(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
2022 年 1 月 27 日 (27.01.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/017103 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2021/101481

(22) 国际申请日: 2021 年 6 月 22 日 (22.06.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010696213.8 2020年7月20日 (20.07.2020) CN

(71) 申请人: 广州汽车集团股份有限公司 (**GUANGZHOU AUTOMOBILE GROUP CO., LTD.**) [CN/CN]; 中国广东省广州市越秀区东风中路 448-458 号成悦大厦 23 楼, Guangdong 510030 (CN)。

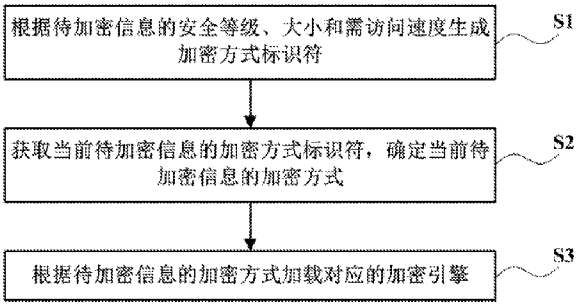
(72) 发明人: 张殷华 (**ZHANG, Yinhua**); 中国广东省广州市番禺区化龙镇金山大道东路 668 号, Guangdong 511434 (CN)。 鲁文峰 (**LU, Wenfeng**); 中国广东省广州市番禺区化龙镇金山大道东路668号, Guangdong 511434 (CN)。 刘金钊 (**LIU, Jinzhao**); 中国广东省广州市番禺区化龙镇金山大道东路668号, Guangdong 511434 (CN)。

(74) 代理人: 深圳汇智容达专利商标事务所（普通合伙）(**SHENZHEN RONDA PATENT AND TRADEMARK LAW OFFICE**); 中国广东省深圳市福田区深南中路求是大厦东座2709-2711, Guangdong 518040 (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, IT, 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,

(54) **Title:** METHOD FOR DYNAMICALLY LOADING ENCRYPTION ENGINE

(54) 发明名称: 一种动态加载加密引擎的方法



S1 GENERATE AN ENCRYPTION MODE IDENTIFIER ACCORDING TO THE SECURITY LEVEL, THE SIZE AND A REQUIRED ACCESS SPEED OF INFORMATION TO BE ENCRYPTED
S2 ACQUIRE THE ENCRYPTION MODE IDENTIFIER OF THE CURRENT INFORMATION TO BE ENCRYPTED, AND DETERMINE AN ENCRYPTION MODE OF THE CURRENT INFORMATION TO BE ENCRYPTED
S3 LOAD A CORRESPONDING ENCRYPTION ENGINE ACCORDING TO THE ENCRYPTION MODE OF THE INFORMATION TO BE ENCRYPTED

图 1

(57) **Abstract:** Disclosed is a method for dynamically loading an encryption engine. The method comprises: step S1, generating an encryption mode identifier according to the security level, the size and a required access speed of information to be encrypted; step S2, acquiring the encryption mode identifier of the current information to be encrypted, and determining an encryption mode of the current information to be encrypted; and step S3, loading a corresponding encryption engine according to the encryption mode of the current information to be encrypted. According to characteristics of different information, two encryption modes, i.e. a soft encryption mode and a hard encryption mode, are designed to be simultaneously present on the same system, and the two encryption modes are dynamically loaded according to the content and the condition of the information, such that not only are the respective advantages of a soft encryption technique and a hard encryption technique utilized, but the disadvantages thereof are also avoided, thereby increasing the encryption strength of highly confidential information and the access speed of non-highly confidential information, reducing resource waste, and improving resource encryption and decryption efficiency.

WO 2022/017103 A1

[见续页]

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, 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, 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：本发明公开一种动态加载加密引擎的方法，包括：步骤S1，根据待加密信息的安全等级、大小和需访问速度生成加密方式标识符；步骤S2，获取当前待加密信息的加密方式标识符，确定当前待加密信息的加密方式；步骤S3，根据当前待加密信息的加密方式加载对应的加密引擎。本发明根据不同信息的特点，在同一个系统上设计同时存在两种加密方式——软加密方式和硬加密方式，根据信息的内容和情况动态加载两种加密方式，从而既利用了软加密技术和硬加密技术各自的优点，也避免了其缺点，提高了高密信息的加密强度和非高密信息的访问速度，同时减少了资源的浪费，增加了资源的加解密效率。

一种动态加载加密引擎的方法

相关申请

本申请要求于 2020 年 7 月 20 日提交中国国家知识产权局、申请号为 CN202010696213.8、发明名称为“一种动态加载加密引擎的方法”的中国专利申请的优先权，上述专利的全部内容通过引用结合在本申请中。

