(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113839782 B
(45)授权公告日 2022.11.08

(21)申请号 202111042795.9

(22)申请日 2021.09.07

(65)同一申请的已公布的文献号
申请公布号 CN 113839782 A

(43)申请公布日 2021.12.24

(73)专利权人 北京航空航天大学
地址 100191 北京市海淀区学院路37号
专利权人 上海工业控制安全创新科技有限公司

(72)发明人 孙钰 赵子安 李大伟 崔剑 关振宇 刘建伟 刘虹 倪华

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 王燕

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 12/40(2006.01)

(56)对比文件
US 2019149324 A1,2019.05.16
CN 110785961 A,2020.02.11

审查员 马文文

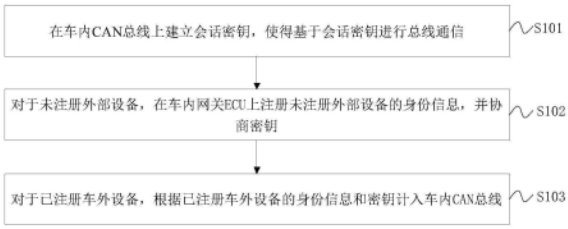
权利要求书2页 说明书9页 附图3页

(54)发明名称

基于PUF的车内网络CAN总线轻量级安全通信方法

(57)摘要

本发明公开了一种基于PUF的车内网络CAN总线轻量级安全通信方法,包括:在车内CAN总线上建立会话密钥,使得基于会话密钥进行总线通信;对于未注册外部设备,在车内网关ECU上注册未注册外部设备的身份信息,并协商密钥;对于已注册车外设备,根据已注册车外设备的身份信息和密钥计入车内CAN总线。该方法可以在实现CAN总线的内部安全密钥协商,以及与外部设备的安全认证接入。



CN 113839782 B

1.一种基于PUF的车内网络CAN总线轻量级安全通信方法,其特征在于,包括以下步骤:

在车内CAN总线上建立会话密钥,使得基于所述会话密钥进行总线通信;

对于未注册外部设备,在车内网关ECU上注册所述未注册外部设备的身份信息,并协商密钥;以及

对于已注册外部设备,根据所述已注册外部设备的身份信息和密钥接入所述车内CAN总线;

所述在车内CAN总线上建立会话密钥,使得基于所述会话密钥进行总线通信,包括:

在每次执行初始密钥分发时,从ECU本地挑战-响应数据库随机选取挑战值,并在每次执行完初始密钥分发后对挑战-响应对进行更新;

在发送所述挑战值至GECU的同时,发送第一新鲜随机值;

在所述GECU接收到所述挑战值后,使用自身附带的PUF生成响应值,并从所述响应值中提取稳定响应值,且生成第二新鲜随机值,并利用所述第一新鲜随机值和所述第二新鲜随机值计算认证杂凑值,以认证所述响应值的正确性,及从本地数据库中预存的挑战-响应对中挑选一个挑战值,以将挑出的挑战值、新生成随机数以及所述认证杂凑值一同在所述CAN总线上进行广播;

所述CAN总线上各ECU在接收到来自GECU的消息后,对所述认证杂凑值进行正确性验证,其中,若验证通过,则根据所述GECU发送的挑战值,使用自身附带的PUF生成对应的响应值,并从所述响应值中提取稳定响应值,利用GECU和ECU各自生成的两个随机数值和两个PUF响应值,各ECU生成一个认证值并发送到所述CAN总线上;

通过GECU对所述CAN总线上每一个ECU发送的认证值进行校验,其中,若验证通过,则计算生成会话密钥,且所述GECU根据由两方生成的两个随机数,确定下一次密钥协商时所需的新挑战值,并使用本地的PUF计算其相对应的响应值,并且将新的响应值使用会话密钥加密后广播到所述CAN总线上;

所述ECU从会话中的中间消息计算出会话密钥,并将所述GECU发来的新响应值解密,保存在本地。

2.根据权利要求1所述的方法,其特征在于,所述对于未注册外部设备,在车内网关ECU上注册所述未注册外部设备的身份信息,并协商密钥,包括:

所述GECU生成一个椭圆曲线上的第一随机点,对所述第一随机点的值使用私钥进行签名,及将己方的数字证书、椭圆曲线上的点以及数字签名一同发送给外部设备;

外部设备在验证所述GECU发送消息的正确性后,生成一个椭圆曲线上的第二随机点,根据所述第一随机点和所述第二随机点计算出面向外部设备PUF的挑战值,并使用本地的PUF计算出相对应的响应值,利用所述GECU的公钥,通过外部设备将新生成的随机点和PUF响应值进行加密,并对其进行数字签名,以及将己方的数字证书、加密值和数字签名值一同发送给所述GECU;

在所述GECU接收到来自外部设备的消息后,使用私钥解密得到由外部设备生成的随机点和PUF响应值,并利用签名校验二者的正确性,其中,若校验通过,则所述GECU在本地数据库中安全保存外部设备ID、PUF挑战值和PUF响应值三元组数据,随后所述GECU由Diffie-Hellman协议导出本轮会话密钥,并向外部设备发送一个校验值确认会话密钥和PUF秘密值。

3.根据权利要求2所述的方法,其特征在于,所述对于已注册外部设备,根据所述已注册外部设备的身份信息和密钥接入所述车内CAN总线,包括:

所述GECU通过待接入外部设备的ID检索数据库,读取上一轮约定好的PUF挑战值和响应值,生成一个随机数,利用该随机数加密PUF响应值并生成一个认证校验值,所述GECU将PUF挑战值、加密后的PUF响应值和所述认证校验值一同发送给所述已注册外部设备;

在所述已注册外部设备在接收到所述GECU发送的消息后,利用本地PUF生成与挑战值相对应的PUF响应值,使用该响应值解密得到所述GECU生成的随机数并验证认证校验值的正确性,若验证正确,则对所述GECU的身份验证通过,所述已注册外部设备在本地生成一个新的随机数,本轮会话的会话密钥由两方生成的两个随机数导出,根据导出的两个随机数,计算出下一轮要使用的PUF挑战值,并随即导出相应的PUF响应值,以及所述已注册外部设备使用所述GECU生成的随机数分别对新生成的PUF响应值和随机数进行加密,并计算出一个校验值保护数据完整性,将两个加密值和校验值一同发送给所述GECU;在所述GECU在接收到消息后,利用生成的随机数解密得到下一轮要使用的PUF响应值和外部设备生成的随机数,其中,若校验值验证通过,所述GECU使用新的PUF挑战值和响应值对所述数据库中的三元组进行更新,且使用两个随机数导出本轮会话的会话密钥,完成身份认证与密钥协商。

