(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113315636 B
(45)授权公告日 2022.02.25

(21)申请号 202110597211.8
(22)申请日 2021.05.31
(65)同一申请的已公布的文献号
申请公布号 CN 113315636 A
(43)申请公布日 2021.08.27
(73)专利权人 暨南大学
地址 510632 广东省广州市天河区黄埔大道西601号
(72)发明人 孙恒 邱培超 翁健 刘志全 罗智耀
(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 郑秋松
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 12/40(2006.01)
(56)对比文件
CN 110492995 A,2019.11.22
CN 101291214 A,2008.10.22
CN 106603483 A,2017.04.26
US 2018006810 A1,2018.01.04
肖亚飞.Diffie-Hellman协议密钥交互系统的研究.《电脑知识与技术》.2018,(第03期),
审查员 张小环

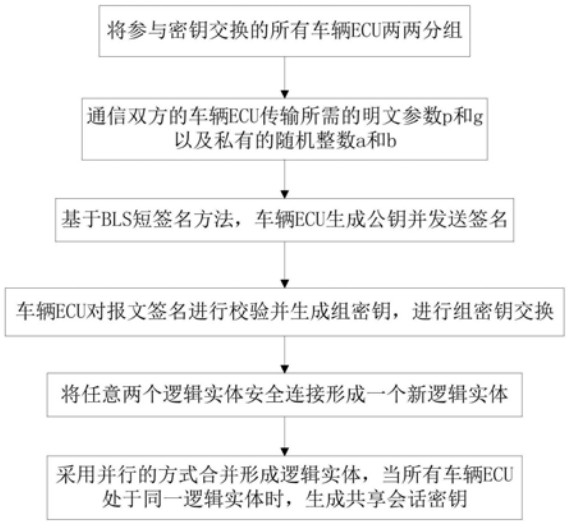
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种用于汽车ECU间安全通信的密钥交换方法

(57)摘要

本发明公开了一种用于汽车ECU间安全通信的密钥交换方法,该方法包括下述步骤:将参与密钥交换的所有车辆ECU两两分组;通信双方的车辆ECU直接传输所需的明文参数以及私有的随机整数;车辆ECU生成公钥并发送签名;车辆ECU对报文签名进行校验并生成组密钥,进行组密钥交换;将任意两个逻辑实体安全连接形成一个新逻辑实体,双方逻辑实体互相验证身份后发送已有组密钥,接收方将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算;采用并行的方式合并形成逻辑实体,当所有车辆ECU处于同一逻辑实体时,生成共享会话密钥。本发明完成ECU之间密钥交换所需存储资源小、消耗计算资源少,适合于有限的CAN总线容量。



CN 113315636 B

1.一种用于汽车ECU间安全通信的密钥交换方法,其特征在于,包括下述步骤:

将参与密钥交换的所有车辆ECU两两分组;

通信双方的车辆ECU直接传输所需的Diffie-Hellman明文参数p和g以及私有的随机整数a和b,通信双方的车辆ECU包括发送方ECU_1和接收方ECU_2,发送方ECU_1和接收方ECU_2单独计算变量$E_1=g^a \bmod p$、$E_2=g^b \bmod p$;

基于BLS短签名方法,车辆ECU生成公钥并发送签名;

车辆ECU对报文签名进行校验并生成组密钥,进行组密钥交换,交换组密钥后的发送方ECU_1和接收方ECU_2为同一逻辑实体;将任意两个逻辑实体安全连接形成一个新逻辑实体,当一个逻辑实体与另一个逻辑实体进行合并时,双方逻辑实体互相验证身份后发送已有组密钥,接收方接收后,将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算;

所述将任意两个逻辑实体安全连接形成一个新逻辑实体,具体步骤包括:

第一逻辑实体内部ECU分别具有私钥$a_1,a_2,a_3,\cdots a_i$,第二逻辑实体内部ECU私钥为$b_1,b_2,b_3,\cdots b_j$,所述第一逻辑实体内部的ECU数目i与第二逻辑实体内部ECU数目j满足关系$|i-j|\leqslant 1$;采用并行的方式合并形成逻辑实体,当所有车辆ECU处于同一逻辑实体时,生成共享会话密钥;

共享会话密钥表示为:

$BK^*=\text{power}(BK_2,a_1a_2a_3\cdots a_i) \bmod p=\text{power}(BK_1,b_1b_2b_3\cdots b_j) \bmod p$

其中,power表示数字乘幂函数,BK_1表示第一逻辑实体的组密钥,BK_2表示第二逻辑实体的组密钥。

2.根据权利要求1所述的用于汽车ECU间安全通信的密钥交换方法,其特征在于,所述将参与密钥交换的所有车辆ECU两两分组,每一分组作为一个逻辑实体,所有ECU若数量为奇数,剩余的ECU作为单独逻辑实体。

3.根据权利要求1所述的用于汽车ECU间安全通信的密钥交换方法,其特征在于,所述车辆ECU生成公钥并发送签名,具体步骤包括:

发送方ECU_1选取接收方ECU_2的椭圆曲线生成点G_1产生公钥$P_1=a\times G_1$,采用椭圆曲线哈希函数$H(E_1)$计算签名$S_1=a\times H(E_1)$后,发送方ECU_1将数字签名S_1发送至接收方ECU_2;

接收方ECU_2选取发送方ECU_1的椭圆曲线生成点G_2产生公钥$P_2=b\times G_2$,采用椭圆曲线哈希函数$H(E_2)$计算签名$S_2=b\times H(E_2)$后,接收方ECU_2将数字签名S_2发送至发送方ECU_1。

4.根据权利要求1所述的用于汽车ECU间安全通信的密钥交换方法,其特征在于,所述车辆ECU对报文签名进行校验并生成组密钥,具体步骤包括:

接收方ECU_2接收到发送方ECU_1的签名信息时,由BLS短签名方法计算双线性映射函数e,若满足$e(P_1,H(E_1))=e(G_1,S_1)$,则接收签名信息;

接收方ECU_2接收信息后,解密E_1并计算$S_1^* = (E_1)^b \bmod p$,

其中,S_1^*是组密钥,E_1^b表示E_1的b次幂;

发送方ECU_1接收到接收方ECU_2的签名信息时,若满足$e(P_2,H(E_2))=e(G_2,S_2)$,则接收签名信息;

发送方ECU_1接收信息后,解密E_2并计算组密钥$S_2^* = (E_2)^a \bmod p$,

其中，S_2^*是组密钥，E_2^a表示E_2的a次幂；

若S_1^*等于S_2^*，则交换后的组密钥$S^*= S_1^* = S_2^*$。

5.一种用于汽车ECU间安全通信的密钥交换系统，其特征在于，包括：分组模块、参数传输模块、变量计算模块、签名模块、签名校验模块、组密钥生成及交换模块、逻辑实体合并模块、共享会话密钥输出模块；

所述分组模块用于将参与密钥交换的所有车辆ECU两两分组；

所述参数传输模块用于传输通信双方的车辆ECU所需的Diffie-Hellman明文参数p和g以及私有的随机整数a和b，通信双方的车辆ECU包括发送方ECU_1和接收方ECU_2；

所述变量计算模块用于单独计算变量$E_1=g^a \bmod p$、$E_2=g^b \bmod p$；

所述签名模块用于基于BLS短签名方法，生成车辆ECU公钥及签名；

所述签名校验模块用于对报文签名进行校验；

所述组密钥生成及交换模块用于生成组密钥并进行组密钥交换，交换组密钥后的发送方ECU_1和接收方ECU_2为同一逻辑实体；

所述逻辑实体合并模块用于将任意两个逻辑实体安全连接形成一个新逻辑实体，当一个逻辑实体与另一个逻辑实体进行合并时，双方逻辑实体互相验证身份后发送已有组密钥，接收方接收后，将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算；