技术领域

本发明涉及车联网通信安全技术领域，尤其涉及一种动态加载加密引擎的方法。

背景技术

目前在车联网通信安全领域的加密技术主要有两种：软加密技术和硬加密技术。软加密指不需要额外硬件的软件保护方式，一般采取序列号或许可证文件的授权方式。通常软加密方案采用与计算机软硬件特征绑定的方式，如 CPU、BIOS、硬盘、MAC、计算机名、用户名等，因为没有使用额外的硬件设备，被认为是一种“软加密”方案。软加密的安全强度没有硬加密高，但也具有诸多优点，例如：没有硬件和物流，加解密速度快，可实现软件的电子化发行；易于管理和维护，有助于提高授权效率和改善用户体验；降低软件开发商整体的软件保护、发行和管理成本，提高其竞争力。

硬加密是指需要额外硬件设备的软件保护技术，目前主要的硬加密方案是加密锁技术。根据加密锁所用 CPU 的不同分为普通加密锁和智能卡加密锁。硬件加密具有比较高的安全强度，但也有不少缺点，例如：适用于传统的一次性永久授权，无法方便实现试用版本和按需购买；硬件的存在带来了生产、初始化、物流、安装和维护的成本；无法实现基于互联网的电子化发行；安装驱动和客户端组件以及额外的硬件设备影响了客户的使用体验，难以进行升级、跟踪及售后管理。

目前行业都是在一个产品上设计一种加密方法进行，要么是使用软加密，要么是使用硬加密。在软加密的情况下，如上所述，信息的安全等级不是很高，但是有些高密信息需要更高安全等级的加密方式，这样就会造成信息的不安全性。在硬件加密情况下，部分信息需要的安全等级较低，如果都用硬

加密技术会导致资源的浪费及加密时间的增加。

综上所述，现有的技术方案存在要么加密安全等级不够，要么造成资源的浪费和加解密时间的增加的缺点，难以做到各方面都满足要求。

发明内容

本发明实施例所要解决的技术问题在于，提供一种动态加载加密引擎的方法，对不同的信息采用不同的加密方式，既满足信息的加密需求，又可减少资源浪费，增加资源的加解密效率。

为解决上述技术问题，本发明提供一种动态加载加密引擎的方法，包括：

步骤 S1，根据待加密信息的安全等级、大小和需访问速度生成加密方式标识符，其中，所述加密方式标识符包括软加密标识符和硬加密标识符，所述软加密标识符用于标识所述待加密信息须采用软加密方式，所述硬加密标识符用于标识所述待加密信息须采用硬加密方式；

步骤 S2，获取当前待加密信息的加密方式标识符，确定当前待加密信息的加密方式；

步骤 S3，根据当前待加密信息的加密方式加载对应的加密引擎。

进一步地，所述安全等级包括安全等级高和安全等级低两种类型，所述待加密信息的大小通过与存储空间阈值的比较，包括存储空间大和存储空间小两种类型，所述待加密信息的需访问速度通过与访问速度阈值的比较，包括需访问速度快和需访问速度慢两种类型。

进一步地，所述步骤 S1 中生成加密方式标识符具体是：对于同时满足安全等级低、存储空间小、需访问速度快的待加密信息生成软加密标识符，其它待加密信息则生成硬加密标识符。

进一步地，所述存储空间阈值设为 500k，大于或等于 500k 的待加密信息属于存储空间大的信息，小于 500k 的待加密信息属于存储空间小的信息；所述访问速度阈值设为 100ms，大于或等于 100ms 的待加密信息属于需访问速度慢的信息，小于 100ms 的待加密信息属于需访问速度快的信息。

进一步地，所述步骤 S2 获取当前待加密信息的加密方式标识符的方式包括：直接读取携带在所述当前待加密信息中的加密方式标识符；或者查询由各待加密信息及其加密方式标识符形成的表格。

进一步地，所述步骤 S3 根据所述步骤 S2 确定的当前待加密信息的加密方式，加载软加密引擎或者硬加密引擎，加载软加密引擎的步骤包括：

进行芯片引擎初始化；

生成芯片秘钥；

加载芯片密钥。

进一步地，所述进行芯片引擎初始化的步骤包括：

调用 SSL 协议初始化函数，然后使用引擎加载函数构造芯片引擎；

调用初始化引擎名函数将构造的所述芯片引擎与索引绑定；

调用加密算法注册函数将所述芯片引擎的加密算法注册到 openssl 引擎中；

调用引擎设置函数将所述芯片引擎的加密算法设置默认为 RSA 方法。

进一步地，所述生成芯片秘钥的步骤包括：

调用密钥生成函数生成密钥对；

判断软加密引擎中是否存在获取密钥的方法，如果存在，则进一步调用内置密钥生成器生成密钥，然后直接返回密钥结构；如果不存在，则调用芯片引擎中的获取密钥方法，通过软算法生成伪私钥，再进一步调用芯片获取密钥接口获取密钥对里的 N 和 E，然后判断芯片密钥是否生成成功，若成功则替换软算法生成的伪密钥中的 N 和 E 并返回密钥结构，若失败则返回错误返回码。

进一步地，所述加载芯片密钥的步骤包括：

调用密钥加载函数读取跟随车辆数字证书一起下载的软密钥文件，并判断是否读取成功；如果读取失败，则新建密钥文件并将默认密钥信息写入到所述软密钥文件，然后将获取的密钥文件句柄传入，构造用于存放非对称密钥信息的 EVP_PKEY 结构；如果读取成功则将获取的密钥文件句柄传入，构造 EVP_PKEY 结构；

