验证。通过本申请提供的数据安全验证方法, 既能够对已存储数据的完整性和真实性进行验证, 数据安全验证方法中采用的无证书密码算法还能够提升数据验证速率, 进而提升EDR数据读取速率。

数据安全验证方法、相关设备及车辆

本申请要求在 2023 年 12 月 21 日提交中国专利局、申请号为 2023117750945、专利申请名称为“数据安全验证方法、相关设备及车辆”的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及车辆数据安全技术领域，尤其涉及一种数据安全验证方法、相关设备及车辆。

背景技术

目前，新生产的乘用车根据安全要求需要配备汽车事件数据记录系统(Event DataRecorder, EDR)。EDR 能够记录车辆在碰撞前、碰撞时和碰撞后三个阶段中的运行参数和安全状态信息，运行参数和安全状态信息等数据通过车身 CAN/LIN 总线实时读取。目前，EDR 数据读取时仍然存在安全威胁，数据读取端无法确定 EDR 数据是否为合法性数据。因此，亟需一种能够在 EDR 数据读取过程中进行有效身份验证的方法，以避免 EDR 数据被非法读取盗用或者数据被非法篡改删除等。

技术内容

有鉴于此，本申请的目的在于提出一种数据安全验证方法、相关设备及车辆，以解决读取 EDR 数据时安全性较差的问题。

基于上述目的，本申请的第一方面提供了一种数据安全验证方法，应用于汽车事件数据记录系统，方法包括：

采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名；

响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据；将与数据传输请求关联的第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对接收到的第一数字签名进行验证。

可选的，采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名，包括：

基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一私钥，采用无证书密码算法中的数字签名生成算法，生成第一数字签名。

可选的，若密码服务系统为无证书系统，基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一私钥，采用无证书密码算法中的数字签名

生成算法，生成第一数字签名，包括：

对第一标识、椭圆曲线系统参数和密码服务端的主公钥拼接后生成的字符串进行密码杂凑计算，得到第一杂凑值；

5 计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第一公钥分量；

利用椭圆曲线系统参数、第一杂凑值、第一公钥分量和第一私钥，采用无证书密码算法中的数字签名生成算法对已存储数据进行签名，生成第一数字签名。

10 可选的，若密码服务系统为隐式证书系统，基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一私钥，采用无证书密码算法中的数字签名生成算法，生成第一数字签名，包括：

利用椭圆曲线系统参数、汽车事件数据记录系统的隐式证书和第一私钥，采用无证书密码算法中的数字签名生成算法对已存储数据进行签名，生成第一数字签名。

可选的，基于椭圆曲线系统参数和随机数，计算得到汽车事件数据记录系统的第一公钥分量，包括：

15 计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第一公钥分量。

可选的，数据安全验证方法还包括：

记录车辆的初始事件数据；

20 基于初始事件数据的终点时刻，采用无证书公钥密码算法中的数字签名生成算法对初始事件数据进行签名，生成时间戳，将时间戳和初始事件数据作为已存储数据。

可选的，基于初始事件数据的终点时刻，采用无证书公钥密码算法中的数字签名生成算法对初始事件数据进行签名，生成时间戳，包括：

采用哈希算法对初始事件数据进行哈希计算，得到第一哈希值；

25 将第一哈希值和初始事件数据的终点时刻发送至时间戳服务中心，以使时间戳服务中心基于第一哈希值和终点时刻生成时间戳。

本申请的第二方面还提供了一种数据安全验证方法，应用于接收端，数据安全验证方法包括：

向汽车事件数据记录系统发送数据传输请求；

接收汽车事件数据记录系统根据数据传输请求返回的第一数字签名和已存储数据；

30 采用无证书密码算法，基于已存储数据对第一数字签名进行验证。

可选的，采用无证书密码算法，基于已存储数据对第一数字签名进行验证，包括：

基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数和随机数计算得到汽车事件数据记录系统的第一公钥；

35 基于第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一公钥，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证。

可选的，若密码服务系统为无证书系统时，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证，包括：

对第一标识、椭圆曲线系统参数和密码服务系统的主公钥拼接后生成的字符串进行密码杂凑计算，得到第二杂凑值；

计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第三公钥分量；

5 利用椭圆曲线系统参数、第二杂凑值、第三公钥分量、已存储数据和第一公钥，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证。

本申请的第三方面提供了一种数据安全验证装置，应用于汽车事件数据记录系统，装置包括：处理器，其中，处理器用于执行存储在存储器中的以下程序模块：

10 确定模块，被配置为采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名；

签名模块，被配置为响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据；

发送模块，被配置为将与数据传输请求关联的第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对接收到的第一数字签名进行验证。

15 本申请的第四方面提供了一种数据安全验证装置，应用于事故数据恢复设备，装置包括：处理器，其中，处理器用于执行存储在存储器中的以下程序模块：

请求模块，被配置为向汽车事件数据记录系统发送数据传输请求；

接收模块，被配置为接收汽车事件数据记录系统根据数据传输请求返回的第一数字签名和已存储数据；

20 验证模块，被配置为采用无证书密码算法，基于已存储数据对第一数字签名进行验证。

本申请的第五方面提供了一种汽车事件数据记录系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时实现如第一方面所述的方法。

25 本申请的第六方面提供了一种事故数据恢复设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时实现如第二方面所述的方法。

本申请的第七方面还提供了一种车辆，车辆包括如第五方面所述的汽车事件数据记录系统。

30 从上面所述可以看出，本申请提供的数据安全验证方法、相关设备及车辆，方法包括采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名，第一数字签名可以用于验证已存储数据的完整性。其中，在生成第一数字签名过程中采用的无证书密码算法去除了数字证书的相关计算，实现公私钥的发放不依赖于数字证书，公私钥生成速率较快。同时，数字证书的去除降低了通信传输过程中数字证书对于通信资源的占用，在数字签名验证过程中降低了算力需求，从而有效提升计算速率，能够更好的与汽车事件数据记录系统的数据处理能力相匹配。响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据，也即在汽车事件数据记录系统中根据数据传输请求确定已存储的与数据传输请求对应的已存储数据。将与数据传输请

35

求关联的第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对接收到的第一数字签名进行验证，验证通过，表示汽车事件数据记录系统身份合法，已存储数据未被篡改，增加了数据读取的安全性。通过本申请提供的数据安全验证方法，能够对汽车事件数据记录系统身份合法性进行验证，避免已存储数据被篡改，且数据安全验证方法中采用的无证书密码算法还能够提升数据验证速率，进而提升 EDR 数据读取速率。

附图说明

为了更清楚地说明本申请或相关技术中的技术方案，下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，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 为本申请实施例的汽车事件数据记录系统和接收端之间的交互示意图；

图 2 为本申请实施例的数据安全验证方法的流程示意图；

图 3 为本申请实施例的第一数字签名的生成方法的流程示意图；

图 4 为本申请另一实施例的数据安全验证方法的流程示意图；

图 5 为本申请实施例的对第一数字签名进行验证方法的流程示意图；

图 6 为本申请实施例的数据安全验证装置的结构示意图；

图 7 为本申请另一实施例的数据安全验证装置的结构示意图；

图 8 为本申请实施例的电子设备硬件结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本申请进一步详细说明。

需要说明的是，除非另外定义，本申请实施例使用的技术术语或者科学术语应当为本申请所属领域内具有一般技能的人士所理解的通常意义。本申请实施例中使用的“第一”、“第二”以及类似的词语并不表示任何顺序、数量或者重要性，而只是用来区分不同的组成部分。“包括”或者“包含”等类似的词语意指出现该词前面的元件或者物件涵盖出现在该词后面列举的元件或者物件及其等同，而不排除其他元件或者物件。“连接”或者“相连”等类似的词语并非限定于物理的或者机械的连接，而是可以包括电性的连接，不管是直接的还是间接的。“上”、“下”、“左”、“右”等仅用于表示相对位置关系，当被描述对象的绝对位置改变后，则该相对位置关系也可能相应地改变。