基于PUF的车内网络CAN总线轻量级安全通信方法

技术领域

[0001] 本发明涉及信息安全技术领域,特别涉及一种基于PUF的车内网络CAN总线轻量级安全通信方法。

背景技术

[0002] 现代汽车已经从单纯的交通运输工具发展为面向多种连接方式的移动计算平台,无论是车辆内部控制单元的协同工作还是车辆与外部设备的连接都需要通过工业总线或无线通信协议进行信息的交互。在车辆内部存在的众多种类总线中,控制器局域网(Controller Area Network,CAN)占有举足轻重的地位,尤其是承担了众多安全关键功能,如碰撞预测和防抱死制动系统。近年来,车内集成的服务变得越发复杂和庞大,CAN总线肩负的功能也在快速扩展。它负责将车内上百个电子控制单元(Electronic Control Unit,ECU)连接起来,综合多个传感器、执行器和控制器完成复杂的驾驶指令,同时可通过车载诊断系统(On-Board Diagnostics,OBD-II)接口,以及车载蓝牙、蜂窝网络和互联网连接(如Wi-Fi和4G)接口等与外部设备相连接,传递消息和指令。

[0003] 随着车辆通信功能的不断增强,车辆通信接口种类的增长,针对现代汽车的攻击手段正在迅速扩展,CAN总线面临的安全威胁也愈发严峻。在过去的十年里,有大量的研究表明,在实际道路测试中,攻击者已经具备了通过物理有线接入甚至无线远程接入等方式恶意控制汽车的能力。作为最重要的汽车接口,OBD-II接口提供了对车辆内部CAN总线网络的直接访问功能,CAN总线会在物理上暴露给来自外部接入设备的攻击者。此外,蓝牙、蜂窝网络等无线接口也可通过车内网关间接地连入CAN总线,攻击者可以通过以上接口实现车内通信的监听、恶意操控车辆的转向、制动、加速等功能,甚至篡改固件和内置代码。

[0004] 目前,车辆面临的最常见的两类攻击手段分别为重放攻击和中继攻击。重放攻击是指攻击者重新发送一个目的主机已接收过的包,以此达到欺骗系统的目的。重放攻击用于身份认证过程时,可以伪装合法身份获得授权;当用于消息传输过程时可以充当一条可通过系统认证的非法消息,干扰系统的正常通信。

[0005] 由于CAN总线在设计之初没有考虑到通信过程中的安全需求,面对着攻击者可以任意接入网络内部的现实情况,CAN总线的以下三大漏洞成为了亟待解决的安全问题:访问控制薄弱、缺乏认证机制和缺乏保密通信机制。同时,随着车内ECU设备的增长,总线上传输的消息更复杂,通信负载更大,这也要求为CAN总线设计的安全解决方案要保证高实时性,最低程度地影响总线传输的通信时延。

[0006] 目前针对CAN总线的安全解决方案分为两类,入侵检测系统(Intrusion Detection System,IDS)和密码协议。入侵检测系统可以在不改变CAN总线消息帧结构的条件下,检测总线中的异常行为。然而,IDS系统只有在攻击者发出攻击行为后才能发现异常,难以具备预防攻击的能力,同时很难对攻击行为做出相应的防御动作。此外,总线上传输的消息依旧没有进行机密性保护,对于被动的窃听者不具备防范能力。相比较而言,密码协议提供了完备的保密性和完整性保护功能,覆盖了初始密钥协商、密钥更新、加密传输、外部

设备接入等车辆通信各方面的安全需求。然而，现有面向CAN总线的密码协议在外部设备接入阶段，由于存在认证的需求，往往会采用计算复杂度很高的非对称密码算法，这会引入较大的计算开销和通信时延。而车内的ECU设备的会话密钥建立，也只依赖于GECU与各ECU间共享的长期对称密钥。这使得一旦长期密钥被窃取，协议的安全性将无法得到保障。因此，CAN总线密码协议需要更为轻量级，安全等级更高的解决方案。

发明内容

[0007] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0008] 为此，本发明的目的在于提出一种基于PUF的车内网络CAN总线轻量级安全通信方法，该方法可用于车内CAN总线内部设备间的身份认证与密钥建立，以及与外部设备的身份认证与密钥建立过程。

[0009] 为达到上述目的，本发明实施例提出了一种基于PUF的车内网络CAN总线轻量级安全通信方法，包括以下步骤：建立车内CAN总线上会话密钥，使得基于所述会话密钥进行总线通信；对于未注册外部设备，在车内网关ECU上注册所述未注册外部设备的身份信息，并协商密钥；对于已注册车外设备，根据所述已注册车外设备的身份信息和密钥计入所述车内CAN总线。

[0010] 本发明实施例的基于PUF的车内网络CAN总线轻量级安全通信方法，具有以下优势：

[0011] 1)提出了一种基于PUF的轻量级车内CAN总线初始密钥分发模块，减少了初始会话密钥分配过程中的计算开销和通信开销，面向更多ECU连接的CAN总线提供良好可扩展性。

[0012] 2)在外部设备接入的密钥建立环节中，除了外部设备的初始注册阶段外，不再依赖非对称密码学工具提供身份认证功能。仅需调用外部设备内部的PUF功能、对称加密功能和杂凑函数，大大降低了计算的复杂度，同时减少了协议的交互轮数，有效降低通信时延。

[0013] 3)由于外部设备中不再保存密钥等秘密信息，而仅使用基于硬件结构实现的PUF进行身份认证，从根本上杜绝了攻击者进行密钥窃取攻击的可能，安全性提升明显。

[0014] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0015] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0016] 图1为根据本发明一个实施例的基于PUF的车内网络CAN总线轻量级安全通信方法流程图；

[0017] 图2为根据本发明一个实施例的初始密钥分发模块执行流程图；

[0018] 图3为根据本发明一个实施例的外部设备注册模块执行流程图；

[0019] 图4为根据本发明一个实施例的外部设备接入模块执行流程图。

具体实施方式

[0020] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终

相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0021] 物理不可克隆函数(Physical Unclonable Function,PUF)是一种利用芯片制造过程中不可避免的随机差异,使得每个芯片根据输入的激励输出不可预测的响应的函数。因此,可以利用基于PUF产生的挑战响应对(Challenge-Response Pair,CRP)作为硬件指纹,完成对硬件的身份认证。由于PUF认证技术可以与硬件绑定,同时结构简单、计算开销小,非常适合在嵌入式设备上进行实现,目前已经在射频识别(Radio Frequency Identification,RFID)领域的安全认证中得到广泛采用:通过预共享的CRP,服务器可以对RFID设备完成单向认证。由于RFID设备内部没有对密钥明文存储,而仅存在PUF这一硬件结构,因此也不会出现针对密钥的窃取攻击。