调用芯片查询密钥接口获取密钥对里的 N 和 E，并判断是否获取成功，若成功，则将从芯片返回的 N 和 E 替换到软密钥生成的 EVP_PKEY 结构中，然后返回 EVP_PKEY 结构，若失败则返回空指针。

进一步地，加载硬加密引擎的步骤包括：

加载硬加密引擎；

通过随机函数产生随机数，将随机数发送给硬加密引擎；

硬加密引擎加载加密算法引擎对随机数进行加密；

将加密结果发送给解密引擎解密；

将解密结果与通过随机函数产生的随机数进行比对，判断是否通过验证。

实施本发明具有如下有益效果：本发明根据不同信息的特点，在同一个系统上设计同时存在两种加密方式——软加密方式和硬加密方式，根据信息的内容和情况动态加载两种加密方式，从而既利用了软加密技术和硬加密技术各自的优点，也避免了其缺点，提高了高密信息的加密强度和非高密信息的访问速度，同时减少了资源的浪费，增加了资源的加解密效率。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有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发明的一些实施例，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 为本发明实施例一种动态加载加密引擎的方法的流程示意图。

图 2 为本发明实施例中加载软加密引擎的流程示意图。

图 3 为本发明实施例中芯片引擎初始化的流程示意图。

图 4 为本发明实施例中生成密钥的流程示意图。

图 5 为本发明实施例中加载芯片密钥的流程示意图。

图 6 为本发明实施例中加载硬加密引擎的流程示意图。

具体实施方式

以下各实施例的说明是参考附图，用以示例本发明可以用以实施的特定实施例。

请参照图 1 所示，本发明实施例提供一种动态加载加密引擎的方法，包括：

步骤 S1，根据待加密信息的安全等级、大小和需访问速度生成加密方式标识符，其中，所述加密方式标识符包括软加密标识符和硬加密标识符，所述软加密标识符用于标识所述待加密信息须采用软加密方式，所述硬加密

标识符用于标识所述待加密信息须采用硬加密方式；

步骤 S2，获取当前待加密信息的加密方式标识符，确定当前待加密信息的加密方式；

步骤 S3，根据当前待加密信息的加密方式加载对应的加密引擎。

具体地，步骤 S1 需要获取的待加密信息的要素包括：（1）安全等级；（2）大小；（3）需访问速度；其中，待加密信息的安全等级是指待加密信息的保密性，保密性高则安全等级也高，表明需要加密程度更高的加密方式；信息大小是指待加密信息所需的存储空间，需访问速度是指待加密信息是否需要被快速访问。本实施例中，安全等级包括安全等级高和安全等级低两种类型，例如大车载娱乐交互信息的安全等级一般为低，而车辆位置信息的安全等级为高；待加密信息的大小通过与存储空间阈值的比较，可分为存储空间大和存储空间小两种类型；待加密信息的需访问速度通过与访问速度阈值的比较，可分为需访问速度快和需访问速度慢两种类型。

作为一种示例，存储空间阈值可设为 500k，大于或等于 500k 的待加密信息属于存储空间大的信息，小于 500k 的待加密信息属于存储空间小的信息。访问速度阈值可设为 100ms，大于或等于 100ms 的待加密信息属于需访问速度慢的信息，小于 100ms 的待加密信息属于需访问速度快的信息。

根据获取的待加密信息的上述三要素，可以生成加密方式标识符，用于标识待加密信息的加密方式，具体地，本实施例中加密方式标识符包括软加密标识符和硬加密标识符，其中，软加密标识符用于标识该待加密信息须采用软加密方式，硬加密标识符用于标识该待加密信息须采用硬加密方式。可以理解的是，软加密标识符和硬加密标识符可以用数值 1 或 0 来区分，例如 0 代表软加密标识符，1 代表硬加密标识符。

生成加密方式标识符的一种标准是：对于同时满足安全等级低、存储空间小、需访问速度快的待加密信息生成软加密标识符，其它待加密信息则生成硬加密标识符。对于安全等级低、存储空间小、需访问速度快的信息使用软加密方式，能够提高加解密效率；对于安全等级较高的信息使用硬加密方式，可以提高数据的加密强度。

步骤 S2 对当前要传输的待加密信息实时获取其加密方式标识符，进而

根据加密方式标识符确定该当前待加密信息的加密方式。获取方式包括两种，一种是直接读取，一种是查表。对于直接获取方式，系直接读取携带在该当前待加密信息中的加密方式标识符；如前所述，加密方式标识符可用数值 1 或 0 增加在该当前待加密信息的消息体中。对于查表方式，则是查询由各待加密信息及其加密方式标识符形成的表格；该表格可以是一维表格，表格里各待加密信息 与其加密方式标识符一一对应，同样地，加密方式标识符可用数值 1 或 0 来表示。