EDR 可以记录车辆行驶信息，EDR 在车辆发生紧急事件时会及时的记录一段时间的数据信息，直到紧急事件解除为止，例如汽车超速、急停等情况。EDR 数据可以作为重要证据来判定事故责任方，EDR 的普及给车辆的取证工作带来了极大的便捷，但是 EDR 也同样面临着数据安全的问题，不论是汽车厂商、车主或者是第三方都有可能出于自己的利益

对数据进行篡改,导致 EDR 数据无法客观还原事故真相。因此,对 EDR 数据的防篡改和完整性保护迫在眉睫。

为了保证读取 EDR 数据的安全性,需要在读取过程中对读取端进行身份认证。目前,国内车企构建的 PKI-CA 体系都是基于网络安全主流的加密标准 RSA 算法 (RSA2048) 来实现,使用 RSA 算法生成的公私钥证书来实现读取端的身份认证。RSA 算法是一种非对称加密算法,生成一对 RSA 秘钥,即公钥和私钥,将公钥提供给调用方,从而完成公钥加密私钥解密和私钥签名公钥验签。但是,在 2017 年,RSA1024 已宣布被破解(1024 表示公钥及私钥分别是 1024bit),如今 RSA2048 (2048 表示公钥及私钥分别是 2048bit) 存在破解方法,理论上已被破解,算法的破解给通信的安全性带来了威胁。除了算法被破解外,由于 RSA 算法的加密长度过长,对于应用端的消耗是比较大的,计算的速度也会比较慢,效率相对较低。

此外,在 RSA 算法中,各端的通信必须通过数字证书实现,数字证书机制虽然解决了密钥管理问题,但是作为公钥载体的数字证书比较大,一般证书大小在 2KB~4KB。大量的数字证书将会导致数字证书管理复杂,且通信效率低。

有鉴于此,本申请提供了一种数据安全验证方法,在确保安全读取 EDR 数据的情况下,提升 EDR 数据读取速率。在实施本申请的方法前,EDR 和读取端需要满足一定的前置条件。具体的前置条件包括:EDR 内部开发完成轻量级密码算法固件,具备安全远程通讯能力(用于导出数据时的建立安全通讯),固件功能涵盖密钥生成、密钥存储、密钥使用、密钥更新、密钥分发、密钥销毁,以及轻量级证书签发时的公私钥一致性检查。接收端设备需要完成密钥的分发与存储、安全远程通讯及可验证带事件戳签名的验证能力。

以下结合附图来详细说明本申请的实施例。

图 1 示出了汽车事件数据记录系统和接收端之间的交互示意图。如图 1 所示,汽车事件数据记录系统 01 与接收端 02 之间能够进行数据交互。本申请提供了一种数据安全验证方法,应用于汽车事件数据记录系统,参考图 2,方法包括以下步骤:

步骤 102、采用无证书密码算法,利用汽车事件数据记录系统的第一私钥对已存储数据进行签名,生成第一数字签名。

具体的,当车辆发生紧急事件时,汽车事件数据记录系统 EDR 记录并存储该紧急事件,作为已存储数据。已存储数据生成后,为了确保已存储数据的安全存储,需要对已存储数据进行签名,通过签名可以证实已存储数据的完整性。本实施例中采用的数字签名生成算法是无证书密码算法中的数字签名生成算法。无证书密码算法为基于椭圆曲线公钥密码算法的无证书及隐式证书公钥密码算法,也称为基于 SM2 算法的无证书及隐式证书公钥密码算法。此算法解决了基于数字证书认证的证书管理复杂、通信效率低等问题。本实施例中采用无证书密码算法中的数字签名生成算法,利用 EDR 的第一私钥对已存储数据进行签名,生成第一数字签名。第一数字签名用于验证 EDR 是否具有合法身份以及已存储事件是否被篡改。如果验证不通过,表示 EDR 身份不合法或已存储数据被篡改,说明已存储数据为不可信数据,需要终止汽车事件数据记录系统与接收端之间的通信。如果验证通过,表示 EDR 身份合法且已存储数据未被篡改,说明已存储数据为可信数据,接收端可以根据已存储数

据进行后续的分析并生成分析报告。

步骤 104、响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据。

具体的，当本实施例中的接收端为能够读取 EDR 数据的设备端，示例性的，接收端可以以为事故数据恢复工具 CDR（Crash Data Retrieval）。当用户需要读取 EDR 数据时，可以借助 CDR 进行读取。将 CDR 设备通过接口插入 EDR 设备内，在数据链路层保持连接，并对 EDR 数据进行读取。用户可以通过 CDR 发送数据传输请求，数据传输请求中携带了需要读取的已存储事件的标识，根据已存储事件的标识，EDR 可以确定与数据传输请求关联的已存储数据。

步骤 106、将与数据传输请求关联的第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对接收到的第一数字签名进行验证。

具体的，汽车事件数据记录系统生成第一数字签名后，将第一数字签名和已存储数据发送至接收端。接收端接收已存储数据和第一数字签名。接收端基于接收到的已存储数据对第一数字签名进行验证，验证算法采用的是无证书密码算法中的数字签名验证算法。若验证通过，表示已存储数据未被篡改，接收端可以根据已存储数据进行后续的分析并生成分析报告。

基于上述步骤 102 至步骤 106，本实施例提供的数据安全验证方法包括：采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名。其中，在生成第一数字签名过程中采用的无证书密码算法去除了数字证书的相关计算，实现公私钥的发放不依赖于数字证书，公私钥生成速率较快。同时，数字证书的去除降低了通信传输过程中数字证书对于通信资源的占用，在数字签名验证过程中降低了算力需求，从而有效提升计算速率，能够更好的与汽车事件数据记录系统的数据处理能力相匹配。响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据，也即在汽车事件数据记录系统中根据数据传输请求确定已存储的与数据传输请求对应的已存储数据。将与数据传输请求关联的第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对接收到的第一数字签名进行验证，验证通过，表示已存储数据未被篡改且 EDR 身份具有合法性。通过本申请提供的数据安全验证方法，能够对汽车事件数据记录系统身份合法性进行验证，避免已存储数据被篡改，且数据安全验证方法中采用的无证书密码算法还能够提升数据验证速率，进而提升 EDR 数据读取速率。

下面通过具体实施例描述第一数字签名的生成方法。

在一些实施例中，采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名，包括：

基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一私钥，采用无证书密码算法中的数字签名生成算法，生成第一数字签名。

需要说明的是，本申请中的密码服务系统为 ECS 密码服务端，负责 ECS 主密钥管理，并提供相应的密码算力支持。密码服务系统可以分为无证书系统和隐式证书系统。无证书系统是一种不依赖数字证书验证用户公钥真实性并且密钥生成中心不具有密钥委托功能的

公钥密码系统。隐式证书是包含用户标识和公钥还原数据等信息但不显式包含证书认证机构 (CA) 的数字签名的数字证书。隐式证书系统是依赖隐式证书的公钥密码系统。下面将分别对无证书系统和隐式证书系统下, 第一数字签名的生成方法进行说明。

进一步的, 当密码服务系统为无证书系统时, 参考图 3, 第一数字签名的生成方法包括以下步骤:

步骤 202、对第一标识、椭圆曲线系统参数和密码服务端的主公钥拼接后生成的字符串进行密码杂凑计算, 得到第一杂凑值。

具体的, 第一标识为接收端的唯一身份标识, 例如接收端 ID (Identity document) 或唯一可识别名称等。椭圆曲线系统参数是椭圆曲线密码系统的参数, 椭圆曲线密码系统是应用 SM2 椭圆曲线公钥密码算法的系统, SM2 椭圆曲线公钥密码算法是国密算法的一种。

进一步的, 按照无证书密码算法的计算方式, 生成第一数字签名时需要依次计算得到第一杂凑值和第一公钥分量, 再采用数字签名生成算法生成得到第一数字签名。在本步骤中, 第一杂凑值 H_A 的计算方法还可以通过下式表示:

$$H_A = H_{256}(ENTL_A \| d'_A \| a \| b \| X_G \| Y_G \| X_{Pub} \| Y_{Pub})$$

其中, $H_{256}()$ 表示消息摘要长度为 256 比特的密码杂凑算法, $ENTL_A$ 是由整数 $entlen_A$ 转换而成的两个字节, $entlen_A$ 为第一标识的比特长度。 $a \| b$ 表示 a 与 b 的拼接, a 与 b 的数据类型可以是比特串或字符串。 a 、 b 、 X_G 、 Y_G 为椭圆曲线系统参数, a 与 b 为椭圆曲线方程参数, (X_G, Y_G) 为 G 的坐标, G 表示椭圆曲线公钥密码算法中椭圆曲线的一个基点。 (X_{Pub}, Y_{Pub}) 为 P_{Pub} 的坐标, P_{Pub} 为密码服务端的主公钥。 X_G 、 Y_G 、 X_{Pub} 、 Y_{Pub} 的数据类型均为比特串。

步骤 204、计算椭圆曲线系统参数和随机数的乘积, 对该乘积和椭圆曲线系统参数的倍数进行求和运算, 得到汽车事件数据记录系统的第一公钥分量。

本步骤中, 根据椭圆曲线系统参数和随机数计算得到第一公钥分量。随机数是 EDR 产生的随机数。进一步的, 第一公钥分量 w_A 的具体计算方法可以通过下式表示:

$$w_A = [w]G + U_A$$

其中, U_A 为第二公钥分量, $U_A = [d'_A]G$ 。 $[d'_A]G$ 表示椭圆曲线上点 G 的 d'_A 倍点, 即 $[d'_A]G = G + G + \dots + G$, 等式右边 G 的数量为 d'_A 个, d'_A 为正整数。 d'_A 为 EDR 生成的随机数, $d'_A \in [1, n-1]$ 。 $[w]G$ 表示椭圆曲线上点 G 的 w 倍点, 即 $[w]G = G + G + \dots + G$, 等式右边 G 的数量为 w 个, w 为正整数。 w 为密码服务系统产生的随机数, $w \in [1, n-1]$ 。 G 表示椭圆曲线的一个基点, 其阶为素数, n 表示基点 G 的阶。

步骤 206、利用椭圆曲线系统参数、第一杂凑值、第一公钥分量和第一私钥, 采用无证书密码算法中的数字签名生成算法对已存储数据进行签名, 生成第一数字签名。

在本步骤中, 根据前述两个步骤中计算得到第一杂凑值和第一公钥分量后, 对已存储数据进行签名, 生成第一数字签名。第一数字签名 (r, s) 的生成方法通过下式表示:

$$(r, s) = \text{SIGN}(\text{param}, H_A, x_{w_A} \| y_{w_A} \| M, O, d_A)$$

其中, $\text{SIGN}()$ 表示数字签名算法, param 表示椭圆曲线系统参数, x_{w_A} 和 y_{w_A} 为 w_A 的坐标, M 表示已存储数据, O 表示椭圆曲线上的一个特殊点, 称为无穷远点或零点, 是椭圆

曲线加法群的单位元， d_A 表示第一私钥。

进一步的，当密码服务系统为隐式证书系统时，第一数字签名的生成方法包括：

基于椭圆曲线系统参数、汽车事件数据记录系统的隐式证书、已存储数据和第一私钥，采用无证书密码算法中的数字签名生成算法对已存储数据进行签名，生成第一数字签名
5 (r,s)。

具体的，隐式证书系统与无证书系统下第一数字签名的生成方法不同，隐式证书系统在生成第一数字签名时，是基于椭圆曲线系统参数、汽车事件数据记录系统的隐式证书、已存储数据和第一私钥，采用数字签名生成算法对已存储数据进行签名生成的，具体生成方法通过下式描述：

$$(r,s) = \text{SIGN}(\text{param}, \text{ZE}, \text{ICA} \parallel M, O, d_A)$$

10 其中，SIGN () 表示数字签名算法，param表示椭圆曲线系统参数，ZE表示空串，ICA表示EDR的隐式证书，ICA至少包括EDR的第一标识和第一公钥分量 w_A 。M表示已存储数据，O表示椭圆曲线上的一个特殊点，称为无穷远点或零点，是椭圆曲线加法群的单位元， d_A 表示第一私钥。ICA $\parallel$ M表示将隐式证书和已存储数据的字符串进行拼接。

本实施例中提供了无证书系统以及隐式证书系统的第一数字签名生成方法，针对不同的密码服务系统，可以灵活生成相应的第一数字签名。采用无证书密码算法中的数字签名生成算法，可以显著提升数字签名计算过程中的计算速率，对于EDR的算力需求较小，有利于提升EDR数据的读取速度。

EDR在对车辆行驶过程中的紧急事件进行记录时，需要确保记录的数据的真实性和唯一性。下面通过具体实施例说明EDR的数据记录方法。

20 在一些实施例中，数据安全验证方法还包括：

记录车辆的初始事件数据；

基于初始事件数据的终点时刻，采用无证书公钥密码算法中的数字签名生成算法对初始事件数据进行签名，生成时间戳，将时间戳和初始事件数据作为已存储数据。

具体的，车辆行驶过程中，当遇到紧急事件时，EDR开始记录初始数据，开始记录的时刻为起点时刻，当事件结束时，记录终点时刻，同时记录事件的持续时间。起点时刻和终点时刻均取自权威时间源。

为了确保初始事件数据的真实性，可以采用数字签名生成算法对初始事件数据的终点时刻进行签名，生成时间戳，通过时间戳可以证明初始事件数据的真实发生时刻，确保初始事件数据的真实性。将时间戳和初始事件数据共同作为已存储数据，并发送至接收端。

30 优选的，时间戳的生成方法包括：采用哈希算法对初始事件数据进行哈希计算，得到第一哈希值；

将第一哈希值和初始事件数据的终点时刻发送至时间戳服务中心，以使时间戳服务中心基于第一哈希值和终点时刻生成时间戳；

接收时间戳服务中心发送的时间戳，将时间戳和初始事件数据作为已存储数据。

35 具体的，采用哈希算法对初始数据进行计算，得到第一哈希值。将第一哈希值和初始数据的终点时刻发送至时间戳服务中心 (TimeStamp Authority, TSA)。时间戳服务中心将

初始数据和终点时刻进行绑定，并对第一哈希值和终点时刻进行签名，生成时间戳。时间戳可以作为初始数据的凭证，可以证明初始数据内容完整，未被更改。之后，时间戳服务中心将时间戳返回至汽车事件数据记录系统，汽车事件数据记录系统将时间戳和初始数据在不可删除的安全路径进行存储，作为已存储数据，并为已存储数据分配标识，便于接收端基于标识发送数据传输请求。通过本实施例的方法，为每个初始数据申请时间戳，便于后续判断已存储数据是否被篡改，为用户提供可靠的判断依据。