所述将任意两个逻辑实体安全连接形成一个新逻辑实体，具体步骤包括：

第一逻辑实体内部ECU分别具有私钥$a_1,a_2,a_3,\cdots a_i$，第二逻辑实体内部ECU私钥为$b_1,b_2,b_3,\cdots b_j$，所述第一逻辑实体内部的ECU数目i与第二逻辑实体内部ECU数目j满足关系$|i-j|\leq 1$；所述共享会话密钥输出模块用于输出共享会话密钥，采用并行的方式合并形成逻辑实体，当所有车辆ECU处于同一逻辑实体时，生成共享会话密钥；

共享会话密钥表示为：

$$BK^*=\text{power}(BK_2,a_1a_2a_3\cdots a_i)\bmod p=\text{power}(BK_1,b_1b_2b_3\cdots b_j)\bmod p$$

其中，power表示数字乘幂函数，BK_1表示第一逻辑实体的组密钥，BK_2表示第二逻辑实体的组密钥。

6.一种存储介质，存储有程序，其特征在于，所述程序被处理器执行时实现如权利要求1-4任一项所述用于汽车ECU间安全通信的密钥交换方法。

7.一种计算设备，包括处理器和用于存储处理器可执行程序的存储器，其特征在于，所述处理器执行存储器存储的程序时，实现如权利要求1-4任一项所述用于汽车ECU间安全通信的密钥交换方法。

一种用于汽车ECU间安全通信的密钥交换方法

技术领域

[0001] 本发明涉及汽车ECU安全通信技术领域，具体涉及一种用于汽车ECU间安全通信的密钥交换方法。

背景技术

[0002] 随着汽车内部ECU的增多，汽车内部ECU的通信越加重要，但是汽车内部总线的传输并不安全。在汽车行驶的时候，汽车内部ECU需要快速、高效、安全地通信，以保证人员安全。虽然Diffie-Hellman算法仅当需要时才生成密钥，减少了密钥长时间存储而产生的泄露风险，但是缺乏身份验证，易遭受第三方的攻击。当前的加密方案涉及密钥分发，这需要消耗大量资源。为此，在资源受限的汽车ECU和总线环境中急需一种安全、高效的密钥交换方法。

发明内容

[0003] 为了克服现有技术存在的缺陷与不足，本发明提供一种用于汽车ECU间安全通信的密钥交换方法，本发明的密钥交换方法存储资源占用少、签名校验速度快、共享密钥生成高效，满足车辆行驶过程中对总线报文进行实时加密的要求。

[0004] 本发明的第二目的在于提供一种用于汽车ECU间安全通信的密钥交换系统。

[0005] 本发明的第三目的在于提供一种存储介质。

[0006] 本发明的第四目的在于提供一种计算设备。

[0007] 为了达到上述目的，本发明采用以下技术方案：

[0008] 本发明提供一种用于汽车ECU间安全通信的密钥交换方法，包括下述步骤：

[0009] 将参与密钥交换的所有车辆ECU两两分组；

[0010] 通信双方的车辆ECU直接传输所需的Diffie-Hellman明文参数p和g以及私有的随机整数a和b，通信双方的车辆ECU包括发送方ECU_1和接收方ECU_2，发送方ECU_1和接收方ECU_2单独计算变量$E_1=g^a \bmod p$、$E_2=g^b \bmod p$；

[0011] 基于BLS短签名方法，车辆ECU生成公钥并发送签名；

[0012] 车辆ECU对报文签名进行校验并生成组密钥，进行组密钥交换，交换组密钥后的发送方ECU_1和接收方ECU_2为同一逻辑实体；

[0013] 将任意两个逻辑实体安全连接形成一个新逻辑实体，当一个逻辑实体与另一个逻辑实体进行合并时，双方逻辑实体互相验证身份后发送已有组密钥，接收方接收后，将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算；