需要说明的是，步骤 S2 的处理是实时的，能够对不同的待加密信息实时确定其加密方式，以便步骤 S3 动态加载对应的加密引擎。例如，对于用户画像信息，因其安全等级高，在步骤 S1 中已生成硬加密标识符，则步骤 S2 通过前述直接读取或查表方式获取其硬加密标识符，从而确定对其将采用硬加密方式；又如，对于车载娱乐交互信息，因其同时满足安全等级低、存储空间小、需访问速度快，在步骤 S1 中已生成软加密标识符，则步骤 S2 通过前述直接读取或查表方式获取其软加密标识符，从而确定对其将采用软加密方式。

步骤 S3 将根据步骤 S2 确定的当前待加密信息的加密方式，加载对应的加密引擎。以下分别介绍加载软加密引擎和加载硬加密引擎的流程。可以理解的是，所介绍的流程仅为举例，本发明实施例对具体的硬加密技术或软加密技术并不做限定，本领域常见的硬加密技术或软加密技术均可用于步骤 S3。

首先介绍加载软加密引擎的流程，请同时结合图 2-图 5 所示：

首先进行芯片引擎初始化：调用 SSL（Secure Sockets Layer，安全套接层）协议初始化函数 SSL_library_init，然后使用引擎加载函数 ENGINE_load 构造芯片引擎。进一步地，调用初始化引擎名函数 ENGINE_by_id 将构造的芯片引擎与索引绑定，即初始化引擎名；再调用加密算法注册函数 ENGINE_register_RSA 将芯片引擎的加密算法（RSA）注册到 openssl 引擎中，最后调用引擎设置函数 ENGINE_set_default_RSA 将芯片引擎的加密算法设置默认为 RSA 方法。

其次生成芯片秘钥：首先调用密钥生成函数 RSA_generate_key 或者

RSA_generate_key_ex 生成密钥对，然后判断软加密引擎中是否存在获取密钥的方法；如果存在，则进一步调用内置密钥生成器 rsa_builtin_keygen 生成密钥，然后直接返回密钥结构；如果不存在，则调用芯片引擎中的获取密钥方法，然后通过软算法生成伪私钥，再进一步地调用芯片获取密钥接口获取密钥对里的 N（模数）和 E（公钥指数），然后判断芯片密钥是否生成成功，若成功则替换软算法生成的伪密钥中的 N 和 E 并返回密钥结构，若失败则返回错误返回码。需要说明的是，调用芯片引擎中的获取密钥方法然后通过软算法生成的是伪私钥，与调用内置密钥生成器 rsa_builtin_keygen 生成的密钥不一样，该伪私钥是为了正常运行 openssl 的流程。

最后加载芯片密钥：首先调用密钥加载函数 ENGINE_load_private_key 或 ENGINE_load_public_key 读取跟随车辆数字证书一起下载的软密钥文件；接着判断是否读取成功；如果读取失败，则新建密钥文件并将默认密钥（是一个假密钥，用来完善流程）信息写入到该软密钥文件，然后调用 PEM_read_PrivateKey 将获取的密钥文件句柄传入，构造用于存放非对称密钥信息的 EVP_PKEY 结构；如果读取成功则直接调用 PEM_read_PrivateKey 将获取的密钥文件句柄传入，构造 EVP_PKEY 结构。进一步地，调用芯片查询密钥接口 MizerQueryRsaKey，获取密钥对里的 N 和 E；然后判断是否获取成功，若成功，则将从芯片返回的 N 和 E 替换到软密钥生成的 EVP_PKEY 结构中，然后返回 EVP_PKEY 结构，若失败则返回空指针。

加载硬加密引擎的流程如图 6 所示：首先加载硬加密引擎，完成硬件引擎设备的枚举等操作；然后通过随机函数产生随机数，将随机数发送给硬加密引擎。硬加密引擎加载加密算法引擎对随机数进行加密，然后将加密结果发给解密引擎解密，再将解密结果与原始随机数（即通过随机函数产生的随机数）进行比对，判断是否通过验证。

通过上述说明可知，与现有技术相比，本发明的有益效果在于：本发明根据不同信息的特点，在同一个系统上设计同时存在两种加密方式——软加密方式和硬加密方式，根据信息的内容和情况动态加载两种加密方式，从而既利用了软加密技术和硬加密技术各自的优点，也避免了其缺点，提高了高密信息的加密强度和非高密信息的访问速度，同时减少了资源的浪费，增加

了资源的加解密效率。

以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权 利 要 求

1. 一种动态加载加密引擎的方法，其特征在于，包括：

步骤 S1，根据待加密信息的安全等级、大小和需访问速度生成加密方式标识符，其中，所述加密方式标识符包括软加密标识符和硬加密标识符，所述软加密标识符用于标识所述待加密信息须采用软加密方式，所述硬加密标识符用于标识所述待加密信息须采用硬加密方式；

步骤 S2，获取当前待加密信息的加密方式标识符，确定当前待加密信息的加密方式；

步骤 S3，根据当前待加密信息的加密方式加载对应的加密引擎。

2. 根据权利要求 1 所述的方法，其特征在于，所述安全等级包括安全等级高和安全等级低两种类型，所述待加密信息的大小通过与存储空间阈值的比较，包括存储空间大和存储空间小两种类型，所述待加密信息的需访问速度通过与访问速度阈值的比较，包括需访问速度快和需访问速度慢两种类型。