[0022] 本方案借助可在CAN总线设备内实现的PUF技术,可以实现车辆内部的轻量级认证与密钥协商协议,同时满足对总线设备的对等实体认证等安全需求,可以确保重放、伪造等攻击无法对认证和密钥协商造成威胁及损失。此外,基于PUF的CAN总线外部设备接入协议仅需在车辆与外部设备首次连接时使用基于非对称密码技术。

[0023] 先介绍本发明中的概念及参数。

[0024] (1)车内CAN总线网络划分

[0025] 通常,车内CAN网络分为三个子网络,例如动力传动子网包含安全关键性操作,包括控制发动机、制动器和底盘控制部件。为了保证实时通信速率,信息娱乐子网通常具有高带宽和稳定的通信能力。这些子网之间的ECU的通信通过网关ECU(GECU)来实现,网关ECU被认为比通常的ECU具备更强大的计算能力以及对车外CAN总线设备的通信能力。

[0026] (2)物理不可克隆函数

[0027] 物理不可克隆函数(PUF)是一种新型的半导体安全技术,它可以作为芯片等半导体器件的唯一标识。PUF依赖于芯片制造过程中自然产生的物理微观结构。物理微观结构依赖于不可预测和不可控的随机物理因素。由于物理微结构的随机变化,不同的PUF对于相同的挑战值具有不同的输出响应。由于这些物理微结构通常是难以复制的,PUF的行为很难预测或提取。因此,攻击者很难伪造一个PUF电路,或者生产出完全相同的两个芯片,这表明PUF技术具有良好的抗克隆攻击能力。目前使用中最经典的PUF架构是仲裁器PUF电路,它可以简单的在FPGA等硬件环境下实现。此外,与加密函数相比,PUF需要更少的硬件计算资源,这适合于轻量级硬件设备的安全认证需求。由于PUF依赖于所制造电路的模拟物理特性来获得秘密信息,很容易受到噪声与其他环境因素的影响,使得输入相同的激励得到的响应有一定差异。为了解决这个问题,使用模糊提取器从噪声和非均匀随机PUF响应中生成具有适当熵的辅助信息。

[0028] 表1 参数含义

[0029]

符号	描述
$GECU$	网关 ECU
ECU_j	第 j 个 ECU
ID_j	第 j 个 ECU 的仲裁标识符
(C_G^i, R_G^i)	GECU 执行第 i 次会话时的 PUF 的挑战-响应对
N_i	新生成的随机值
P	有限域上椭圆曲线群的生成元
(EK, AK)	会话密钥，其中 EK 为加密密钥，AK 为完整性密钥
$PUF_j(\cdot)$	第 j 个 ECU 搭载的 PUF 函数
$H(\cdot)$	杂凑函数
$KDF(\cdot)$	密钥衍生算法，杂凑函数
$FE.Gen(\cdot)$	模糊提取器，可以从 PUF 不稳定响应值提取稳定响应
(sk, pk)	GECU 和外部设备的公私钥对
$Enc_k(\cdot)$	对称加密算法
$Dec_k(\cdot)$	对称解密算法
$Sig_{sk}(\cdot)$	签名算法

[0030]

$Vrfy_{pk}(\cdot)$	验签算法

[0031] 下面参照附图描述根据本发明实施例提出的基于PUF的车内网络CAN总线轻量级安全通信方法。

[0032] 本发明的目的是提供一种基于物理不可克隆函数(PUF)的轻量级CAN总线安全通信密码协议，涵盖车内CAN总线会话密钥建立协议和外部设备接入协议两个安全场景，相较于现有CAN总线安全协议在执行效率和可扩展性方面有明显提升。本发明在设备认证中除外部设备注册阶段外无需使用包含复杂运算的数字证书、公钥加密等非对称密码学技术，计算开销小，易于在嵌入式设备中实现。

[0033] 在本发明中，通过在每次新会话中利用挑战-响应机制建立新会话密钥的方式，可以有效抵御跨会话的消息重放攻击和认证信息重放攻击；通过进一步细化消息加密的计数器机制则可有效抵御单一会话内的重放攻击。中继攻击则可捕获并放大电子钥匙的电磁信号，制造钥匙就在汽车附近的假象并与车辆通信，从而利用漏洞直接开启车门。本发明在外部设备与车辆交互过程中，定义了一轮有状态的交互过程，当外部设备的状态发生变化并开启通信交互时可以按需进行提示报警，以此成功检出中继攻击的存在。

[0034] 本方案设计的协议族共包含三个模块，其中初始密钥分发模块可以完成车内CAN总线上会话密钥的建立，为总线上的安全通信创造条件。外部设备注册模块可以提供未注册外部设备在车内网关ECU(GECU)上的身份注册和密钥协商；外部设备介入模块可以对于

已注册过的车外设备实现与车内CAN总线的轻量级安全接入。

[0035] 图1为根据本发明一个实施例的基于PUF的车内网络CAN总线轻量级安全通信方法流程图。

[0036] 如图1所示，该基于PUF的车内网络CAN总线轻量级安全通信方法包括以下步骤：

[0037] 在步骤S101中，在车内CAN总线上建立会话密钥，使得基于会话密钥进行总线通信。

[0038] 在本发明的一个实施例中，在车内CAN总线上建立会话密钥，使得基于会话密钥进行总线通信，包括：

[0039] 在每次执行初始密钥分发时，从ECU本地挑战-相应数据库随机选取挑战值，并在每次执行完初始密钥分发后对挑战-响应对进行更新；

[0040] 在发送挑战值至GECU的同时，发送第一新鲜随机值；

[0041] 在GECU接收到挑战值后，使用自身附带的PUF生成响应值，并从响应值中提取稳定响应值，且生成第二新鲜随机值，并利用第一新鲜随机值和第二新鲜随机值计算认证杂凑值，以认证响应值的正确性，及从本地数据库中预存的挑战-响应对中挑选一个挑战值，以将挑出的挑战值、新生成随机数以及认证杂凑值一同在CAN总线上进行广播；

[0042] CAN总线上各ECU在接收到来自GECU的消息后，对认证杂凑值进行正确性验证，其中，若验证通过，则根据GECU发送的挑战值，使用自身附带的PUF生成对应的响应值，并从响应值中提取稳定响应值，利用GECU和ECU各自生成的两个随机数值和两个PUF响应值，各ECU生成一个认证值并发送到CAN总线上；

[0043] 通过GECU对CAN总线上每一个ECU发送的认证值进行校验，其中，若验证通过，则计算生成会话密钥，且GECU根据由两方生成的两个随机数，确定下一次密钥协商时所需的新挑战值，并使用本地的PUF计算其相对应的响应值，并且将新的响应值使用会话密钥加密后广播到CAN总线上；