[0014] 采用并行的方式合并形成逻辑实体，当所有车辆ECU处于同一逻辑实体时，生成共享会话密钥。

[0015] 作为优选的技术方案，所述将参与密钥交换的所有车辆ECU两两分组，每一分组作为一个逻辑实体，所有ECU若数量为奇数，剩余的ECU作为单独逻辑实体。

[0016] 作为优选的技术方案，所述车辆ECU生成公钥并发送签名，具体步骤包括：

[0017] 发送方ECU_1选取接收方ECU_2的椭圆曲线生成点G_1产生公钥$P_1=a\times G_1$，采用椭圆曲线哈希函数$H(E_1)$计算签名$S_1=a\times H(E_1)$后，发送方ECU_1将数字签名S_1发送至接收方ECU_2；

[0018] 接收方ECU_2选取发送方ECU_1的椭圆曲线生成点G_2产生公钥$P_2=b\times G_2$，采用椭圆曲线哈希函数$H(E_2)$计算签名$S_2=b\times H(E_2)$后，接收方ECU_2将数字签名S_2发送至发送方ECU_1。

[0019] 作为优选的技术方案，所述车辆ECU对报文签名进行校验并生成组密钥，具体步骤包括：

[0020] 接收方ECU_2接收到发送方ECU_1的签名信息时，由BLS短签名方法计算双线性映射函数e，若满足$e(P_1,H(E_1))=e(G_1,S_1)$，则接收签名信息；

[0021] 接收方ECU_2接收信息后，解密E_1并计算$S_1^* = (E_1)^b \bmod p$，

[0022] 其中，S_1^*是组密钥，E_1^b表示E_1的b次幂；

[0023] 发送方ECU_1接收到接收方ECU_2的签名信息时，若满足$e(P_2,H(E_2))=e(G_2,S_2)$，则接收签名信息；

[0024] 发送方ECU_1接收信息后，解密E_2并计算组密钥$S_2^* = (E_2)^a \bmod p$，

[0025] 其中，S_2^*是组密钥，E_2^a表示E_2的a次幂；

[0026] 若S_1^*等于S_2^*，则交换后的组密钥$S^* = S_1^* = S_2^*$。

[0027] 作为优选的技术方案，所述将任意两个逻辑实体安全连接形成一个新逻辑实体，具体步骤包括：

[0028] 第一逻辑实体内部ECU分别具有私钥$a_1,a_2,a_3,\cdots a_i$，第二逻辑实体内部ECU私钥为$b_1,b_2,b_3,\cdots b_j$，所述第一逻辑实体内部的ECU数目i与第二逻辑实体内部ECU数目j满足关系$|i-j|\leqslant 1$；

[0029] 共享会话密钥表示为：

[0030] $BK^*=power(BK_2,a_1a_2a_3\cdots a_i)\bmod p=power(BK_1,b_1b_2b_3\cdots b_j)\bmod p$

[0031] 其中，power表示数字乘幂函数，BK_1表示第一逻辑实体的组密钥，BK_2表示第二逻辑实体的组密钥。

[0032] 为了达到上述第二目的，本发明采用以下技术方案：

[0033] 一种用于汽车ECU间安全通信的密钥交换系统，包括：分组模块、参数传输模块、变量计算模块、签名模块、签名校验模块、组密钥生成及交换模块、逻辑实体合并模块、共享会话密钥输出模块；

[0034] 所述分组模块用于将参与密钥交换的所有车辆ECU两两分组；

[0035] 所述参数传输模块用于传输通信双方的车辆ECU所需的Diffie-Hellman明文参数p和g以及私有的随机整数a和b，通信双方的车辆ECU包括发送方ECU_1和接收方ECU_2；

