(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
2023 年 5 月 25 日 (25.05.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/087423 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)

(21) 国际申请号: PCT/CN2021/135874

(22) 国际申请日: 2021 年 12 月 6 日 (06.12.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111372411.X 2021年11月18日 (18.11.2021) CN

(71) 申请人: 成都市卡蛙科技有限公司 (CHENGDU KAWA TECHNOLOGY CO., LTD) [CN/CN]; 中国四川省成都市中国（四川）自由贸易试验区成都高新区天府大道北段1480号1楼16号, Sichuan 610041 (CN)。

(72) 发明人: 陈禧 (CHEN, Xi); 中国四川省成都市中国（四川）自由贸易试验区成都高新区天府大道北段1480号1楼16号, Sichuan 610041 (CN)。 郑旭明 (ZHENG, Xuming); 中国四川省成都市中国（四川）自由贸易试验区成都高新区天府大道北段1480号1楼16号, Sichuan 610041 (CN)。 吴勇波 (WU, Yongbo); 中国四川省成都市中国（四川）自由贸易试验区成都高新区天府大道北段1480号1楼16号, Sichuan 610041 (CN)。 双建平 (SHUANG, Jianping); 中国四川省成都市中国（四川）自由贸易试验区成都高新区天府大道北段1480号1楼16号, Sichuan 610041 (CN)。

(74) 代理人: 广州粤高专利商标代理有限公司 (YOGO PATENT AND TRADEMARK AGENCY LIMITED COMPANY); 中国广东省广州市天

(54) **Title:** IN-VEHICLE NETWORK OTA SECURITY COMMUNICATION METHOD AND APPARATUS, VEHICLE-MOUNTED SYSTEM, AND STORAGE MEDIUM

(54) **发明名称:** 车内网OTA安全通讯方法、装置、车载系统及存储介质

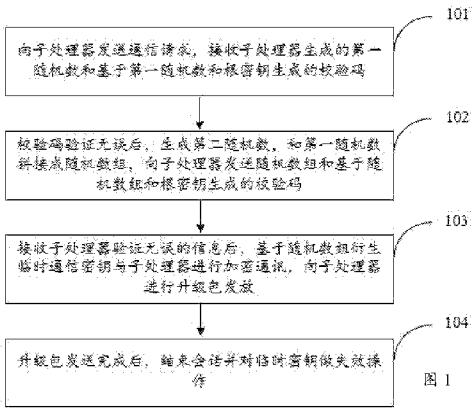

图 1

101 Send a communication request to a sub-processor, and receive a first random number generated by the sub-processor and a check code generated based on the first random number and a root key

102 After the check code is verified to be correct, generate a second random number, concatenate the second random number and the first random number into a random number set, and send to the sub-processor the random number set and a check code generated based on the random number set and the root key

103 After receiving the information that the verification by the sub-processor succeeds, derive a temporary communication key on the basis of the random number set for encrypted communication with the sub-processor, and issue an upgrade package to the sub-processor

104 After the upgrade package is sent, end a session and invalidate the temporary key

(57) **Abstract:** An in-vehicle network OTA security communication method and apparatus, a vehicle-mounted system, and a storage medium. The method comprises: sending a communication request to a sub-processor, and receiving a first random number generated by the sub-processor and a check code generated based on the first random number and a root key (101); after the check code is verified to be correct, generating a second random number, concatenating the second random number and the first random number into a random number set, and sending to the sub-processor the random number set and a check code generated based on the random number set and the root key (102); after receiving the information that the verification by the sub-processor succeeds, deriving a temporary communication key on the basis of the random number set for encrypted communication with the sub-processor, and issuing an upgrade package to the sub-processor (103); and after the upgrade package is sent, ending a session and invalidating the temporary key (104). The key for each encryption is randomly generated during in-vehicle network communication, and the OTA service is different each time, thereby avoiding key leakage and replay attacks, and ensuring the security of in-vehicle network OTA communication.