3. 根据权利要求 2 所述的方法，其特征在于，所述步骤 S1 中生成加密方式标识符具体是：对于同时满足安全等级低、存储空间小、需访问速度快的待加密信息生成软加密标识符，其它待加密信息则生成硬加密标识符。

4. 根据权利要求 2 所述的方法，其特征在于，所述存储空间阈值设为 500k，大于或等于 500k 的待加密信息属于存储空间大的信息，小于 500k 的待加密信息属于存储空间小的信息；所述访问速度阈值设为 100ms，大于或等于 100ms 的待加密信息属于需访问速度慢的信息，小于 100ms 的待加密信息属于需访问速度快的信息。

5. 根据权利要求 4 所述的方法，其特征在于，所述步骤 S2 获取当前待加密信息的加密方式标识符的方式包括：直接读取携带在所述当前待加密信息中的加密方式标识符；或者查询由各待加密信息及其加密方式标识符形成的表格。

6. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S3 根据所述步骤 S2 确定的当前待加密信息的加密方式，加载软加密引擎或者硬加密引擎，加载软加密引擎的步骤包括：

进行芯片引擎初始化；

生成芯片秘钥；

加载芯片密钥。

7. 根据权利要求 6 所述的方法，其特征在于，所述进行芯片引擎初始化的步骤包括：

调用 SSL 协议初始化函数，然后使用引擎加载函数构造芯片引擎；

调用初始化引擎名函数将构造的所述芯片引擎与索引绑定；

调用加密算法注册函数将所述芯片引擎的加密算法注册到 openssl 引擎中；

调用引擎设置函数将所述芯片引擎的加密算法设置默认为 RSA 方法。

8. 根据权利要求 7 所述的方法，其特征在于，所述生成芯片秘钥的步骤包括：

调用密钥生成函数生成密钥对；

判断软加密引擎中是否存在获取密钥的方法，如果存在，则进一步调用内置密钥生成器生成密钥，然后直接返回密钥结构；如果不存在，则调用芯片引擎中的获取密钥方法，通过软算法生成伪私钥，再进一步调用芯片获取密钥接口获取密钥对里的 N 和 E，然后判断芯片密钥是否生成成功，若成功则替换软算法生成的伪密钥中的 N 和 E 并返回密钥结构，若失败则返回错误返回码。

9. 根据权利要求 8 所述的方法，其特征在于，所述加载芯片密钥的步骤包括：

调用密钥加载函数读取跟随车辆数字证书一起下载的软密钥文件，并判断是否读取成功；如果读取失败，则新建密钥文件并将默认密钥信息写入到所述软密钥文件，然后将获取的密钥文件句柄传入，构造用于存放非对称密钥信息的 EVP_PKEY 结构；如果读取成功则将获取的密钥文件句柄传入，构造 EVP_PKEY 结构；

调用芯片查询密钥接口获取密钥对里的 N 和 E，并判断是否获取成功，若成功，则将从芯片返回的 N 和 E 替换到软密钥生成的 EVP_PKEY 结构中，然后返回 EVP_PKEY 结构，若失败则返回空指针。

10. 根据权利要求 6 所述的方法，其特征在于，加载硬加密引擎的步骤

包括：

加载硬加密引擎；

通过随机函数产生随机数，将随机数发送给硬加密引擎；

硬加密引擎加载加密算法引擎对随机数进行加密；

将加密结果发送给解密引擎解密；

将解密结果与通过随机函数产生的随机数进行比对，判断是否通过验证。

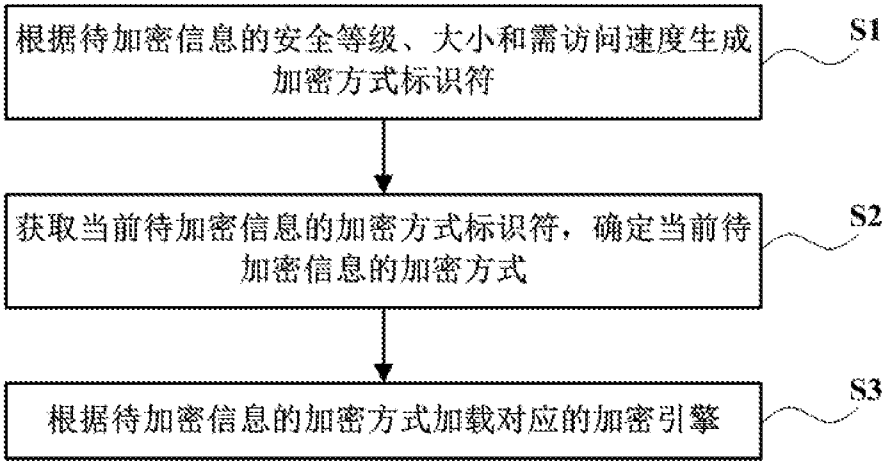

根据待加密信息的安全等级、大小和需访问速度生成加密方式标识符
S1
获取当前待加密信息的加密方式标识符，确定当前待加密信息的加密方式
S2
根据待加密信息的加密方式加载对应的加密引擎
S3