[0036] 所述变量计算模块用于单独计算变量$E_1=g^a \bmod p$、$E_2=g^b \bmod p$；

[0037] 所述签名模块用于基于BLS短签名方法，生成车辆ECU公钥及签名；

[0038] 所述签名校验模块用于对报文签名进行校验；

[0039] 所述组密钥生成及交换模块用于生成组密钥并进行组密钥交换，交换组密钥后的发送方ECU_1和接收方ECU_2为同一逻辑实体；

[0040] 所述逻辑实体合并模块用于将任意两个逻辑实体安全连接形成一个新逻辑实体，

当一个逻辑实体与另一个逻辑实体进行合并时，双方逻辑实体互相验证身份后发送已有组密钥，接收方接收后，将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算；

[0041] 所述共享会话密钥输出模块用于输出共享会话密钥，采用并行的方式合并形成逻辑实体，当所有车辆ECU处于同一逻辑实体时，生成共享会话密钥。

[0042] 为了达到上述第三目的，本发明采用以下技术方案：

[0043] 一种存储介质，存储有程序，所述程序被处理器执行时实现如上述用于汽车ECU间安全通信的密钥交换方法。

[0044] 为了达到上述第四目的，本发明采用以下技术方案：

[0045] 一种计算设备，包括处理器和用于存储处理器可执行程序的存储器，所述处理器执行存储器存储的程序时，实现如上述用于汽车ECU间安全通信的密钥交换方法。

[0046] 本发明与现有技术相比，具有如下优点和有益效果：

[0047] (1)本发明用于资源受限的汽车内部环境，具有以下优势：本发明的方法是轻量级的，完成ECU之间密钥交换所需存储资源小、消耗计算资源少，适合于有限的CAN总线容量。

[0048] (2)与传统Diffie-Hellman算法相比，本发明借助BLS(Boneh-Lynn-Shacham)短签名能有效防止中间人攻击，保护CAN总线的安全性。

[0049] (3)本发明基于Diffie-Hellman算法和BLS的密钥交换适合于CAN总线的广播通信环境，且字节级长度的共享密钥可直接写入CAN帧，避免了密钥交换过程中总线过载，提升了本发明与现有CAN协议的兼容性。

附图说明

[0050] 图1为本发明用于汽车ECU间安全通信的密钥交换方法的流程示意图；

[0051] 图2为本发明汽车ECU密钥交换方案示意图；

[0052] 图3为本发明汽车共享会话密钥生成示意图。

具体实施方式

[0053] 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。

[0054] 实施例

[0055] 如图1所示，本实施例提供一种用于汽车ECU间安全通信的密钥交换方法，在车内网资源有限的环境下，通过密钥交换使得ECU之间的通信更为安全，结合Diffie-Hellman密钥交换和BLS短签名方案，吸取了BLS短签名的认证方法，避免了传统的Diffie-Hellman算法易遭受中间人攻击的缺点，同时本发明采用并行ECU分组可以快速地实现ECU身份认证下的密钥交换，包括下述步骤：

[0056] S1:将参与密钥交换的所有ECU两两分组；

[0057] 本实施例的所有ECU两两分组能够加快组内有限数量ECU快速完成密钥交换，且便于并发计算组密钥。

[0058] 本实施例的所有ECU若数量为奇数，剩余的ECU作为单独逻辑实体，其余每一分组

看作一个逻辑实体。实体内两个ECU可以凭借已经交换的组密钥进行安全通信。

[0059] S2:通信双方ECU选择直接传输所需的明文参数p和g以及私有的随机整数a和b;

[0060] 本实施例的Diffie-Hellman明文参数p和g为通信双方ECU公认的整数,p是素数,g是p的原根,a是发送方ECU生成小于p的随机整数,b是接收方ECU生成小于p的随机整数,发送方ECU_1和接收方ECU_2单独计算变量$E_1=g^a \bmod p$,$E_2=g^b \bmod p$,如图2所示,组内及组间ECU均可同步发送签名并完成校验。

[0061] S3:车辆ECU生成公钥P,并发送签名S;