WO 2023/087423 A1

[见续页]

河区体育西路中石化大厦B塔4416室, Guangdong 510620 (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, 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：一种车内网OTA安全通讯方法、装置、车载系统及存储介质。该方法包括：向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码（101）；校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码（102）；接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放（103）；升级包发送完成后，结束会话并对临时密钥做失效操作（104）。车内网通讯时每次加密的密钥是随机生成，每次OTA业务都不一样，从而防止密钥泄露和重放攻击，保证了车内网OTA通讯的安全性。

车内网 OTA 安全通讯方法、装置、车载系统及存储介质

技术领域

本发明涉及汽车全景标定技术领域，尤其涉及一种车内网 OTA 安全通讯方法、装置、车载系统及存储介质。

背景技术

随着车联网的发展，OTA （Over-the-Air Technology，空中下载技术）在汽车中的应用逐渐增多，车企对于该技术越来越重视。由于该技术直接刷写车辆内所有搭载的 ECU 的系统版本，直接影响车辆的安全，所以 OTA 技术本身的安全防护尤为重要。OTA 主要是架构为基于互联网的云管端架构与车内网“云管端”架构。互联网的云管端主要功能为车辆通过联网与云端交互将升级包下载到车内主节点 ECU（Electronic Control Unit，电子控制单元）之中；而车内网的“云管端”则是以该主节点 ECU 为云，以车内网通信为管，与各个子 ECU 的端信，将各个升级包分发到各个子 ECU 并进行系统版本刷写。目前 OTA 技术安全防护主要关注在车辆和云端之间的网联信息安全，而车内网的通信的安全则目前几乎还处于“裸奔”状态。随着车内以太网的高速发展，车内通信速度越来越快，业务层的通信协议选择越来越多，且 OTA 也正在从基于传统车内 can 总线向车内以太网架构发展，越来越多的数据和信息基于车内网在各个 ECU 之间快速传输，其数据的安全性问题亟待解决。

目前 OTA 主要基于车内以太网和车内 can（Controller Area Network，控制器域网）总线通信，主节点和各子节点之间在通信之前没有身份认证功能，所有的业务交互数据如升级包分发，升级命令，升级进度等数据都是明文传输，数据未经过任何加密，所以主节点或者子节点被攻击，都有可能进行非法的 OTA 活动，影响车辆安全。

发明内容

本发明为克服上述现有技术所述的至少一种缺陷（不足），提供一种车内网 OTA 安全通讯方法、装置、车载系统及存储介质。

为解决上述技术问题，本发明的技术方案如下：

第一方面，本发明提供一种车内网 OTA 安全通讯方法，应用于车载系统，所述车载系统包括主处理器和子处理器，所述主处理器预置根密钥，所述子处理器预置根密钥种子或者根密钥，所述主处理器与外部传输连接，在线或离线获取升级包；所述方法包括：

向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码；

校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码；

接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放；

升级包发送完成后，结束会话并对临时密钥做失效操作。

进一步的，所述校验码为 MAC 值，所述 MAC 值是基于 MAC 算法和根密钥对随机数数据进行的 MAC 计算而得出的校验值。

进一步的，随机数的拼接由第一随机数和第二随机数并列成数据组的方式形成。

进一步的，所述基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放包括：

子处理器向主处理器请求升级包；

主处理器基于外部传输获取的升级包向子处理器返回升级包；

下载完成后，子处理器向主处理器发送完成信号；

其中，上述会话传输均采用基于随机数组衍生临时通信密钥进行加密通讯。

进一步的，所述升级包发送完成后，结束会话并对临时密钥做失效操作具体包括：

在升级包升级完成后，子处理器发送会话终止标识给主处理器，临时密钥失效，后续有新的升级任务，再生成新的临时密钥进行通信数据加密。

进一步的，所述主处理器通过从云端在线下载或 USB 端口离线下载的方式获取升级包。

进一步的，所述校验码验证方法包括：

获取随机数数据；

利用随机数数据并基于根密钥计算校验码；

将计算得到的校验码和消息中的校验码进行匹配，匹配一致则验证通过，否则验证不通过；

其中，校验码为 MAC 值。

第二方面，本发明提供一种车内网 OTA 安全通讯装置，所述通讯装置包括主处理器，所述主处理器通过上述的车内网 OTA 安全通讯方法与车载系统中的子处理器通讯连接，向子处理器发送升级包。