需要说明的是，时间戳服务器与权威的国家授时中心对接，通过与数字签名的有效结合，可为行车数据提供保密性、完整性、防抵赖等功能，通过数字签名保证内容和签发人的不可抵赖性，通过时间戳提供准确的、权威的、不可篡改的时间证明和内容完整性证明。

本申请还提供了一种数据安全验证方法，应用于接收端，参考图 4，方法包括以下步骤：
步骤 302、向汽车事件数据记录系统发送数据传输请求。

当存在针对 EDR 的数据读取需求时，用户通过接收端向 EDR 发送数据传输请求。示例性的，本实施例中的接收端为 CDR。数据传输请求中携带了待读取 EDR 数据的标识。EDR 根据 EDR 数据的标识在已存储的全部数据中查询对应的已存储数据。EDR 采用无证书密码算法中的数字签名生成算法，利用 EDR 的第一私钥对已存储数据进行签名，生成第一数字签名。第一数字签名用于验证已存储事件是否被篡改，如果被篡改，说明已存储数据为不可信数据，终止汽车事件数据记录系统与接收端之间的通信。若未被篡改，说明已存储数据为可信数据，接收端可以根据已存储数据进行后续的分析并生成分析报告。

步骤 304、接收汽车事件数据记录系统根据数据传输请求返回的第一数字签名和已存储数据。

EDR 将第一数字签名和已存储数据发送至接收端，接收端接收第一数字签名和已存储数据。在第一数字签名和已存储数据传输的过程中，已存储数据可能被篡改或未被篡改，接收端接收后，判断接收到的已存储数据是否为身份合法的 EDR 发送的未被篡改的数据。

步骤 306、采用无证书密码算法，基于已存储数据对第一数字签名进行验证。

具体的，接收端基于接收到的已存储数据对第一数字签名进行验证，验证算法采用的是无证书密码算法中的数字签名验证算法。采用对数字签名进行验证的方法能够对已存储数据的完整性和真实性验证，如果验证通过，说明已存储数据未被篡改，且数据保持完整，同时还能够确定 EDR 身份的合法性。此外，无证书密码算法还能够提升数据验证速率，进而提高 EDR 数据读取速率。接收端可以根据已存储数据进行后续的分析并生成分析报告。

下面通过实施例详细说明接收端对第一数字签名进行验证的方法。

在一些实施例中，采用无证书密码算法，基于已存储数据对第一数字签名进行验证，包括：

步骤 A，基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数和随机数计算得到汽车事件数据记录系统的第一公钥。

具体的，第一标识为 EDR 的唯一身份标识，例如 EDR 的 ID (Identity document) 或唯一可识别名称等。椭圆曲线系统参数是椭圆曲线密码系统的参数，椭圆曲线密码系统是应用 SM2 椭圆曲线公钥密码算法的系统，SM2 椭圆曲线公钥密码算法是国密算法的一种。随

机数为接收端产生的随机数。

进一步的，由于第一数字签名时 EDR 采用第一私钥进行签名生成，因此，接收端需要首先计算得到第一公钥，再根据第一公钥对第一数字签名进行验证。计算第一公钥时需要依次计算得到第二杂凑值、第三公钥分量、第一中间数，最后计算得到第一公钥。其中，

5 第二杂凑值 H_B 的计算方法可以通过下式表示：

$$H_B = H_{256}(ENTL_A \| ID_A \| a \| b \| X_G \| Y_G \| X_{Pub} \| Y_{Pub})$$

其中， $H_{256}()$ 表示消息摘要长度为 256 比特的密码杂凑算法， $ENTL_A$ 是由整数 $entlen_A$ 转换而成的两个字节， $entlen_A$ 为第一标识的比特长度， ID_A 为 EDR 的第一标识。 $a \| b$ 表示 a 与 b 的拼接，a 与 b 的数据类型可以是比特串或字符串。a、b、 X_G 、 Y_G 为椭圆曲线系统参数，
 10 a 与 b 为椭圆曲线方程参数， (X_G, Y_G) 为 G 的坐标，G 表示椭圆曲线公钥密码算法中椭圆曲线的一个基点。 (X_{Pub}, Y_{Pub}) 为 P_{Pub} 的坐标， P_{Pub} 为密码服务系统的主公钥。 X_G 、 Y_G 、 X_{Pub} 、 Y_{Pub} 的数据类型均为比特串。

第三公钥分量的计算方法还可以通过下式表示：

$$w_B = [w]G + U_B$$

其中， U_B 为第四公钥分量， $U_B = [d'_B]G$ 。 $[d'_B]G$ 表示椭圆曲线上点 G 的 d'_B 倍点，即
 15 $[d'_B]G = G + G + \dots + G$ ，等式右边 G 的数量为 d'_B 个， d'_B 为正整数。 d'_B 为接收端生成的随机数， $d'_B \in [1, n-1]$ 。 $[w]G$ 表示椭圆曲线上点 G 的 w 倍点，即 $[w]G = G + G + \dots + G$ ，等式右边 G 的数量为 w 个， w 为正整数。 w 为密码服务系统产生的随机数， $w \in [1, n-1]$ 。G 表示椭圆曲线的一个基点，其阶为素数，n 表示基点 G 的阶。

第一中间数的计算方法包括：对第二杂凑值 H_B 和第三公钥分量 w_B 拼接后生成的字符串
 20 进行密码杂凑计算，得到第三杂凑值；对第三杂凑值进行模运算，以得到第一中间数。

第三杂凑值的具体计算方法通过下式表示：

$$H_{B'} = H_{256}(x_{w_B} \| y_{w_B} \| H_B)$$

进一步的，第一中间数 λ' 的具体计算方法通过下式表示：

$$\lambda' = H_{B'} \bmod n = H_{256}(x_{w_B} \| y_{w_B} \| H_B) \bmod n$$

其中， (x_{w_B}, y_{w_B}) 为 w_B 的坐标。

确定了第二杂凑值、第三公钥分量、第一中间数后，计算第一公钥，第一公钥的计算
 25 方法表示为： $P_B = w_B + [\lambda']P_{Pub}$ ，由此计算得到 EDR 的第一公钥。

步骤 B，基于第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一公钥，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证。

在无证书系统和隐式证书系统中，数字签名的生成方法不同，响应的，对于数字签名的验证方法也不同。下面分别对无证书系统和隐式证书系统中，数字签名的验证过程进行
 30 说明。

进一步的，参考图 5，当密码服务系统为无证书系统时，对第一数字签名进行验证的方法，包括：

步骤 402、对第一标识、椭圆曲线系统参数和密码服务系统的主公钥拼接后生成的字符串进行密码杂凑计算，得到第二杂凑值。

步骤 404、计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第三公钥分量。

具体的，当对第一数字签名进行验证时，需要依次计算得到第二杂凑值、第三公钥分量，然后再对第一数字签名进行验证。其中，步骤 402 和步骤 404 中，对于第二杂凑值和第三公钥分量的计算方法同前述步骤 A，此处不再赘述。

步骤 406、利用椭圆曲线系统参数、第二杂凑值、第三公钥分量、已存储数据和第一公钥，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证。

具体的，通过前述步骤计算得到第二杂凑值、第三公钥分量后，通过下式对第一数字签名进行验证，验证后输出验证结果：

$$\text{VERIFY}(\text{param}, H_B, x_{w_B} \parallel y_{w_B} \parallel M, P_B, (r, s))$$

10 其中，param 表示椭圆曲线系统参数， (x_{w_B}, y_{w_B}) 为 w_B 的坐标， P_B 表示第一公钥， (r, s) 表示第一签名。若输出结果正确，则表示已存储数据未被篡改，EDR 身份具有合法性，若输出结果为不正确，则表示已存储数据被篡改或 EDR 身份不合法。