[0062] 根据BLS短签名方法,发送方ECU_1选取接收方ECU_2的椭圆曲线生成点G_1产生公钥$P_1=a\times G_1$,运用椭圆曲线哈希函数$H(E_1)$计算签名$S_1=a\times H(E_1)$后,ECU_1立即将数字签名S_1发送至ECU_2。同时,接收方ECU_2选取发送方ECU_1的椭圆曲线生成点G_2产生公钥$P_2=b\times G_2$,运用椭圆曲线哈希函数$H(E_2)$计算签名$S_2=b\times H(E_2)$后,ECU_2立即将数字签名S_2发送至ECU_1。

[0063] S4:车辆ECU对报文签名进行校验,并生成组密钥;

[0064] 接收方ECU_2接收到发送方ECU_1的签名信息时,由BLS短签名方法计算双线性映射函数e,若满足$e(P_1,H(E_1))=e(G_1,S_1)$,则接收签名信息,否则丢弃。接收方ECU_2接收信息后,解密E_1并计算$S_1^* = (E_1)^b \bmod p$,S_1^*是组密钥,E_1^b表示E_1的b次幂,p是步骤S2提到的素数。发送方ECU_1接收到接收方ECU_2的签名信息时,若$e(P_2,H(E_2))=e(G_2,S_2)$,则接收签名信息,否则丢弃。发送方ECU_1接收信息后,解密E_2,并计算组密钥$S_2^* = (E_2)^a \bmod p$,S_2^*是组密钥,E_2^a表示E_2的a次幂。若S_1^*等于S_2^*,则交换后的组密钥$S^*= S_1^* = S_2^*$,此时ECU_1和ECU_2被看作同一逻辑实体;若S_1^*不等于S_2^*,则组密钥交换失败。

[0065] 本实施例的ECU组密钥长度取决于所选取的椭圆曲线,当选定了椭圆曲线后,生成点和ECU的数量不会影响密钥长度。椭圆曲线的位数越大,密钥长度越大,安全等级越高,但计算时间也越长。密钥长度在车内通信环境中,选择256位即可满足CAN总线安全性要求,且小于CAN-FD报文中数据域64字节上限,与现有协议兼容。

[0066] S5:合并逻辑实体,生成统一的共享会话密钥,本实施例的共享会话密钥由逻辑实体合并生成。

[0067] 将任意两个逻辑实体安全连接形成一个新逻辑实体。采取并行的方式,当第一分组在形成逻辑实体时,第二分组也形成逻辑实体。同样的,其他新的逻辑实体也在这时并行生成。当所有ECU处于同一逻辑实体时,共享会话密钥生成,各ECU有各自私有的私钥且共享同一共享会话密钥,所有ECU之间可以进行安全高效地通信。

[0068] 当一个逻辑实体与另一个逻辑实体进行合并的时候,只需要执行BLS短签名方案,双方逻辑实体互相验证身份后发送已有密钥BK_1、BK_2,接收方接收后,将发送方的密钥与逻辑实体内部各个ECU的私钥都进行幂运算。在本实施例中,组内ECU交换密钥时幂运算指数所使用的随机参数为ECU的私钥,即私有整数a为ECU的私钥;逻辑实体间合并时幂运算指数为实体内部ECU私钥。

[0069] 第一个逻辑实体内部ECU分别具有私钥$a_1,a_2,a_3,\cdots a_i$,另一具有相同或i±1ECU数目的逻辑实体内部ECU私钥为$b_1,b_2,b_3,\cdots b_j$,,则第一个将生成与第二个相等的$BK^*=power(BK_2,a_1a_2a_3\cdots a_i)\bmod p=power(BK_1,b_1b_2b_3\cdots b_j)\bmod p$。