第三方面，本发明提供一种车载系统，包括子处理器和上述的车内网 OTA 安全通讯装置。

第四方面，本发明还提供一种存储介质，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述的车内网 OTA 安全通讯方法中的步骤。

本发明在车内网利用随机数、根密钥进行临时密钥的生成，利用MAC值进行完整性校验，车内网的主节点和各个子节点进行 OTA 业务之前需要对双方的身份进行认证，认证通过后才能开始 OTA 业务。在业务进行时，主节点和各子节点之间需要交互的数据包括各种命令，升级包内容，升级进度传输等等一切数据都会经过加密，且每次加密的密钥是随机生成，每次 OTA 业务都不一样，从而防止密钥泄露和重放攻击，保证了车内网 OTA 通讯的安全度，提高了车载系统的安全性。

附图说明

图 1 为本发明实施例中车内网 OTA 安全通讯方法的结构流程图。

图 2 为本发明实施例中车内网 OTA 安全通讯方法具体实施方式的流程图。

图 3 为本发明实施例中数据传输封装结构图。

图 4 为本发明实施例中随机数拼装示意图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，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。

本申请实施例的附图中相同或相似的标号对应相同或相似的部件；在本申请的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本申请和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制。

此外，若有“第一”、“第二”等术语仅用于描述目的，主要是用于区分不同的装置、元件或组成部分（具体的种类和构造可能相同也可能不同），并非用于表明或暗示所指示装置、元件或组成部分的相对重要性和数量，而不能理解为指示或者暗示相对重要性。

实施例一

整车 OTA 是基于车内网对车辆各个 ECU 系统版本进行刷写更新的过程，针对目前车内网

通信几乎无任何安全措施的通信现状，本实施例中的方法主要用于防止各 ECU 的系统被随意篡改和刷写。

图 1 示出了本实施例中车内网 OTA 安全通讯方法的结构流程图。

如图 1 所示，本实施例提供了一种车内网 OTA 安全通讯方法，该方法应用于车载系统中，主要用于实现车内网中，主处理器和子处理器之间的信息通讯，主要来实现提高车辆本省的 OTA 技术安全防护，防止车内网升级包分发传输过程中，主节点或者子节点被攻击，被外部利用进行非法的 OTA 活动，进而影响车辆安全。

具体的，本方案基于车载系统，该车载系统具体包括有主处理器和子处理器，其中，主处理器预置根密钥，而子处理器则预置根密钥种子或者根密钥，若采用根密钥种子，则需要通过根密钥种子来生成根密钥，具体的，该根密钥可以根据实际情况预置在安全芯片或者安全分区或者普通分区。更为具体的，所述主处理器与外部传输连接，在线或离线获取升级包，本实施例中的方法利用主处理器来执行以下步骤：

101、向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码；

102、校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码；

103、接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放；

104、升级包发送完成后，结束会话并对临时密钥做失效操作。

其中，在子处理器要获取升级包时，和主处理器进行通信请求，两者通过生成的随机数以及预置的根密钥来生成临时密钥。

如步骤 101、102 和 103 所述，具体的临时密钥生成方法为，主处理器和子处理器分别产生一个随机数，并通过两次传输使两者分别获取两个随机数拼接得到的随机数组，利用该随机数组形成临时密钥。

在随机数传输过程中，为了防止传输过程被劫持并篡改，本实施例通过校验码的方式来进行验证，其中，本实施例的校验码采用 MAC 值（Media Access Control Address，媒体存取控制位址）。具体的，发送端在发送时利用随机数计算得到一个 MAC 值，并将 MAC 值发送给接收端，接收端接收数据后再使用预置的根密钥计算 MAC 值，若 MAC 值不对，即可知道数

据有被篡改，从而以此进行验证。

临时密钥确认后，主处理器和子处理器后续的升级包升级会话过程中，均采用该临时密钥进行通讯，并在升级包发送完毕后，使临时密钥失效，后续会话在重新生成临时密钥，以确保后续会话的安全性，避免防止密钥泄露和重放攻击。