[0044] ECU从会话中的中间消息计算出会话密钥，并将GECU发来的新响应值解密，保存在本地。

[0045] 具体地，步骤0:在车辆出厂时，GECU可在本地预先保存1000个挑战值，以及与这些挑战值相对应的总线上各ECU相应的响应值，构建GECU本地挑战-相应数据库。在每次执行初始密钥分发模块时，会从数据库中随机选取一个挑战值。各ECU需要在本地保存GECU对应的相同一对挑战-响应对，并在每次执行完初始密钥分发模块后对该挑战-响应对进行更新。

[0046] 步骤1:如图2所示，协议由某一指定的ECU发起。该ECU首先发送在上一轮通信中约定好的挑战值发送给GECU，同时还会发送一个新鲜的随机值。

[0047] 步骤2:GECU接收到挑战值后，使用自身附带的PUF生成响应值，并使用模糊特征提取器从响应值中提取稳定响应值。随后，GECU也生成一个新鲜的随机值，并利用步骤1和步骤2中由两方新生成的随机值计算认证杂凑值，用于认证响应值的正确性。GECU从数据库中预存的若干挑战-响应对中挑选一个挑战值。最终，GECU将挑出的挑战值、新生成随机数以及认证杂凑值一同在CAN总线上进行广播。

[0048] 步骤3:总线上各ECU在接收到来自GECU的消息后，首先对其认证杂凑值进行正确性验证。若验证通过，则根据GECU发送的挑战值，使用自身附带的PUF生成对应的响应值，并

使用模糊特征提取器从响应值中提取稳定响应值。利用GECU和ECU各自生成的两个随机数值和两个PUF响应值，各ECU可以生成一个认证值并发送到总线上。

[0049] 步骤4:GECU首先对总线上每一个ECU发送的认证值进行校验。若验证通过，则使用上述步骤中涉及到的中间消息计算生成会话密钥。随后，GECU根据由两方生成的两个随机数，确定下一次密钥协商时所需的新挑战值，并使用本地的PUF计算其相对应的响应值。最终，将新的响应值使用会话密钥加密后广播到总线上。

[0050] 步骤5:ECU同样使用上述会话中的中间消息计算出会话密钥，并将GECU发来的新响应值解密，保存在本地。至此，GECU与总线上其他各ECU完成了双向的身份认证和会话密钥协商，后续总线上传送的消息可以使用会话密钥保护消息的保密性和完整性。

[0051] 在步骤S102中，对于未注册外部设备，在车内网关ECU上注册未注册外部设备的身份信息，并协商密钥。

[0052] 在本发明的一个实施例中，对于未注册外部设备，在车内网关ECU上注册未注册外部设备的身份信息，并协商密钥，包括：

[0053] GECU生成一个椭圆曲线上的第一随机点，对第一随机点的值使用私钥进行签名，及将己方的数字证书、椭圆曲线上的点以及数字签名一同发送给外部设备；

[0054] 外部设备在验证GECU发送消息的正确性后，生成一个椭圆曲线上的第二随机点，根据第一随机点和第二随机点计算出面向外部设备PUF的挑战值，并使用本地的PUF计算出相对应的响应值，利用GECU的公钥，通过外部设备将新生成的随机点和PUF响应值进行加密，并对其进行数字签名，以及将己方的数字证书、加密值和数字签名值一同发送给GECU；

[0055] 在GECU接收到来自外部设备的消息后，使用私钥解密得到由外部设备生成的随机点和PUF响应值，并利用签名校验二者的正确性，其中，若校验通过，则GECU在本地数据库中安全保存外部设备ID、PUF挑战值和PUF响应值三元组数据，随后ECU由Diffie-Hellman协议导出本轮会话密钥，并向外部设备发送一个校验值确认会话密钥和PUF秘密值。

[0056] 具体地，外部设备注册模块，可以在外部设备第一次与汽车相连接时完成身份注册并协商密钥具体由三个步骤实现，如图3所示：

[0057] 步骤6:GECU首先生成一个椭圆曲线上的随机点，随后对该点的值使用私钥进行签名以保护该点数据的完整性和消息源认证。最终将己方的数字证书、椭圆曲线上点以及数字签名一同发送给外部设备。

[0058] 步骤7:外部设备在验证GECU发送消息的正确性后，同样可以生成一个椭圆曲线上的随机点，根据这两个随机点可以计算出面向外部设备PUF的挑战值，并使用本地的PUF计算出相对应的响应值。利用GECU的公钥，外部设备可以将新生成的随机点和PUF响应值进行加密，并对其进行数字签名。最终，外部设备可以将己方的数字证书、加密值和数字签名值一同发送给GECU。此外，在外部设备一方，本轮会话的会话密钥已可以由椭圆曲线上的Diffie-Hellman协议计算生成。

[0059] 步骤8:GECU在接收到来自外部设备的消息后，首先使用私钥解密得到由外部设备生成的随机点和PUF响应值，并利用签名校验二者的正确性。若校验通过，则GECU在本地数据库中安全保存外部设备ID、PUF挑战值和PUF响应值三元组数据，便于下一次外部设备接入时使用。GECU同样可以由Diffie-Hellman协议导出本轮会话密钥，并向外部设备发送一个校验值完成会话密钥和PUF秘密值的确认。

[0060] 在步骤S103中，对于已注册车外设备，根据已注册车外设备的身份信息和密钥计入车内CAN总线。

[0061] 在本发明的一个实施例中，对于已注册车外设备，根据已注册车外设备的身份信息和密钥计入车内CAN总线，包括：

[0062] GECU通过待接入外部设备的ID检索数据库，读取上一轮约定好的PUF挑战值和响应值，生成一个随机数，利用该随机数加密PUF响应值并生成一个认证校验值，GECU将PUF挑战值、加密后的PUF响应值和认证校验值一同发送给已注册外部设备；

[0063] 在已注册外部设备在接收到GECU发送的消息后，利用本地PUF生成与挑战值相对应的PUF响应值，使用该响应值解密得到GECU生成的随机数并验证认证校验值的正确性，若验证正确，则对GECU的身份验证通过，已注册外部设备在本地生成一个新的随机数，本轮会话的会话密钥由两方生成的两个随机数导出，根据导出的两个随机数，计算出下一轮要使用的PUF挑战值，并随即导出相应的PUF响应值，以及已注册外部设备使用GECU生成的随机数分别对新生成的PUF响应值和随机数进行加密，并计算出一个校验值保护数据完整性，将两个加密值和校验值一同发送给GECU；

[0064] 在GECU在接收到消息后，利用生成的随机数解密得到下一轮要使用的PUF响应值和外部设备生成的随机数，其中，若校验值验证通过，GECU使用新的PUF挑战值和响应值对数据库中的三元组进行更新，且使用两个随机数导出本轮会话的会话密钥，完成身份认证与密钥协商。