进一步的，当密码服务系统为隐式证书系统时，对第一数字签名进行验证的方法，包括：

15 基于椭圆曲线系统参数、汽车事件数据记录系统的隐式证书、已存储数据和第一公钥，采用无证书密码算法中的数字签名验证算法，对第一数字签名进行验证。

具体的，在隐式证书系统中，需要根据椭圆曲线系统参数、汽车事件数据记录系统的隐式证书、已存储数据和第一公钥，对第一数字签名进行验证。

进一步的，通过下式描述在隐式证书系统中对第一数字签名进行验证的方法，验证后
20 输出验证结果：

$$\text{VERIFY}(\text{param}, ZE, ICA \parallel M, P_B, (r, s))$$

其中，param 表示椭圆曲线系统参数，ZE 表示空串，ICA 表示 EDR 的隐式证书，至少包括 EDR 的第一标识和第一公钥分量， P_B 表示第一公钥， (r, s) 表示第一签名。

若输出结果正确，则表示已存储数据未被篡改，EDR 身份具有合法性，若输出结果不正确，则表示已存储数据被篡改或 EDR 身份不合法。

25 本实施例中分别提供了无证书系统以及隐式证书系统的第一数字签名验证方法，针对不同的密码服务系统，可以灵活的对第一数字签名进行验证。采用无证书密码算法中的数字签名验证算法，可以显著提升数字签名验证过程中的计算速率，对于 EDR 的算力需求较小，有利于提升 EDR 数据的读取速度。

需要说明的是，本申请实施例的方法可以由单个设备执行，例如一台计算机或服务器
30 等。本实施例的方法也可以应用于分布式场景下，由多台设备相互配合来完成。在这种分布式场景的情况下，这多台设备中的一台设备可以只执行本申请实施例的方法中的某一个或多个步骤，这多台设备相互之间会进行交互以完成所述的方法。

需要说明的是，上述对本申请的一些实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于上述实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求
35

示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

基于同一技术构思，与上述任意实施例方法相对应的，本申请还提供了一种数据安全验证装置。

5 参考图 6，数据安全验证装置，应用于汽车事件数据记录系统，包括：

确定模块 502，被配置为响应于接收到接收端发送的数据传输请求，确定与数据传输请求关联的已存储数据；

签名模块 504，被配置为采用无证书密码算法，利用汽车事件数据记录系统的第一私钥对已存储数据进行签名，生成第一数字签名；

10 发送模块 506，被配置为将第一数字签名和已存储数据发送至接收端，以使接收端基于已存储数据对第一数字签名进行验证。

在一些实施例中，签名模块 504，还被配置为基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一私钥，采用无证书密码算法中的数字签名生成算法，生成第一数字签名。

15 在一些实施例中，若密码服务系统为无证书系统，签名模块 504，还被配置为

对第一标识、椭圆曲线系统参数和密码服务端的主公钥拼接后生成的字符串进行密码杂凑计算，得到第一杂凑值；

计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第一公钥分量；

20 利用椭圆曲线系统参数、第一杂凑值、第一公钥分量和第一私钥，采用无证书密码算法中的数字签名生成算法对已存储数据进行签名，生成第一数字签名。

在一些实施例中，签名模块 504，还被配置为计算椭圆曲线系统参数和随机数的乘积，对该乘积和椭圆曲线系统参数的倍数进行求和运算，得到汽车事件数据记录系统的第一公钥分量。

25 在一些实施例中，若密码服务系统为隐式证书系统，签名模块 504，还被配置为利用椭圆曲线系统参数、汽车事件数据记录系统的隐式证书和第一私钥，采用无证书密码算法中的数字签名生成算法对已存储数据进行签名，生成第一数字签名。在一些实施例中，还包括存储模块 508，存储模块 508，被配置为记录车辆的初始事件数据；基于初始事件数据的终点时刻，采用无证书公钥密码算法中的数字签名生成算法对初始事件数据进行签名，生成时间戳，将时间戳和初始事件数据作为已存储数据。

30 在一些实施例中，存储模块 508，被配置为采用哈希算法对初始事件数据进行哈希计算，得到第一哈希值；将第一哈希值和初始事件数据的终点时刻发送至时间戳服务中心，以使时间戳服务中心基于第一哈希值和终点时刻生成时间戳。

35 基于同一技术构思，与上述任意实施例方法相对应的，本申请还提供了一种数据安全验证装置。

参考图 7，数据安全验证装置，应用于事故数据恢复设备，包括：

请求模块 602，被配置为向汽车事件数据记录系统发送数据传输请求；

接收模块 604, 被配置为接收汽车事件数据记录系统根据数据传输请求返回的第一数字签名和已存储数据;

验证模块 606, 被配置为采用无证书密码算法, 基于已存储数据对第一数字签名进行验证。

5 在一些实施例中, 验证模块 606, 还被配置为基于汽车事件数据记录系统的第一标识、椭圆曲线系统参数和随机数计算得到汽车事件数据记录系统的第一公钥; 基于第一标识、椭圆曲线系统参数、随机数、已存储数据和/或第一公钥, 采用无证书密码算法中的数字签名验证算法, 对第一数字签名进行验证。在一些实施例中, 若密码服务系统为无证书系统, 验证模块 606, 还被配置为对第一标识、椭圆曲线系统参数和服务端的主公钥拼接后生成的
10 字符串进行密码杂凑计算, 得到第二杂凑值;

计算椭圆曲线系统参数和随机数的乘积, 对该乘积和椭圆曲线系统参数的倍数进行求运算, 得到汽车事件数据记录系统的第三公钥分量;

利用椭圆曲线系统参数、第二杂凑值、第三公钥分量、已存储数据和第一公钥, 采用无证书密码算法中的数字签名验证算法, 对第一数字签名进行验证。

15 在一些实施例中, 若密码服务系统为隐式证书系统, 验证模块 606, 还被配置为利用椭圆曲线系统参数、汽车事件数据记录系统的隐式证书、已存储数据和第一公钥, 采用无证书密码算法中的数字签名验证算法, 对第一数字签名进行验证。

为了描述的方便, 描述以上装置时以功能分为各种模块分别描述。当然, 在实施本申请时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

20 上述实施例的装置用于实现前述任一实施例中相应的数据安全验证方法, 并且具有相应的方法实施例的有益效果, 在此不再赘述。

基于同一技术构思, 与上述任意实施例方法相对应的, 本申请还提供了一种汽车事件数据记录系统, 包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序, 处理器执行程序时实现上任意如上第一方面所述的数据安全验证方法。

25 基于同一技术构思, 与上述任意实施例方法相对应的, 本申请还提供了一种事故数据恢复设备, 包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序, 处理器执行程序时实现如第二方面所述的数据安全传输方法。

图 8 示出了本实施例所提供的一种更为具体的电子设备(汽车事件数据记录系统或事故数据恢复设备)硬件结构示意图, 该设备可以包括: 处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出
30 接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

处理器 1010 可以采用通用的 CPU (Central Processing Unit, 中央处理器)、微处理器、应用专用集成电路 (Application Specific Integrated Circuit, ASIC)、或者一个或多个集成电路等方式实现, 用于执行相关程序, 以实现本说明书实施例所提供的技术方案。

35 存储器 1020 可以采用 ROM (Read Only Memory, 只读存储器)、RAM (Random Access Memory, 随机存取存储器)、静态存储设备, 动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序, 在通过软件或者固件来实现本说明书实施例所提供的技术

方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/ 模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040）之间传输信息。