其中，作为前提，主处理器可以通过从云端在线下载或USB端口离线下载的方式获取升级包。

以下提供本实施例中的一些优选方案。

其中，优选的，本实施例中的校验码采用MAC值，该MAC值是基于MAC算法和根密钥对随机数数据进行的MAC计算而得出的校验值，在会话通讯被挟持后，该MAC值会发生变化，因此可以以此作为校验。

优选的，随机数的拼接由第一随机数和第二随机数并列成数据组的方式形成。例如，若第一随机数为Ra，第二随机数为Rb，则拼接完毕的随机数组为RaRb。

作为优选的，步骤103中的基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放包括：

201、子处理器向主处理器请求升级包。

202、主处理器基于外部传输获取的升级包向子处理器返回升级包。

203、下载完成后，子处理器向主处理器发送完成信号。

其中，上述会话传输均采用基于随机数组衍生临时通信密钥进行加密通讯。

在上述步骤中，主处理器可以分为一个FTP服务端和一个云端通讯端，其中，FTP（File Transfer Protocol，文件传输协议）服务端类似于一个FTP服务器，便于子处理器通过FTP传输协议从主处理器下载升级包文件。而云端通讯端是负责与云端通信的，负责从云端将所有处理器的升级文件下载到主处理器，然后各个子处理器再从主处理器通过FTP传输协议将各自的升级包文件下载下来。

在上述升级包请求中，子处理器通过临时密钥向主处理器的FTP服务端请求升级包，并在主处理器返回升级包时进行接收，并在下载成功后返回下载成功的信号，以结束会话。

优选的，步骤104中的升级包发送完成后，结束会话并对临时密钥做失效操作具体包括：

在升级包升级完成后，子处理器发送会话终止标识给主处理器，临时密钥失效，后续有新的升级任务，再生成新的临时密钥进行通信数据加密。

具体的，子处理器得到升级包后开始进行升级，升级完成后，使用临时密钥加密升级完成的消息并附带完成标识给主处理器，临时密钥失效，后续有新的升级任务，再生成新的临时密钥进行通信数据加密。

优选的，在本实施例的方法中，校验码验证方法包括：

301、获取随机数数据；

302、利用随机数数据并基于根密钥计算校验码；

303、将计算得到的校验码和消息中的校验码进行匹配，匹配一致则验证通过，否则验证不通过；

其中，校验码为 MAC 值。

在上述验证方法中，MAC 值的作用主要是完整性校验，如果传输的消息在通信通道中被劫持并篡改，那么这个接收端接收数据后再使用预置的根密钥计算 MAC 值，会发现 MAC 值不对，即可知道数据有被篡改，从而实现验证。

为了更好的操作体验，本实施例提供一个具体的实施方式，请参阅图 2，其中，图 2 中的主 ECU 为本实施例中的主处理器，子 ECU 为本实施例中的子处理器，具体步骤如下：

作为前提，首先，在进行升级包传输前：

主处理器内预置有根密钥，而子处理器预置根密钥种子或者根密钥，其中，根密钥可以预置在安全芯片或者安全分区或者普通分区，视实际情况而定。其次，升级包可通过在线下载到主处理器，也可以通过 USB 等离线方式传到主处理器。

在升级包传输过程中：

S1，当子处理器的升级包准备好后，主处理器发送通信请求给子处理器。

S2，子处理器在收到通信请求后，产生第一随机数 Ra，基于根密钥种子利用密钥衍生算法，例如 KDF（一种密钥派生函数）算法，生成根密钥，再使用 MAC 算法计算发送给主处理器的消息的 MAC 值，最后的消息数据结构如图 3，其中，Data 包含随机数 Ra 以及其他自定的通信数据字段，MAC 值是基于 MAC 算法和根密钥对 Data 进行的 MAC 计算而得出的值。

S3，主处理器验证子处理器发过来的消息：获取 Data（Ra）,基于根密钥计算 MAC 值，最后和消息中的 MAC 值进行匹配，一样说明验证通过，不一样则验证不通过。