图 1

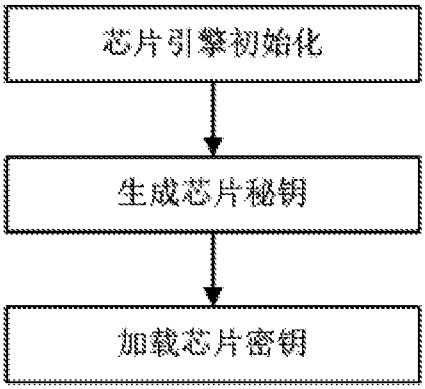

芯片引擎初始化
生成芯片秘钥
加载芯片密钥

图 2

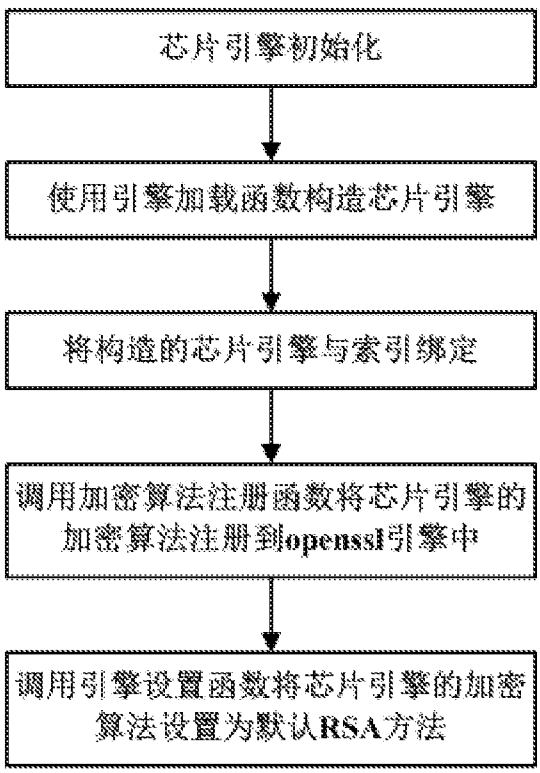

芯片引擎初始化
使用引擎加载函数构造芯片引擎
将构造的芯片引擎与索引绑定
调用加密算法注册函数将芯片引擎的加密算法注册到openssl引擎中
调用引擎设置函数将芯片引擎的加密算法设置为默认RSA方法