需要说明的是，尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

上述实施例的电子设备用于实现前述任一实施例中相应的数据安全验证方法，并且具有相应的方法实施例的有益效果，在此不再赘述。

基于同一技术构思，与上述任意实施例方法相对应的，本申请还提供了一种非暂态计算机可读存储介质，非暂态计算机可读存储介质存储计算机指令，计算机指令用于使计算机执行如上任一实施例所述的数据安全验证方法。

本实施例的计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带、磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。

上述实施例的存储介质存储的计算机指令用于使所述计算机执行如上任一实施例所述的数据安全验证方法，并且具有相应的方法实施例的有益效果，在此不再赘述。

所属领域的普通技术人员应当理解：以上任何实施例的讨论仅为示例性的，并非旨在暗示本申请的范围（包括权利要求）被限于这些例子；在本申请的思路下，以上实施例或者不同实施例中的技术特征之间也可以进行组合，步骤可以以任意顺序实现，并存在如上所述的本申请实施例的不同方面的许多其它变化，为了简明它们没有在细节中提供。

另外，为简化说明和讨论，并且为了不会使本申请实施例难以理解，在所提供的附图中可以示出或不示出与集成电路（IC）芯片和其它部件的公知的电源/接地连接。此外，可以以框图的形式示出装置，以便避免使本申请实施例难以理解，并且这也考虑了以下事实，即关于这些框图装置的实施方式的细节是高度取决于将要实施本申请实施例的平台的

(即, 这些细节应当完全处于本领域技术人员的理解范围内)。在阐述了具体细节(例如, 电路)以描述本申请的示例性实施例的情况下, 对本领域技术人员来说显而易见的是, 可以在没有这些具体细节的情况下或者这些具体细节有变化的情况下实施本申请实施例。因此, 这些描述应被认为是说明性的而不是限制性的。

5 尽管已经结合了本申请的具体实施例对本申请进行了描述, 但是根据前面的描述, 这些实施例的很多替换、修改和变型对本领域普通技术人员来说将是显而易见的。例如, 其它存储器架构(例如, 动态 RAM (DRAM))可以使用所讨论的实施例。

10 本申请实施例旨在涵盖落入所附权利要求的宽泛范围之内的所有这样的替换、修改和变型。因此, 凡在本申请实施例的精神和原则之内, 所做的任何省略、修改、等同替换、改进等, 均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种数据安全验证方法，其特征在于，应用于汽车事件数据记录系统，所述方法包括：

采用无证书密码算法，利用所述汽车事件数据记录系统的第一私钥对已存储数据进行
5 签名，生成第一数字签名；

响应于接收到接收端发送的数据传输请求，确定与所述数据传输请求关联的已存储数据；

将与所述数据传输请求关联的第一数字签名和已存储数据发送至所述接收端，以使所述接收端基于所述已存储数据对接收到的第一数字签名进行验证。

10 2. 根据权利要求 1 所述的方法，其特征在于，所述采用无证书密码算法，利用所述汽车事件数据记录系统的第一私钥对所述已存储数据进行签名，生成第一数字签名，包括：

基于所述汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、所述已存储数据和/或所述第一私钥，采用无证书密码算法中的数字签名生成算法，生成所述第一数字签名。

15 3. 根据权利要求 2 所述的方法，其特征在于，若密码服务系统为无证书系统，所述基于所述汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、所述已存储数据和/或所述第一私钥，采用无证书密码算法中的数字签名生成算法，生成所述第一数字签名，包括：

20 基于所述第一标识、所述椭圆曲线系统参数和所述密码服务系统的主公钥进行密码杂凑计算，得到第一杂凑值；

基于所述椭圆曲线系统参数和所述随机数，计算得到所述汽车事件数据记录系统的第一公钥分量；

25 利用所述椭圆曲线系统参数、所述第一杂凑值、所述第一公钥分量和所述第一私钥，采用无证书密码算法中的数字签名生成算法对所述已存储数据进行签名，生成所述第一数字签名。

4. 根据权利要求 3 所述的方法，其特征在于，所述基于所述椭圆曲线系统参数和所述随机数，计算得到所述汽车事件数据记录系统的第一公钥分量，包括：

计算所述椭圆曲线系统参数和所述随机数的乘积，对该乘积和所述椭圆曲线系统参数的倍数进行求和运算，得到所述汽车事件数据记录系统的第一公钥分量。

30 5. 根据权利要求 2 所述的方法，其特征在于，若密码服务系统为隐式证书系统，所述基于所述汽车事件数据记录系统的第一标识、椭圆曲线系统参数、随机数、所述已存储数据和/或所述第一私钥，采用无证书密码算法中的数字签名生成算法，生成所述第一数字签名，包括：

35 利用所述椭圆曲线系统参数、所述汽车事件数据记录系统的隐式证书和所述第一私钥，采用无证书密码算法中的数字签名生成算法对所述已存储数据进行签名，生成所述第一数字签名。

6. 根据权利要求1所述的方法, 其特征在于, 所述方法还包括:

记录车辆的初始事件数据;

基于所述初始事件数据的终点时刻, 采用无证书公钥密码算法中的数字签名生成算法对所述初始事件数据进行签名, 生成时间戳, 将所述时间戳和所述初始事件数据作为所述
5 已存储数据。

7. 根据权利要求6所述的方法, 其特征在于, 所述基于所述初始事件数据的终点时刻, 采用无证书公钥密码算法中的数字签名生成算法对所述初始事件数据进行签名, 生成时间戳, 包括:

采用哈希算法对所述初始事件数据进行哈希计算, 得到第一哈希值;

10 将所述第一哈希值和所述初始事件数据的终点时刻发送至时间戳服务中心, 以使所述时间戳服务中心基于所述第一哈希值和所述终点时刻生成时间戳。

8. 一种数据安全验证方法, 其特征在于, 应用于接收端, 所述方法包括:

向汽车事件数据记录系统发送数据传输请求;

15 接收所述汽车事件数据记录系统根据所述数据传输请求返回的第一数字签名和已存储数据;

采用无证书密码算法, 基于所述已存储数据对所述第一数字签名进行验证。

9. 根据权利要求8所述的方法, 其特征在于, 所述采用无证书密码算法, 基于所述已存储数据对所述第一数字签名进行验证, 包括:

20 基于所述汽车事件数据记录系统的第一标识、椭圆曲线系统参数和随机数计算得到所述汽车事件数据记录系统的第一公钥;

基于所述第一标识、所述椭圆曲线系统参数、随机数、所述已存储数据和/或所述第一公钥, 采用无证书密码算法中的数字签名验证算法, 对所述第一数字签名进行验证。

10. 根据权利要求9所述的方法, 其特征在于, 若密码服务系统为无证书系统时, 所述采用无证书密码算法中的数字签名验证算法, 对所述第一数字签名进行验证, 包括:

25 对所述第一标识、所述椭圆曲线系统参数和所述密码服务系统的主公钥拼接后生成的字符串进行密码杂凑计算, 得到第二杂凑值;

计算所述椭圆曲线系统参数和所述随机数的乘积, 对该乘积和所述椭圆曲线系统参数的倍数进行求和运算, 得到所述汽车事件数据记录系统的第三公钥分量;

30 利用所述椭圆曲线系统参数、所述第二杂凑值、所述第三公钥分量、所述已存储数据和所述第一公钥, 采用无证书密码算法中的数字签名验证算法, 对所述第一数字签名进行验证。

11. 一种数据安全验证装置, 其特征在于, 应用于汽车事件数据记录系统, 所述装置包括: 处理器, 其中, 所述处理器用于执行存储在存储器中的以下程序模块:

35 确定模块, 被配置为采用无证书密码算法, 利用所述汽车事件数据记录系统的第一私钥对已存储数据进行签名, 生成第一数字签名;

签名模块, 被配置为响应于接收到接收端发送的数据传输请求, 确定与所述数据传输请求关联的已存储数据;