S4，验证通过后，主处理器产生随机数 Rb，并拼接 Ra 和 Rb，拼接模型如下图 4。在拼接完成后，并使用根密钥计算 Data（RaRb）的 MAC 值，然后发送给子处理器。

S5,子处理器基于步骤3的原理验证主处理器发送过来的消息,验证通过得到随机数RaRb,并返回验证通过的消息给主处理器。这样主处理器和子处理器都拥有随机数RaRb，后续的通信使用的加密临时密钥都使用基于随机数RaRb衍生的临时密钥。

6，主处理器获得验证通过的消息后，使用基于RaRb衍生的临时密钥加密请求子处理器下载升级包的消息发送给子处理器，子处理器使用基于RaRb的临时密钥解密消息，得到下载升级包的地址等信息，并使用临时密钥加密返回信息“OK”给主处理器。

7，子处理器基于升级包下载地址向主处理器的FTP服务发起升级包下载请求，主处理器循环返回升级包给子处理器，直到升级包下载完成。

8，子处理器下载完成后，使用临时密钥加密下载完成的消息给主处理器。

9，子处理器得到升级包后开始进行升级，升级完成后，使用临时密钥加密升级完成的消息并附带Final标识给主处理器，临时密钥失效，后续有新的升级任务，再生成新的临时密钥进行通信数据加密。

本实施例的好处在于,该安全通讯方法在车内网利用随机数、根密钥进行临时密钥的生成,利用MAC值进行完整性校验，车内网的主节点和各个子节点进行OTA业务之前需要对双方的身份进行认证，认证通过后才能开始OTA业务。在业务进行时，主节点和各子节点之间需要交互的数据包括各种命令，升级包内容，升级进度传输等等一切数据都会经过加密，且每次加密的密钥是随机生成，每次OTA业务都不一样，从而防止密钥泄露和重放攻击，保证了车内网OTA通讯的安全度，提高了车载系统的安全性。

实施例二

本实施例提供一种车内网OTA安全通讯装置，该通讯装置包括主处理器，主处理器能够与车载系统中的子处理器进行通讯连接，向子处理器发送从云端在线或者通过USB等接口离线获取的升级包。

其中，主处理器与车载系统中的子处理器的通讯方式采用随机数来产生临时密钥，具体通讯时，通讯装置通过主处理器，执行以下步骤：

向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码；

校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码；

接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放；

升级包发送完成后，结束会话并对临时密钥做失效操作。

优选的，本实施例中主处理器与车载系统中的子处理器的通讯方式采用实施例一种的车内网 OTA 安全通讯方法。

其安全通讯装置通过产生临时密钥，利用该密钥加密升级包通讯的方式来完成车内网安全通讯，进而有效提高了汽车车内网的安全性。

实施例三

本实施例提供一种车载系统，该车载系统包括子处理器和实施例二中车内网 OTA 安全通讯装置，其中，车载系统内的子处理器和安全通讯装置中的主处理器采用随机数来产生临时密钥，以临时密钥来进行会话，保证了车内网 OTA 通讯的安全。

实施例四

本实施例提供一种存储介质，该存储介质上存储有计算机程序，其中，计算机程序被处理器执行时，能够实现实施例一中车内网 OTA 安全通讯方法的步骤。

显然，本发明的上述实施例仅是为清楚地说明本发明所作的举例，而并非是对本发明的实施方式的限定。对于所属领域的普通技术人员来说，在上述说明的基础上还可以做出其它不同形式的变化或变动。这里无需也无法对所有的实施方式予以穷举。凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明权利要求的保护范围之内。

权 利 要 求 书

1.一种车内网 OTA 安全通讯方法，其特征在于，应用于车载系统，所述车载系统包括主处理器和子处理器，所述主处理器预置根密钥，所述子处理器预置根密钥种子或者根密钥，所述主处理器与外部传输连接，在线或离线获取升级包；所述方法包括：

向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码；

校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码；

接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放；

升级包发送完成后，结束会话并对临时密钥做失效操作。

2.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，所述校验码为 MAC 值,所述 MAC 值是基于 MAC 算法和根密钥对随机数数据进行的 MAC 计算而得出的校验值。