[0065] 具体地，外部设备接入模块，可以为已在GECU完成身份注册的外部设备完成轻量级的身份认证与密钥协商，具体由三个步骤实现，如图4所示：

[0066] 步骤9:GECU首先通过待接入外部设备的ID检索数据库，读取上一轮约定好的PUF挑战值和响应值。随后生成一个随机数，使用该随机数加密PUF响应值并生成一个认证校验值。最终，GECU将PUF挑战值、加密后的PUF响应值和认证校验值一同发送给外部设备。

[0067] 步骤10:外部设备在接收到消息后，首先使用本地PUF生成与挑战值相对应的PUF响应值，使用该响应值解密得到GECU生成的随机数并验证认证校验值的正确性。若验证正确，则对GECU的身份验证通过。外部设备在本地生成一个新的随机数，本轮会话的会话密钥即可使用两方生成的两个随机数导出。根据两个随机数，外部设备还可以计算出下一轮要使用的PUF挑战值，并随即导出相应的PUF响应值。随后，外部设备使用GECU生成的随机数分别对新生成的PUF响应值和随机数进行加密，并计算出一个校验值保护数据完整性。最终，外部设备将两个加密值和校验值一同发送给GECU。

[0068] 步骤11:GECU在接收到消息后，可以用自身在步骤9中生成的随机数，解密得到下一轮要使用的PUF响应值和外部设备生成的随机数。若校验值验证通过，GECU将使用新的PUF挑战值和响应值对数据库中的三元组进行更新。最后，GECU也可使用两个随机数导出本轮会话的会话密钥，完成全部身份认证与密钥协商功能。

[0069] 下面通过具体实施例介绍本发明的技术方案。

[0070] 模块一:初始密钥分发模块具体由五个步骤实现：

[0071] 步骤1:选定的发起方ECU首先生成一个随机数N_1，并将该随机数与GECU的挑战值C_G^i一同发送到总线上。

[0072] 步骤2:GECU在接收到挑战值后，使用本地附带的PUF计算其相应的响应值

$R_G^i = PUF_G(C_G^i)$。由于PUF直接计算得到的响应值可能不稳定，还需要使用模糊提取器计算出其稳定值，$(r_G^i, hd_G^i) = FE.Gen(R_G^i)$，其中$r_G^i$是稳定响应值，$hd_G^i$是辅助信息。随后，GECU从本地挑战-响应数据库中随机选取一个挑战值C_E^i，同时生成一个随机数N_2，并计算出认证杂凑值$Hash_G = H(r_G^i||C_E^i||N_1||N_2)$。最终，GECU将各ECU的挑战值$C_E^i$，随机数$R_2$和认证杂凑值$Hash_G$广播到总线上。

[0073] 步骤3：总线上其他ECU在收到来自GECU的消息后，首先验证认证杂凑值$Hash_G$的正确性。若验证通过，以总线上第j个ECU即ECU_j为例，首先使用本地的PUF计算出响应值$R_{Ej}^i = PUF_j(C_E^i)$，并用模糊提取器计算出稳定响应值$(r_{Ej}^i, hd_{Ej}^i) = FE.Gen(R_E^i)$。随后，ECU使用双方生成的稳定响应值和随机数计算校验值$Hash_i = H(r_{Ej}^i||r_G^i||N_1||N_2)$，并将该校验值发送到CAN总线上。

[0074] 步骤4：GECU在接收到总线上各ECU发送的校验值，即$Hash_1$，...，$Hash_n$，验证它们的正确性。若验证通过，则对各ECU的认证通过，GECU将导出会话密钥$EK||AK = KDF(C_G^i||r_G^i||Hash_1||\ldots||Hash_n)$。GECU下一次执行初始密钥分发模块时约定的挑战值将规定为$C_G^{i+1} = H(N_1||N_2)$，随后GECU将使用本地PUF和模糊提取器生成其对应的稳定响应值r_G^{i+1}，对其使用协商出的会话密钥进行加密，生成$r_{enc} = Enc_{EK}(r_G^{i+1})$，并将其发送到总线上。

[0075] 步骤5：总线上各ECU同样可以导出本轮会话密钥EK和AK，随后从GECU在步骤4发送的消息中解密获得下一轮GECU响应值$r_G^{i+1} = Dec_{EK}(r_{enc})$，并将挑战-响应对$(C_G^{i+1}, r_G^{i+1})$在本地保存。至此，GECU与总线上其他各ECU完成了双向的身份认证和会话密钥协商，后续总线上传送的消息可以使用会话密钥保护消息的保密性和完整性。

[0076] 模块二：外部设备注册模块具体由三个步骤实现：

[0077] 步骤6：GECU首先生成一个随机数a，并将其映射到椭圆曲线群上的一个随机点N_G＝a·P。随后，GECU对该随机点用自身的私钥生成一个数字签名$S_G = Sig_{sk_G}(N_G)$。最终，GECU将自身的数字证书、随机点和数字签名($Cert_G$，N_G，S_G)一同发送给外部设备。

[0078] 步骤7：外部设备在收到消息后，同样生成一个随机数b，并将其映射到椭圆曲线群上得到N_E＝b·P。若S_G校验通过，则使用椭圆曲线上的Diffie-Hellman协议导出本轮会话密钥$EK||AK = KDF(N_G^b)$。使用两方发送的随机数，可以定义出下一次接入时要使用的PUF挑战值C_{init}＝H(N_G||N_E)，并使用本地PUF生成相应的响应值R_{init}＝PUF_E(C_{init})。随后，外部设备将新生成的PUF响应值和两个随机数一同使用GECU的公钥加密，生成加密值$CT = ENC_{pk_G}(R_{init}||N_E||N_G)$，并计算出数字签名$S_E = Sig_{sk_E}(N_E||R_{init})$以保证数据完整性和认证性。最终，外部设备将自身的数字证书、加密值和数字签名值($Cert_E$，CT，S_E)发送给GECU。

[0079] 步骤8：GECU在接收到消息后，可以解密得到外部设备新生成的PUF响应值和随机数$R_{init}||N_E||N_G = DEC_{sk_G}(CT)$，并校验$N_E||R_{init} = Vrfy_{pk_E}(S_E)$是否成立。若校验通过，则生成PUF挑战值$C_{init}$＝H($N_G$||$N_E$)，并将外部设备ID、PUF挑战值、PUF响应值三元组(ID_E，C_{init}，R_{init})安全存储在数据库中。最终，GECU也可使用Diffie-Hellman协议导出本轮会话密钥$EK||AK = KDF(N_E^a)$，并计算校验值Auth＝H(AK||R_{init}||N_G||N_E)发送给外部设备，确认本