图 3

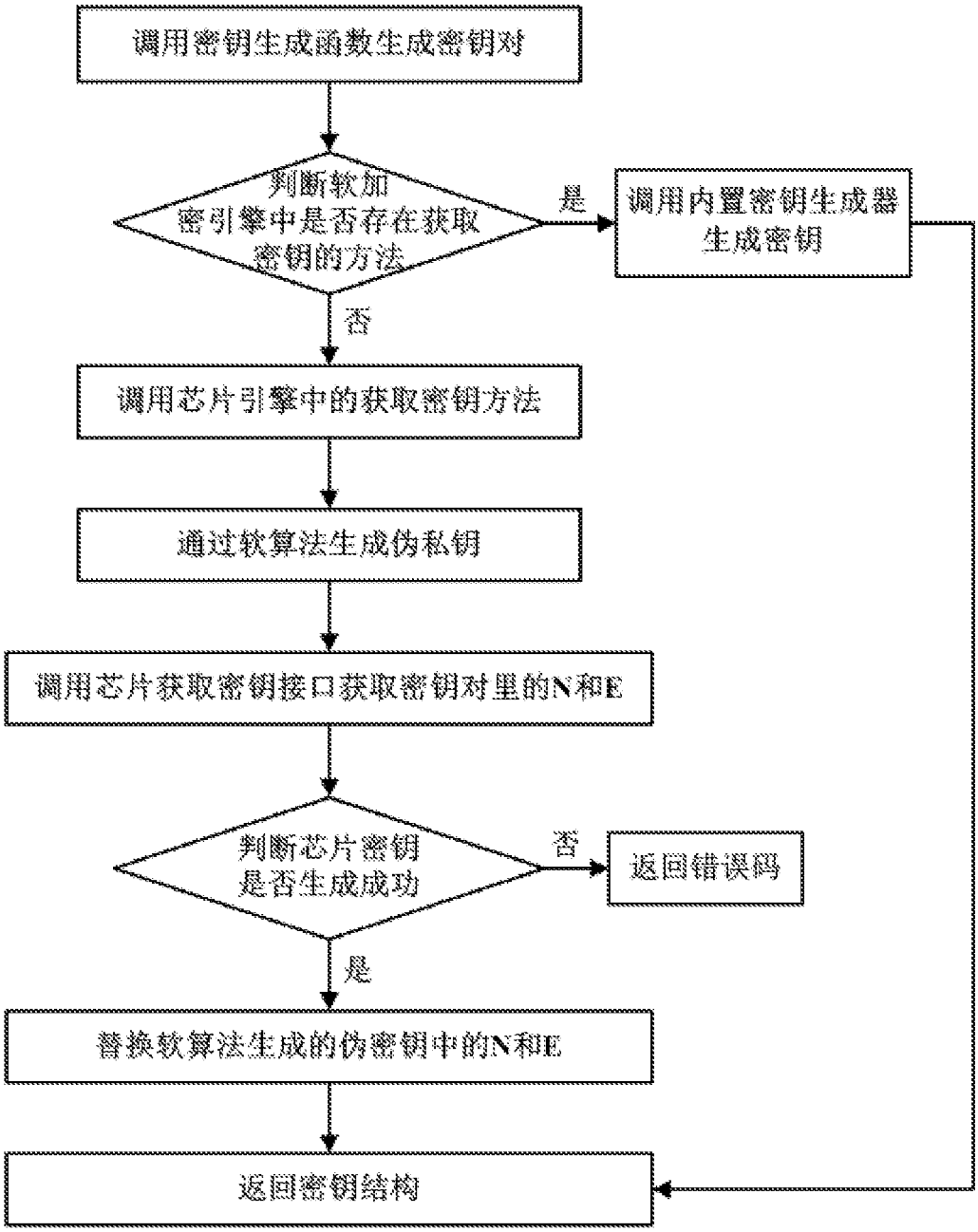

调用密钥生成函数生成密钥对
判断软加密引擎中是否存在获取密钥的方法
是
调用内置密钥生成器生成密钥
否
调用芯片引擎中的获取密钥方法
通过软算法生成伪私钥
调用芯片获取密钥接口获取密钥对里的N和E
判断芯片密钥是否生成成功
否
返回错误码
是
替换软算法生成的伪密钥中的N和E
返回密钥结构