3.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，随机数的拼接由第一随机数和第二随机数并列成数据组的方式形成。

4.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，所述基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放包括：

子处理器向主处理器请求升级包；

主处理器基于外部传输获取的升级包向子处理器返回升级包；

下载完成后，子处理器向主处理器发送完成信号；

其中，上述会话传输均采用基于随机数组衍生临时通信密钥进行加密通讯。

5.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，所述升级包发送完成后，结束会话并对临时密钥做失效操作具体包括：

在升级包升级完成后，子处理器发送会话终止标识给主处理器，临时密钥失效，后续有新的升级任务，再生成新的临时密钥进行通信数据加密。

6.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，所述主处理器通过从云端在线下载或 USB 端口离线下载的方式获取升级包。

7.根据权利要求 1 所述的车内网 OTA 安全通讯方法，其特征在于，所述校验码验证方法包括：

获取随机数数据；

利用随机数数据并基于根密钥计算校验码；

将计算得到的校验码和消息中的校验码进行匹配，匹配一致则验证通过，否则验证不通过；

其中，校验码为 MAC 值。

8.一种车内网 OTA 安全通讯装置，其特征在于，所述通讯装置包括主处理器，所述主处理器通过权利要求 1-7 任一项所述的车内网 OTA 安全通讯方法与车载系统中的子处理器通讯连接，向子处理器发送升级包。

9.一种车载系统，其特征在于，包括子处理器和权利要求 8 所述的车内网 OTA 安全通讯装置。

10.一种存储介质，其特征在于，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1-7 任一项所述的车内网 OTA 安全通讯方法中的步骤。

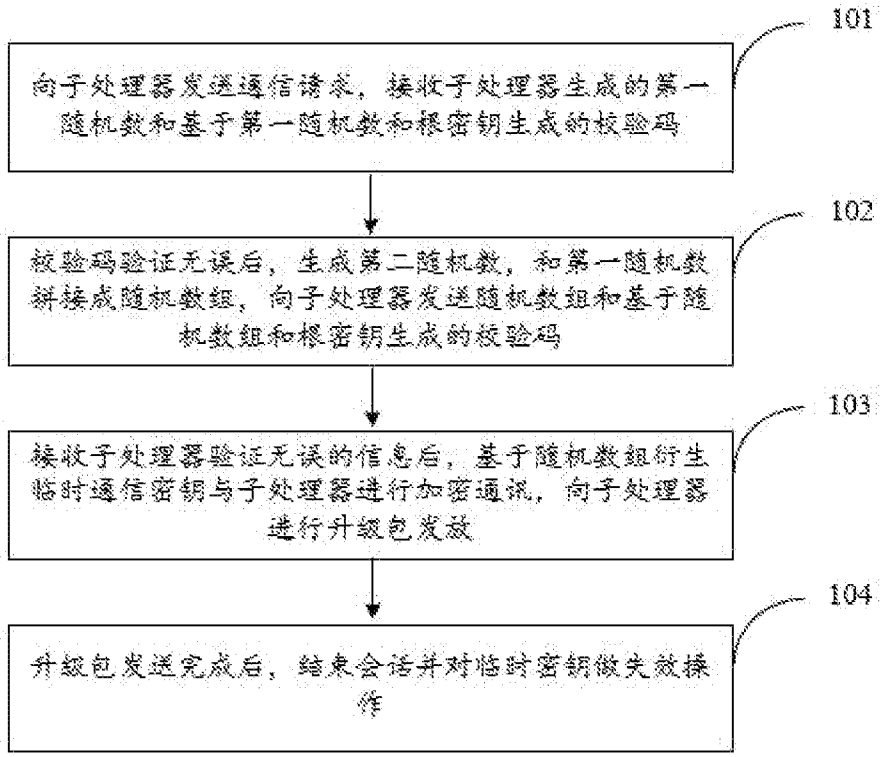
101
向子处理器发送通信请求，接收子处理器生成的第一随机数和基于第一随机数和根密钥生成的校验码
102
校验码验证无误后，生成第二随机数，和第一随机数拼接成随机数组，向子处理器发送随机数组和基于随机数组和根密钥生成的校验码
103
接收子处理器验证无误的信息后，基于随机数组衍生临时通信密钥与子处理器进行加密通讯，向子处理器进行升级包发放
104
升级包发送完成后，结束会话并对临时密钥做失效操作