轮密钥协商的正确性。

[0080] 模块三:外部设备接入模块具体由三个步骤实现,以外部设备第i次接入车内GECU为例说明:

[0081] 步骤9:GECU首先通过待接入外部设备的ID检索数据库,读取上一轮约定好的PUF挑战值和响应值(C_i,R_i)。随后,GECU生成随机数N_1。使用该随机数对PUF响应值加密$Mask_1 = N_1 \oplus R_i$,并生成一个校验值$Auth_1 = H(N_1||R_i)$。最终,GECU将PUF挑战值、加密值和校验值三元组(C_i,$Mask_1$,$Auth_1$)发送给外部设备。

[0082] 步骤10:外部设备接收到消息后,根据PUF挑战值生成对应的响应值$R_i = PUF_E(C_i)$,并使用该响应值解密得到GECU生成的随机数$N_1 = Mask_1 \oplus R_i$。根据新生成的数据,若$Auth_1$校验通过,则生成一个新的随机数N_2,并导出本轮的会话密钥$EK||AK = KDF(N_1||N_2)$。随后,外部设备可以导出下一次接入时要使用的PUF挑战值$C_{i+1} = H(C_i||N_1||N_2)$和响应值$R_{i+1} = PUF_E(C_{i+1})$。最终,外部设备将新生成的PUF响应值和随机数加密生成$Mask_2 = N_2 \oplus R_{i+1}$和$Mask_3 = N_1 \oplus N_2$,计算校验值$Auth_2 = H(N_1||N_2||R_{i+1})$,将三元组($Mask_2$,$Mask_3$,$Auth_2$)发送给GECU。

[0083] 步骤11:GECU在收到消息后,可以解密得到$N_2 = N_1 \oplus Mask_3$和$R_{i+1} = N_2 \oplus Mask_2$。若$Auth_2$能够校验通过,则GECU可以计算下一次会话所需的PUF挑战值$C_{i+1} = H(C_i||N_1||N_2)$,并将数据库中保存的三元组更新为($ID_E$,$C_{i+1}$,$R_{i+1}$)。最后,GECU可以导出本轮会话密钥$EK||AK = KDF(N_1||N_2)$,完成全部身份认证与密钥协商功能。

[0084] 根据本发明实施例提出的基于PUF的车内网络CAN总线轻量级安全通信方法,通过借助可在CAN总线设备内实现的PUF技术,可以实现车辆内部的轻量级认证与密钥协商协议,同时满足对总线设备的对等实体认证等安全需求,可以确保重放、伪造等攻击无法对认证和密钥协商造成威胁及损失。基于PUF的CAN总线外部设备接入协议仅需在车辆与外部设备首次连接时使用基于非对称密码技术。

[0085] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0086] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0087] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

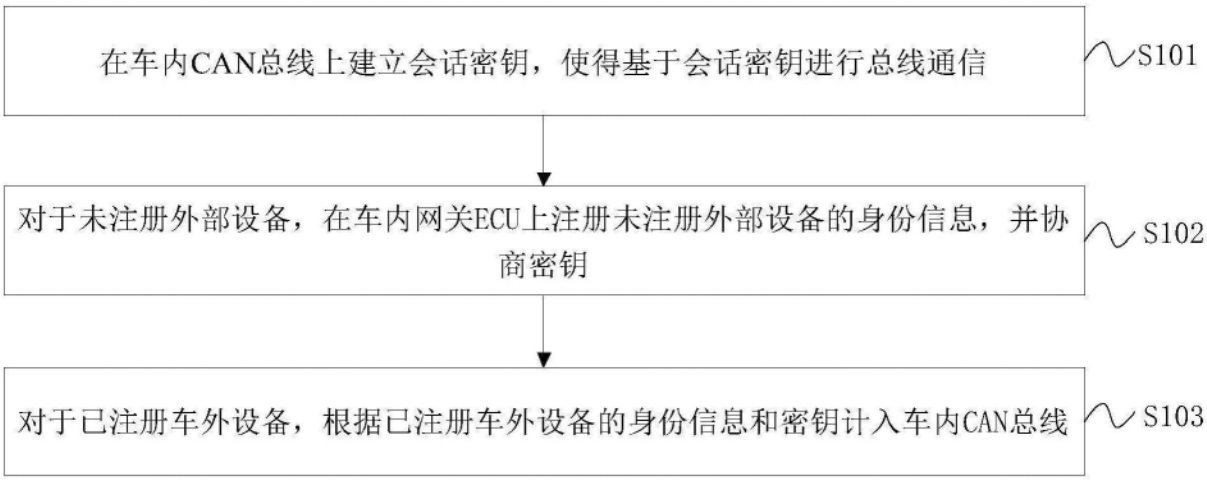

在车内CAN总线上建立会话密钥，使得基于会话密钥进行总线通信
S101
对于未注册外部设备，在车内网关ECU上注册未注册外部设备的身份信息，并协商密钥
S102
对于已注册车外设备，根据已注册车外设备的身份信息和密钥计入车内CAN总线
S103