[0070] 如图3所示,逻辑实体在产生共享会话密钥的过程中,逻辑实体(ECU_1,ECU_2)发送

$Level_2$组密钥BK_1至逻辑实体(ECU_3,ECU_4)，具有$Level_2$组密钥BK_2的逻辑实体(ECU_3,ECU_4)在接收BK_1后使用私钥计算$Level_1$组密钥$(BK_5)_1^* = (BK_2)^{a1a2} \bmod p$。其中，$a_1$、$a_2$表示逻辑实体$(ECU_1,ECU_2)$私钥，同时，逻辑实体$(ECU_3,ECU_4)$发送组密钥$BK_2$至逻辑实体$(ECU_1,ECU_2)$，逻辑实体$(ECU_1,ECU_2)$在接收$BK_2$后使用私钥计算$Level_1$组密钥$(BK_5)_2^* = (BK_1)^{a3a4} \bmod p$，其中，$a_3$、$a_4$表示逻辑实体$(ECU_3,ECU_4)$私钥。若$(BK_5)_1^* = (BK_5)_2^*$，则$BK_5$为上述两逻辑实体合并后的$Level_1$组密钥。在左子树生成$BK_5$的过程中，右子树采取相同的方法并行生成了$Level_1$组密钥$BK_6$。类似地，逻辑实体$(ECU_1,ECU_2,ECU_3,ECU_4)$与逻辑实体$(ECU_5,ECU_6,ECU_7,ECU_8)$合并，最终得到$Level_0$组密钥$BK^*$，即合并后的共享会话密钥。

[0071] 本发明的密钥交换方法存储资源占用少、签名校验速度快、共享密钥生成高效，满足车辆行驶过程中对总线报文进行实时加密的要求。

[0072] 实施例2

[0073] 本实施例提供一种用于汽车ECU间安全通信的密钥交换系统，包括：分组模块、参数传输模块、变量计算模块、签名模块、签名校验模块、组密钥生成及交换模块、逻辑实体合并模块、共享会话密钥输出模块；

[0074] 在本实施例中，分组模块用于将参与密钥交换的所有车辆ECU两两分组；

[0075] 在本实施例中，参数传输模块用于传输通信双方的车辆ECU所需的Diffie-Hellman明文参数p和g以及私有的随机整数a和b，通信双方的车辆ECU包括发送方ECU_1和接收方ECU_2；

[0076] 在本实施例中，变量计算模块用于单独计算变量$E_1 = g^a \bmod p$、$E_2 = g^b \bmod p$；

[0077] 在本实施例中，签名模块用于基于BLS短签名方法，生成车辆ECU公钥及签名；

[0078] 在本实施例中，签名校验模块用于对报文签名进行校验；

[0079] 在本实施例中，组密钥生成及交换模块用于生成组密钥并进行组密钥交换，交换组密钥后的发送方ECU_1和接收方ECU_2为同一逻辑实体；

[0080] 在本实施例中，逻辑实体合并模块用于将任意两个逻辑实体安全连接形成一个新逻辑实体，当一个逻辑实体与另一个逻辑实体进行合并时，双方逻辑实体互相验证身份后发送已有组密钥，接收方接收后，将发送方的组密钥与逻辑实体内部各个车辆ECU的私钥都进行幂运算；

[0081] 在本实施例中，共享会话密钥输出模块用于输出共享会话密钥，采用并行的方式合并形成逻辑实体，当所有车辆ECU处于同一逻辑实体时，生成共享会话密钥。

[0082] 实施例3

[0083] 本实施例提供一种存储介质，存储介质可以是ROM、RAM、磁盘、光盘等储存介质，该存储介质存储有一个或多个程序，所述程序被处理器执行时，实现实施例1的用于汽车ECU间安全通信的密钥交换方法。

[0084] 实施例4

[0085] 本实施例提供一种计算设备，所述的计算设备可以是台式电脑、笔记本电脑、智能手机、PDA手持终端、平板电脑或其他具有显示功能的终端设备，该计算设备包括处理器和存储器，存储器存储有一个或多个程序，处理器执行存储器存储的程序时，实现实施例1的用于汽车ECU间安全通信的密钥交换方法。