图 1

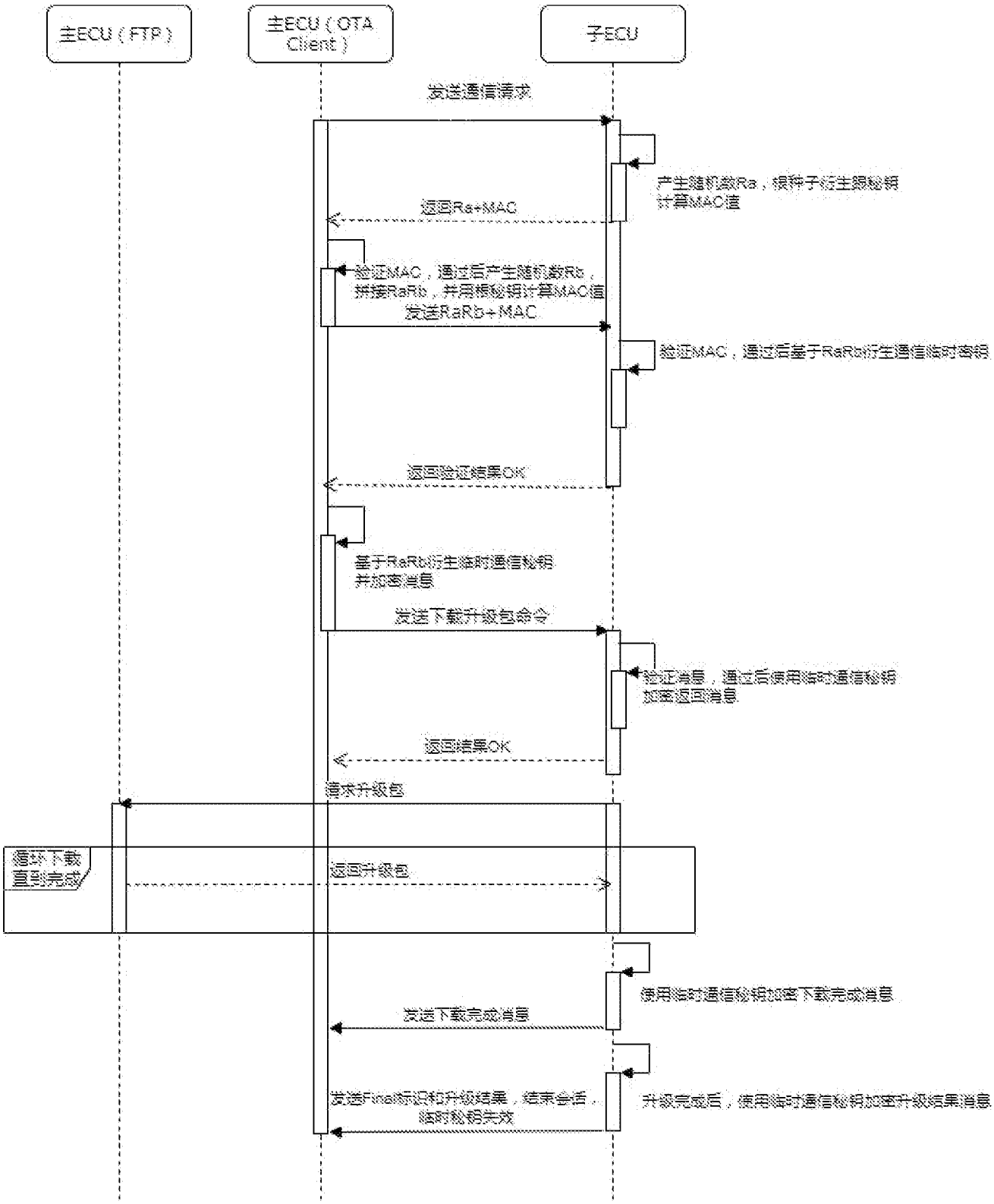
主ECU（FTP）
主ECU（OTA Client）
子ECU
发送通信请求
产生随机数Ra，根种子衍生预秘钥计算MAC值
返回Ra+MAC
验证MAC，通过后产生随机数Rb，拼接RaRb，并用预秘钥计算MAC值
发送RaRb+MAC
验证MAC，通过后基于RaRb衍生通信临时密钥
返回验证结果OK
基于RaRb衍生临时通信秘钥并加密消息
发送下载升级包命令
验证消息，通过后使用临时通信秘钥加密返回消息
返回结果OK
请求升级包
循环下载直到完成
返回升级包
使用临时通信秘钥加密下载完成消息
发送下载完成消息
发送Final标识和升级结果，结束会话，临时秘钥失效
升级完成后，使用临时通信秘钥加密升级结果消息