图1

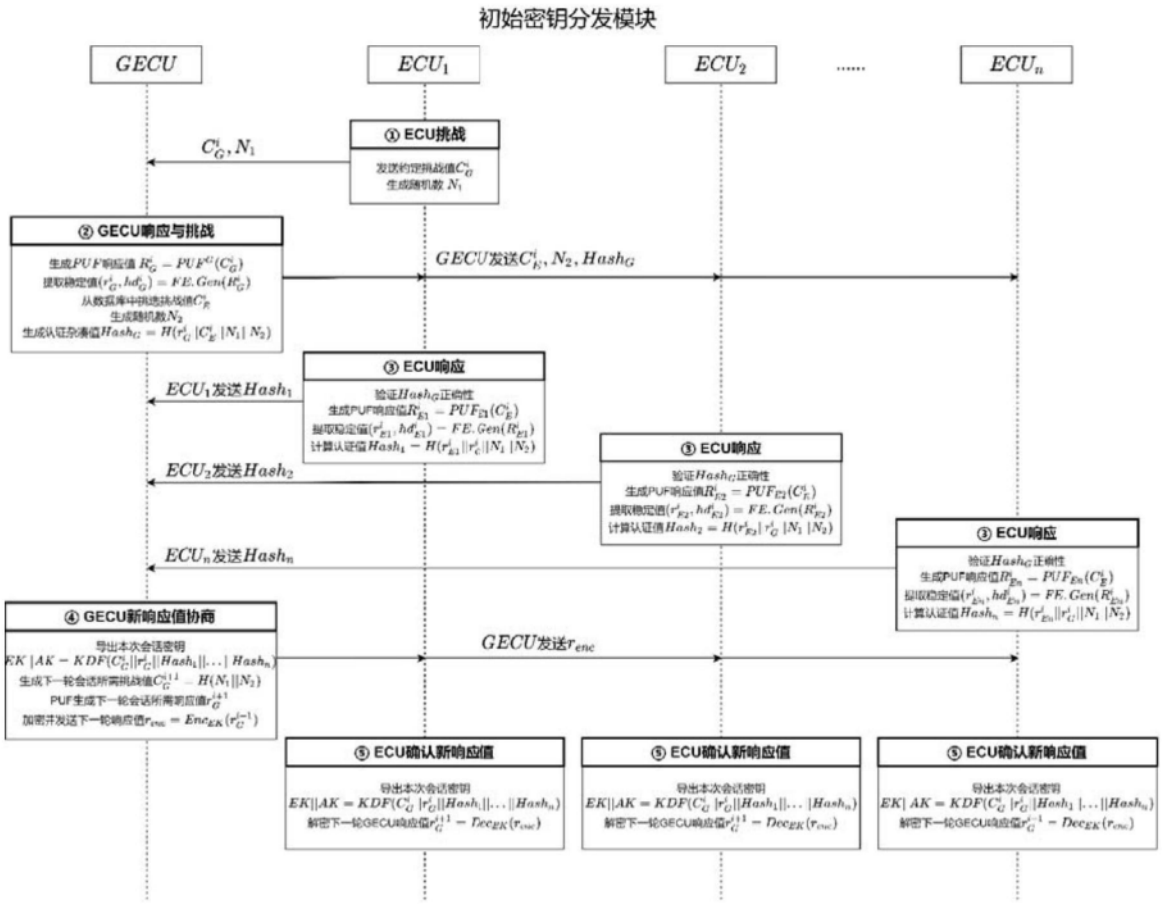

初始密钥分发模块
GECU
ECU1
ECU2
.....
ECUn
① ECU挑战
发送初始挑战值 C_G^i
生成随机数 N_1
C_G^i, N_1
② GECU响应与挑战
生成PUF响应值 $R_G^i = PUF^G(C_G^i)$
提取稳定值 $(r_G^i, hd_G^i) = FE.Gen(R_G^i)$
从数据库中挑选挑战值 C_E^i
生成随机数 N_2
生成认证杂凑值 $Hash_G = H(r_G^i | C_E^i | N_1 | N_2)$
GECU发送 $C_E^i, N_2, Hash_G$
③ ECU响应
验证 $Hash_G$ 正确性
生成PUF响应值 $R_{E1}^i = PUF_{E1}(C_E^i)$
提取稳定值 $(r_{E1}^i, hd_{E1}^i) = FE.Gen(R_{E1}^i)$
计算认证值 $Hash_1 = H(r_{E1}^i || r_G^i | N_1 | N_2)$
ECU_1发送 $Hash_1$
③ ECU响应
验证 $Hash_G$ 正确性
生成PUF响应值 $R_{E2}^i = PUF_{E2}(C_E^i)$
提取稳定值 $(r_{E2}^i, hd_{E2}^i) = FE.Gen(R_{E2}^i)$
计算认证值 $Hash_2 = H(r_{E2}^i | r_G^i | N_1 | N_2)$
ECU_2发送 $Hash_2$
③ ECU响应
验证 $Hash_G$ 正确性
生成PUF响应值 $R_{En}^i = PUF_{En}(C_E^i)$
提取稳定值 $(r_{En}^i, hd_{En}^i) = FE.Gen(R_{En}^i)$
计算认证值 $Hash_n = H(r_{En}^i || r_G^i | N_1 | N_2)$
ECU_n发送 $Hash_n$
④ GECU新响应值协商
导出本次会话密钥
$EK | AK = KDF(C_G^i || r_G^i || Hash_1 || \dots | Hash_n)$
生成下一轮会话所需挑战值 $C_G^{i+1} = H(N_1 || N_2)$
PUF生成下一轮会话所需响应值 r_G^{i+1}
加密并发送下一轮响应值 $r_{enc} = Enc_{EK}(r_G^{i-1})$
GECU发送 r_{enc}
⑤ ECU确认新响应值
导出本次会话密钥
$EK || AK = KDF(C_G^i || r_G^i || Hash_1 || \dots || Hash_n)$
解密下一轮GECU响应值 $r_G^{i+1} = Dec_{EK}(r_{enc})$
⑤ ECU确认新响应值
导出本次会话密钥
$EK || AK = KDF(C_G^i || r_G^i || Hash_1 || \dots || Hash_n)$
解密下一轮GECU响应值 $r_G^{i+1} = Dec_{EK}(r_{enc})$
⑤ ECU确认新响应值
导出本次会话密钥
$EK | AK = KDF(C_G^i || r_G^i || Hash_1 | \dots | Hash_n)$
解密下一轮GECU响应值 $r_G^{i-1} = Dec_{EK}(r_{enc})$