图 4

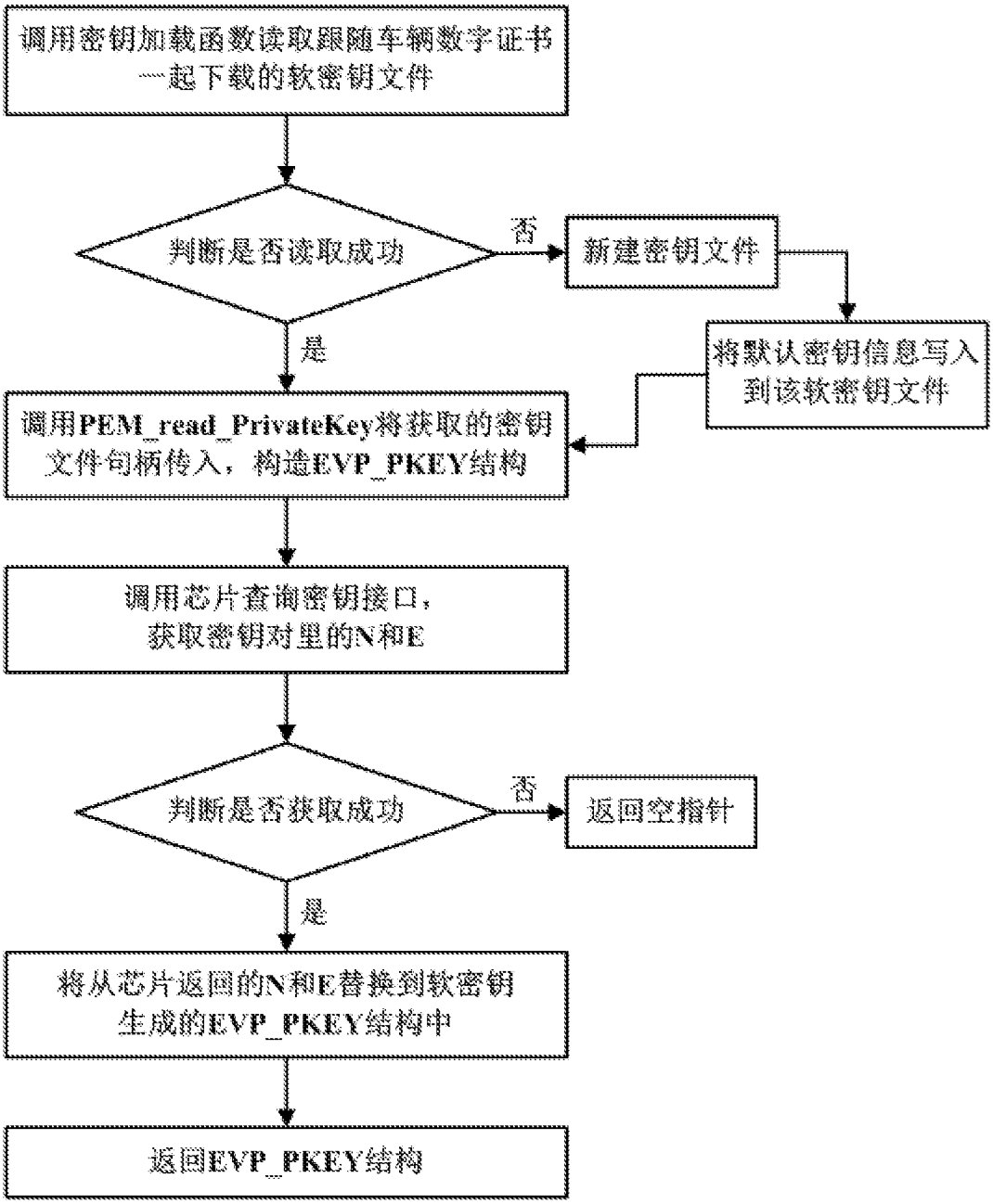

调用密钥加载函数读取跟随车辆数字证书一起下载的软密钥文件
判断是否读取成功
否
新建密钥文件
将默认密钥信息写入到该软密钥文件
是
调用PEM_read_PrivateKey将获取的密钥文件句柄传入，构造EVP_PKEY结构
调用芯片查询密钥接口，获取密钥对里的N和E
判断是否获取成功
否
返回空指针
是
将从芯片返回的N和E替换到软密钥生成的EVP_PKEY结构中
返回EVP_PKEY结构

图 5

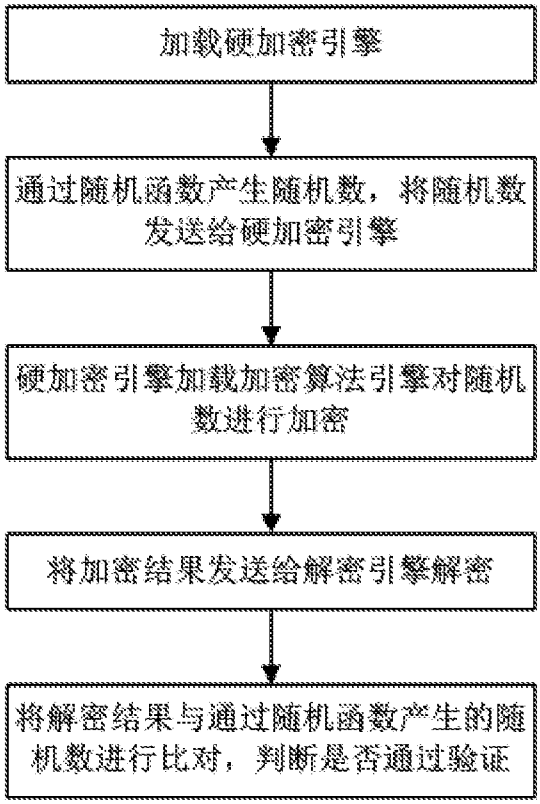

加载硬加密引擎
通过随机函数产生随机数，将随机数发送给硬加密引擎
硬加密引擎加载加密算法引擎对随机数进行加密
将加密结果发送给解密引擎解密
将解密结果与通过随机函数产生的随机数进行比对，判断是否通过验证

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/101481

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(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)

CNABS; CNTXT; VEN; WOTXT; USTXT; EPTXT; CNKI: 硬件, 软件, 加密, 硬加密, 软加密, 动态, 加载, 策略, 选择, 确定, 安全等级, 大小, 速度, hardware, software, encryption, hard encryption, soft encryption, dynamic, loading, strategy, select, determine, security, level, size, speed

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105376051 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) 02 March 2016 (2016-03-02) description, paragraphs [0026]-[0053]	1-10
A	CN 104123506 A (BEIJING ERENEBEN INFORMATION TECHNOLOGY CO., LTD.) 29 October 2014 (2014-10-29) entire document	1-10
A	US 6028933 A (LUCENT TECHNOLOGIES INC.) 22 February 2000 (2000-02-22) entire document	1-10

☐ 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
01 September 2021	**13 September 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/101481

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 105376051 A	02 March 2016	None	
CN 104123506 A	29 October 2014	CN 104123506 B	09 March 2018
US 6028933 A	22 February 2000	None	

国际检索报告

国际申请号
PCT/CN2021/101481

A. 主题的分类

H04L 9/06(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））

CNABS;CNTXT;VEN;WOTXT;USTXT;EPTXT;CNKI：硬件，软件，加密，硬加密，软加密，动态，加载，策略，选择，确定，安全等级，大小，速度，hardware, software, encryption, hard encryption, soft encryption, dynamic, loading, strategy, select, determine, security, level, size, speed

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
X	CN 105376051 A (宇龙计算机通信科技深圳有限公司) 2016年 3月 2日 (2016-03-02) 说明书第[0026]-[0053]段	1-10
A	CN 104123506 A (北京壹人壹本信息科技有限公司) 2014年 10月 29日 (2014-10-29) 全文	1-10
A	US 6028933 A (LUCENT TECHNOLOGIES INC) 2000年 2月 22日 (2000-02-22) 全文	1-10

☐ 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
2021年 9月 1日	2021年 9月 13日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088	白坦
传真号 (86-10)62019451	电话号码 86-(010)-62411245

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/101481

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 105376051 A	2016年 3月 2日	无	
CN 104123506 A	2014年 10月 29日	CN 104123506 B	2018年 3月 9日
US 6028933 A	2000年 2月 22日	无	