图 2

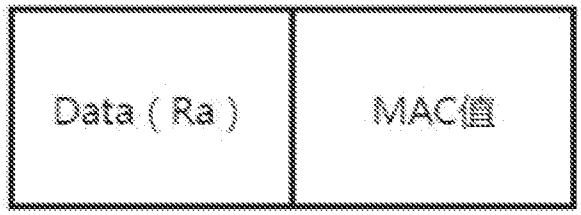

图 3

$$Ra + Rb = RaRb$$

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/135874

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; 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, CNKI, CNPAT, IEEE, GOOGLE: 车内网, 安全, 处理器, 根秘钥, 升级包, 固件, 随机数, 校验码, network, vehicle, security, processor, ECU, root, key, upgrade, package, firmware, random, number, check, code, OTA, MAC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112994898 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 18 June 2021 (2021-06-18) description, paragraphs 44-84, and figure 1	1-10
A	CN 113411285 A (GUANGZHOU AUTOMOBILE GROUP CO., LTD.) 17 September 2021 (2021-09-17) entire document	1-10
A	US 2019068381 A1 (KDDI CORPORATION) 28 February 2019 (2019-02-28) entire document	1-10
A	US 2019394046 A1 (SF MOTORS, INC.) 26 December 2019 (2019-12-26) 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
06 July 2022	**17 August 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/135874

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112994898 A	18 June 2021	None	
CN 113411285 A	17 September 2021	None	
US 2019068381 A1	28 February 2019	EP 3425842 A1	09 January 2019
		JP 2017157984 A	07 September 2017
		WO 2017150270 A1	08 September 2017
US 2019394046 A1	26 December 2019	US 10447483 B1	15 October 2019
		CN 111556836 A	18 August 2020
		WO 2019242288 A1	26 December 2019

国际检索报告

国际申请号
PCT/CN2021/135874

A. 主题的分类

H04L 9/32(2006.01)i; 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, CNKI, CNPAT, IEEE, GOOGLE: 车内网, 安全, 处理器, 根秘钥, 升级包,固件, 随机数, 校验码, network, vehicle, security, processor, ECU, root, key, upgrade, package, firmware, random, number, check, code, OTA, MAC

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	CN 112994898 A (北京邮电大学) 2021年6月18日 (2021-06-18) 说明书第44-84段, 附图1	1-10
A	CN 113411285 A (广州汽车集团股份有限公司) 2021年9月17日 (2021-09-17) 全文	1-10
A	US 2019068381 A1 (KDDI CORPORATION) 2019年2月28日 (2019-02-28) 全文	1-10
A	US 2019394046 A1 (SF MOTORS, INC.) 2019年12月26日 (2019-12-26) 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
2022年7月6日	2022年8月17日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 刘曼 电话号码 86-(10)-53961297

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/135874

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	112994898	A	2021年6月18日	无			
CN	113411285	A	2021年9月17日	无			
US	2019068381	A1	2019年2月28日	EP	3425842	A1	2019年1月9日
				JP	2017157984	A	2017年9月7日
				WO	2017150270	A1	2017年9月8日
US	2019394046	A1	2019年12月26日	US	10447483	B1	2019年10月15日
				CN	111556836	A	2020年8月18日
				WO	2019242288	A1	2019年12月26日