发送模块，被配置为将与所述数据传输请求关联的第一数字签名和已存储数据发送至所述接收端，以使所述接收端基于所述已存储数据对接收到的第一数字签名进行验证。

12. 一种数据安全验证装置，其特征在于，应用于事故数据恢复设备，所述装置包括：处理器，其中，所述处理器用于执行存储在存储器中的以下程序模块：

5 请求模块，被配置为向汽车事件数据记录系统发送数据传输请求；

接收模块，被配置为接收所述汽车事件数据记录系统根据所述数据传输请求返回的第一数字签名和已存储数据；

验证模块，被配置为采用无证书密码算法，基于所述已存储数据对所述第一数字签名进行验证。

10 13. 一种汽车事件数据记录系统，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求 1 至 5 任意一项所述的方法。

14. 一种事故数据恢复设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求 6 至 7 任意一项所述的方法。

15 15. 一种车辆，其特征在于，所述车辆包括如权利要求 8 所述的汽车事件数据记录系统。

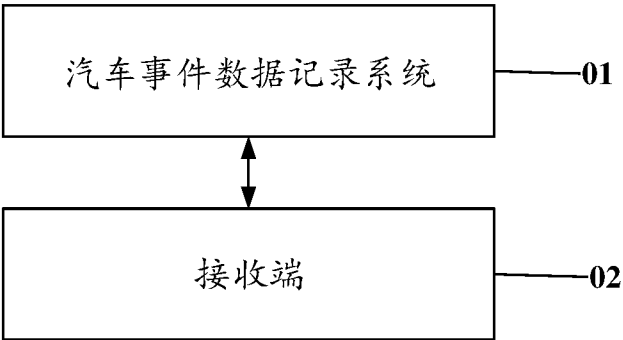


图 1

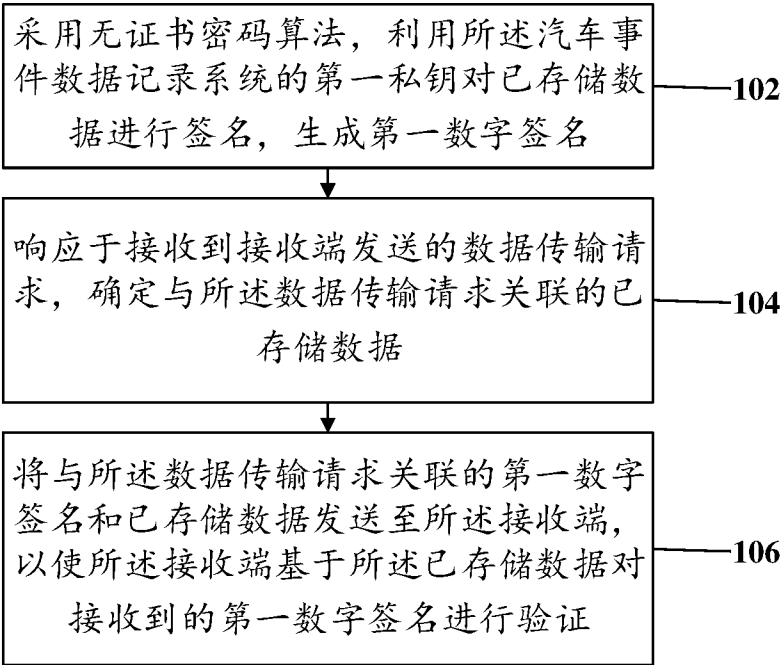


图 2

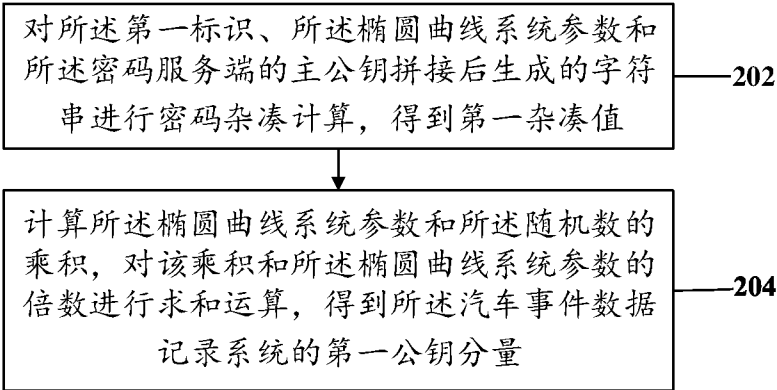


图 3

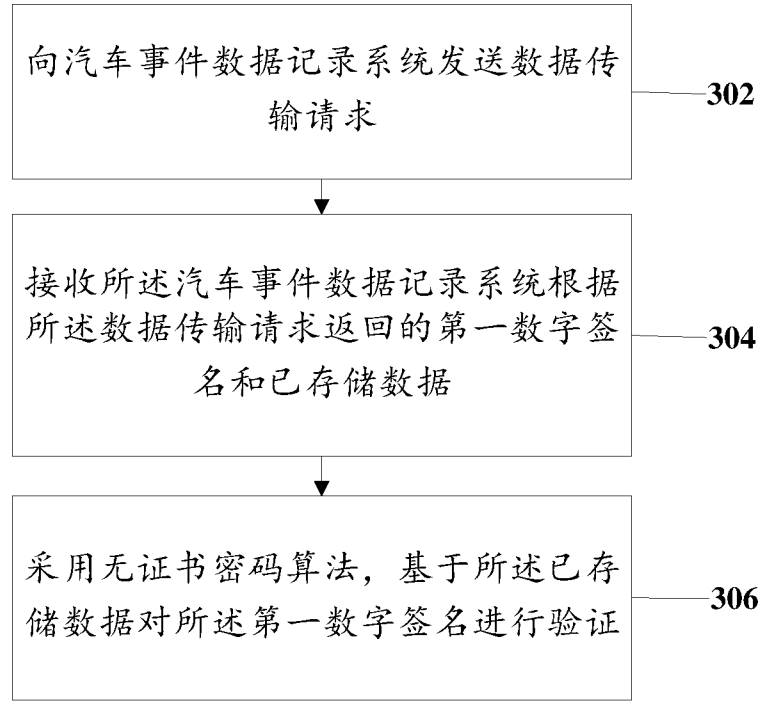


图 4

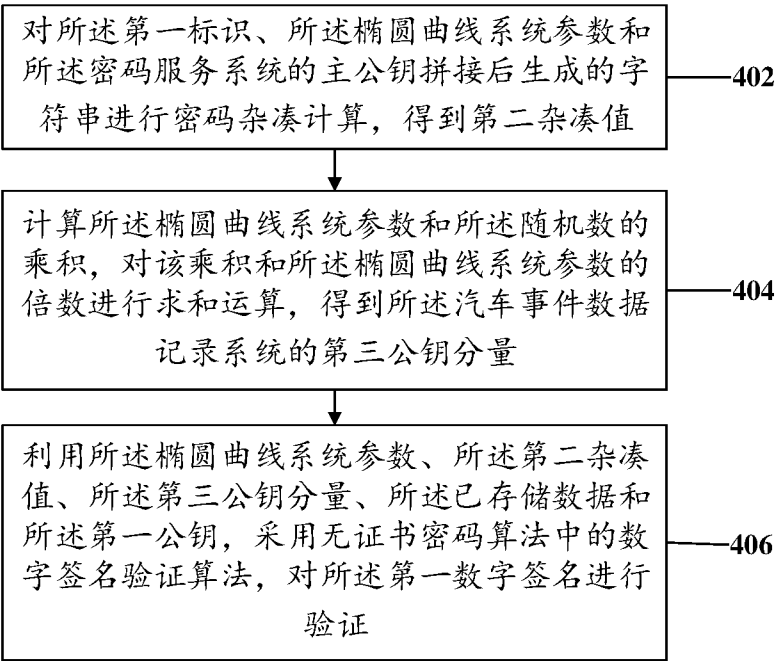


图 5

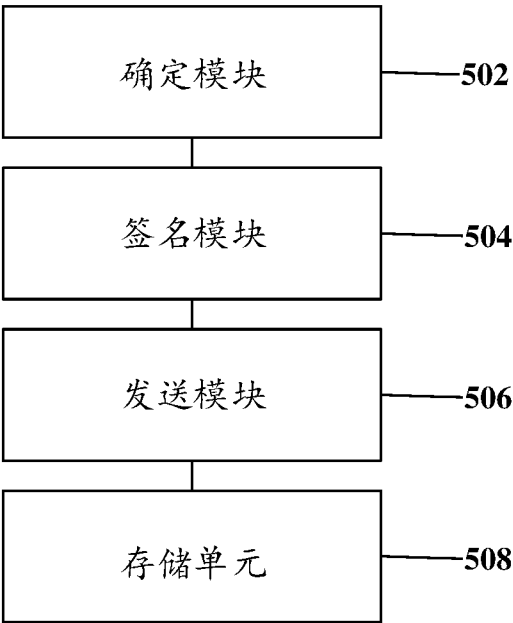


图 6

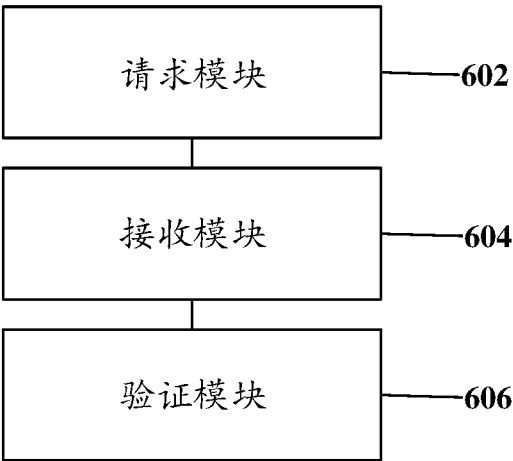


图 7

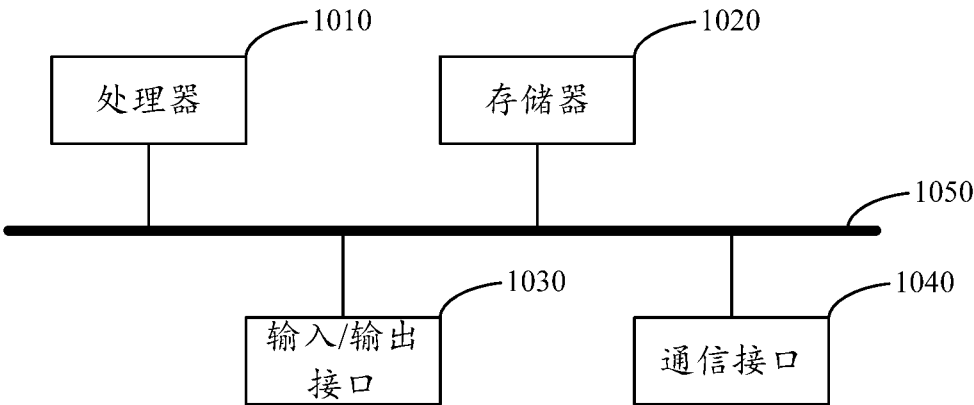


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/136887

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)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 G06F G07C

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)

CNTXT, ENTXTC, VEN: 车辆, 避免, 篡改, 存储, 签名, 私钥, 加密, 椭圆曲线, 完整性, 隐式, 证书, 验证, EDR, car, avoid, juggle, memory, signature, key, encrypt, ellipse, curve, integrality, implicit, certificate, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 117768181 A (GREAT WALL MOTOR CO., LTD.) 26 March 2024 (2024-03-26) claims 1-10	1-15
PX	CN 117768177 A (GREAT WALL MOTOR CO., LTD.) 26 March 2024 (2024-03-26) claims 1-10	1-15
PX	CN 117768176 A (GREAT WALL MOTOR CO., LTD.) 26 March 2024 (2024-03-26) claims 1-10	1-15
PX	CN 117763040 A (GREAT WALL MOTOR CO., LTD.) 26 March 2024 (2024-03-26) claims 1-10	1-15
X	CN 116631093 A (MERCEDES-BENZ GROUP AG) 22 August 2023 (2023-08-22) description, paragraphs 7-42, and figure 1	1-15
A	CN 109815732 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 28 May 2019 (2019-05-28) entire document	1-15
A	CN 112367175 A (XIDIAN UNIVERSITY) 12 February 2021 (2021-02-12) entire document	1-15



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

04 March 2025

Date of mailing of the international search report

11 March 2025

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/136887