图2

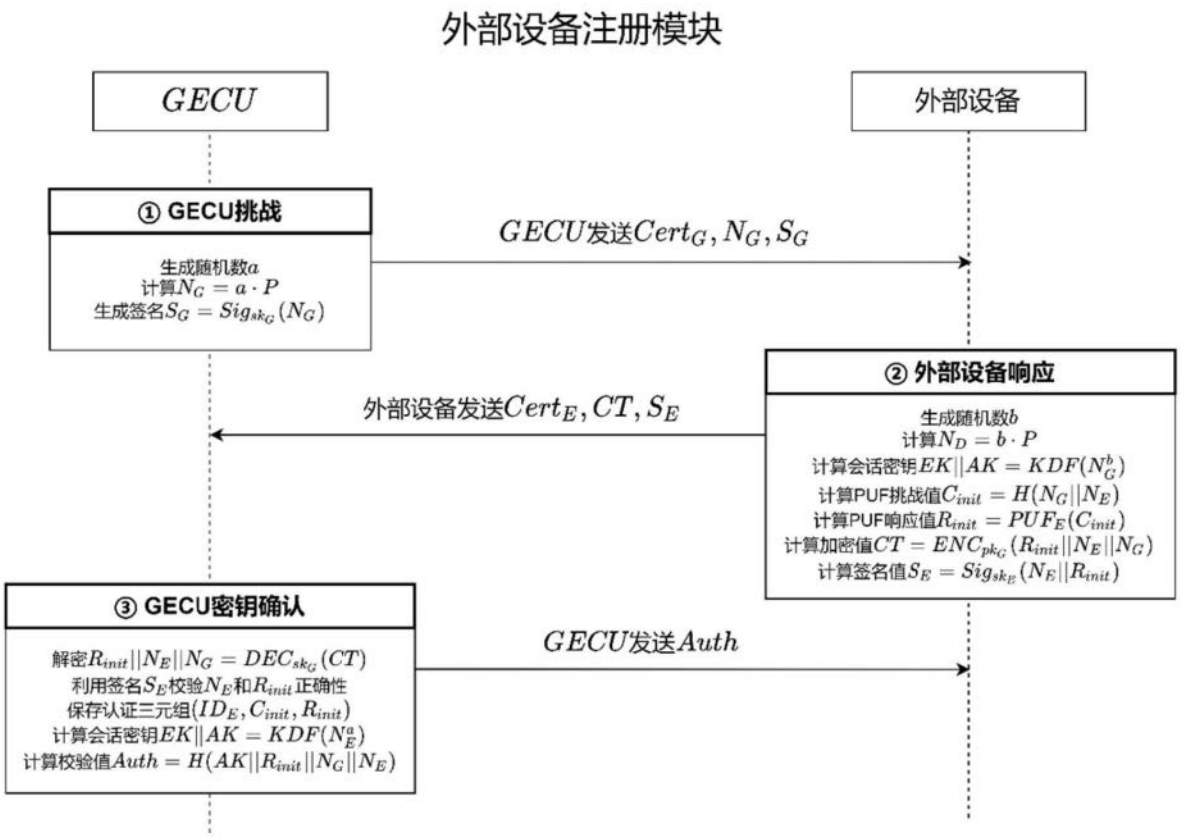

外部设备注册模块
GECU
外部设备
① GECU挑战
生成随机数a
计算$N_G = a \cdot P$
生成签名$S_G = Sig_{sk_G}(N_G)$
$GECU$发送$Cert_G, N_G, S_G$
② 外部设备响应
生成随机数b
计算$N_D = b \cdot P$
计算会话密钥$EK||AK = KDF(N_G^b)$
计算PUF挑战值$C_{init} = H(N_G||N_E)$
计算PUF响应值$R_{init} = PUF_E(C_{init})$
计算加密值$CT = ENC_{pk_G}(R_{init}||N_E||N_G)$
计算签名值$S_E = Sig_{sk_E}(N_E||R_{init})$
外部设备发送$Cert_E, CT, S_E$
③ GECU密钥确认
解密$R_{init}||N_E||N_G = DEC_{sk_G}(CT)$
利用签名S_E校验N_E和R_{init}正确性
保存认证三元组$(ID_E, C_{init}, R_{init})$
计算会话密钥$EK||AK = KDF(N_E^a)$
计算校验值$Auth = H(AK||R_{init}||N_G||N_E)$
$GECU$发送$Auth$

图3

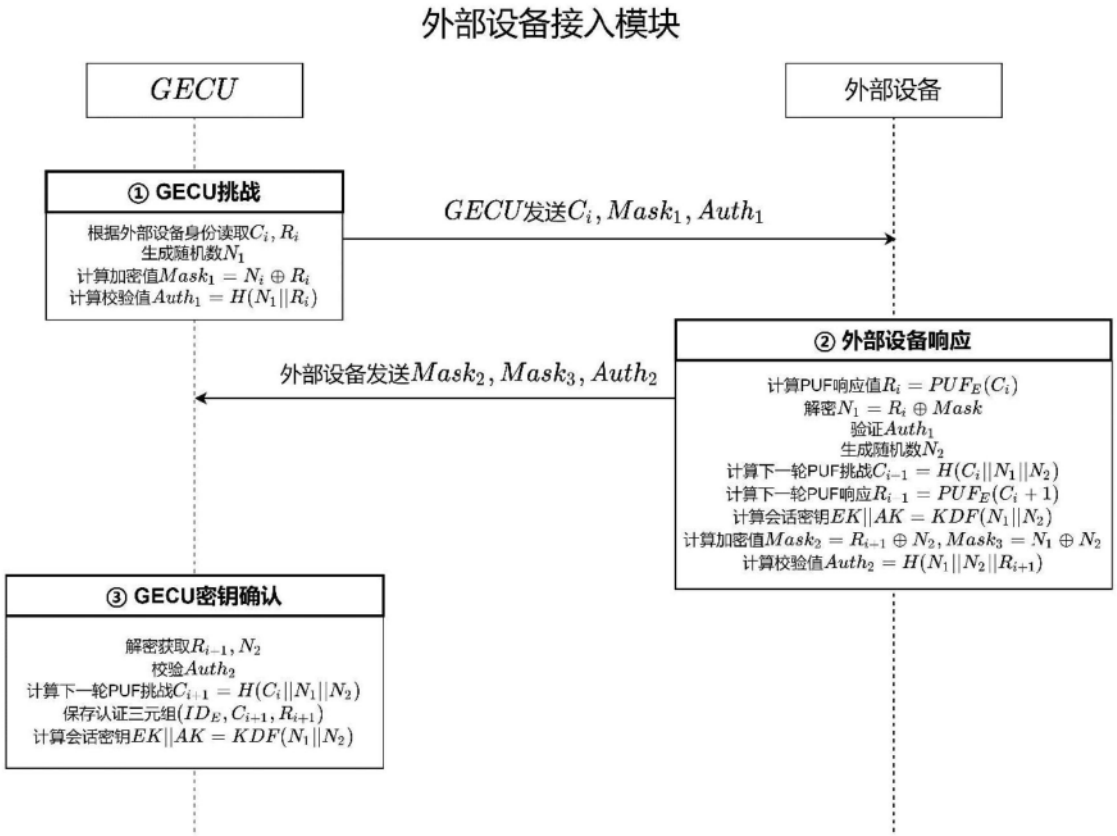

外部设备接入模块
GECU
外部设备
① GECU挑战
根据外部设备身份读取C_i, R_i
生成随机数N_1
计算加密值$Mask_1 = N_i \oplus R_i$
计算校验值$Auth_1 = H(N_1||R_i)$
$GECU$发送$C_i, Mask_1, Auth_1$
② 外部设备响应
计算PUF响应值$R_i = PUF_E(C_i)$
解密$N_1 = R_i \oplus Mask$
验证$Auth_1$
生成随机数N_2
计算下一轮PUF挑战$C_{i-1} = H(C_i||N_1||N_2)$
计算下一轮PUF响应$R_{i\ 1} = PUF_E(C_i + 1)$
计算会话密钥$EK||AK = KDF(N_1||N_2)$
计算加密值$Mask_2 = R_{i-1} \oplus N_2, Mask_3 = N_1 \oplus N_2$
计算校验值$Auth_2 = H(N_1||N_2||R_{i+1})$
外部设备发送$Mask_2, Mask_3, Auth_2$
③ GECU密钥确认
解密获取R_{i-1}, N_2
校验$Auth_2$
计算下一轮PUF挑战$C_{i+1} = H(C_i||N_1||N_2)$
保存认证三元组(ID_E, C_{i+1}, R_{i+1})
计算会话密钥$EK||AK = KDF(N_1||N_2)$

图4