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2023231782 A1 (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 07 December 2023 (2023-12-07) entire document	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/136887

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	117768181	A	26 March 2024	None		
CN	117768177	A	26 March 2024	None		
CN	117768176	A	26 March 2024	None		
CN	117763040	A	26 March 2024	None		
CN	116631093	A	22 August 2023	None		
CN	109815732	A	28 May 2019	None		
CN	112367175	A	12 February 2021	None		
WO	2023231782	A1	07 December 2023	CN	114826772	A 29 July 2022

A. 主题的分类

H04L 9/40(2022.01)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 G06F G07C

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))

CNTEXT,ENTXTC,VEN:车辆, 避免, 篡改, 存储, 签名, 私钥, 加密, 椭圆曲线, 完整性,隐式, 证书, 验证, EDR, car, avoid, juggle, memory, signature, key, encrypt, ellipse, curve, integrity, implicit, certificate, validate

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 117768181 A (长城汽车股份有限公司) 2024年3月26日 (2024 - 03 - 26) 权利要求1-10	1-15
PX	CN 117768177 A (长城汽车股份有限公司) 2024年3月26日 (2024 - 03 - 26) 权利要求1-10	1-15
PX	CN 117768176 A (长城汽车股份有限公司) 2024年3月26日 (2024 - 03 - 26) 权利要求1-10	1-15
PX	CN 117763040 A (长城汽车股份有限公司) 2024年3月26日 (2024 - 03 - 26) 权利要求1-10	1-15
X	CN 116631093 A (梅赛德斯-奔驰集团股份公司) 2023年8月22日 (2023 - 08 - 22) 说明书第7-42段和附图1	1-15
A	CN 109815732 A (北京邮电大学) 2019年5月28日 (2019 - 05 - 28) 全文	1-15
A	CN 112367175 A (西安电子科技大学) 2021年2月12日 (2021 - 02 - 12) 全文	1-15

☒ 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

2025年3月4日

国际检索报告邮寄日期

2025年3月11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

授权官员

郭婧

电话号码 (+86) 010-53961671

PCT/ISA/210 表(第2页) (2022年7月)

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
A	WO 2023231782 A1 (CHINA UNITED NETWORK COMMUNICATIONS GROUP COMPANY LTD.) 2023年12月7日 (2023 - 12 - 07) 全文	1-15

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/136887

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	117768181	A	2024年3月26日	无	
CN	117768177	A	2024年3月26日	无	
CN	117768176	A	2024年3月26日	无	
CN	117763040	A	2024年3月26日	无	
CN	116631093	A	2023年8月22日	无	
CN	109815732	A	2019年5月28日	无	
CN	112367175	A	2021年2月12日	无	
WO	2023231782	A1	2023年12月7日	CN 114826772	A 2022年7月29日