[0086] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

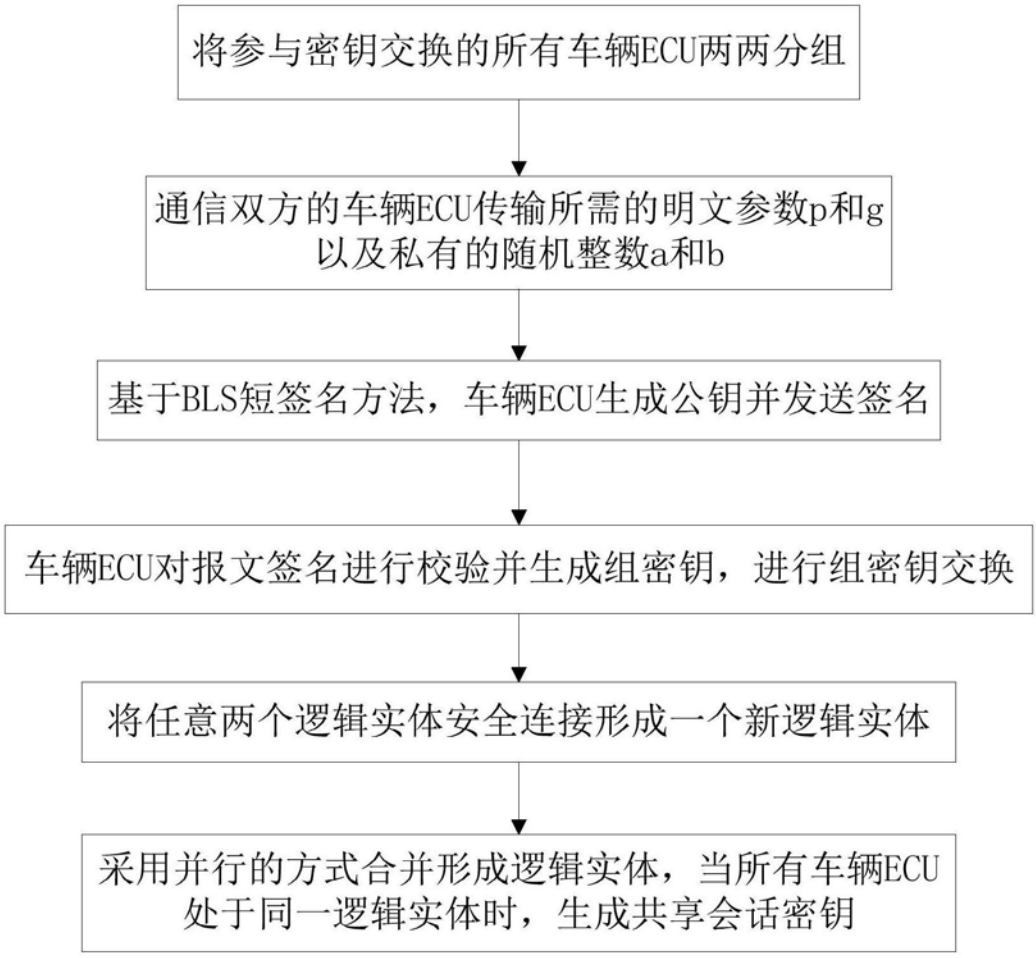

将参与密钥交换的所有车辆ECU两两分组
通信双方的车辆ECU传输所需的明文参数p和g以及私有的随机整数a和b
基于BLS短签名方法，车辆ECU生成公钥并发送签名
车辆ECU对报文签名进行校验并生成组密钥，进行组密钥交换
将任意两个逻辑实体安全连接形成一个新逻辑实体
采用并行的方式合并形成逻辑实体，当所有车辆ECU处于同一逻辑实体时，生成共享会话密钥

图1

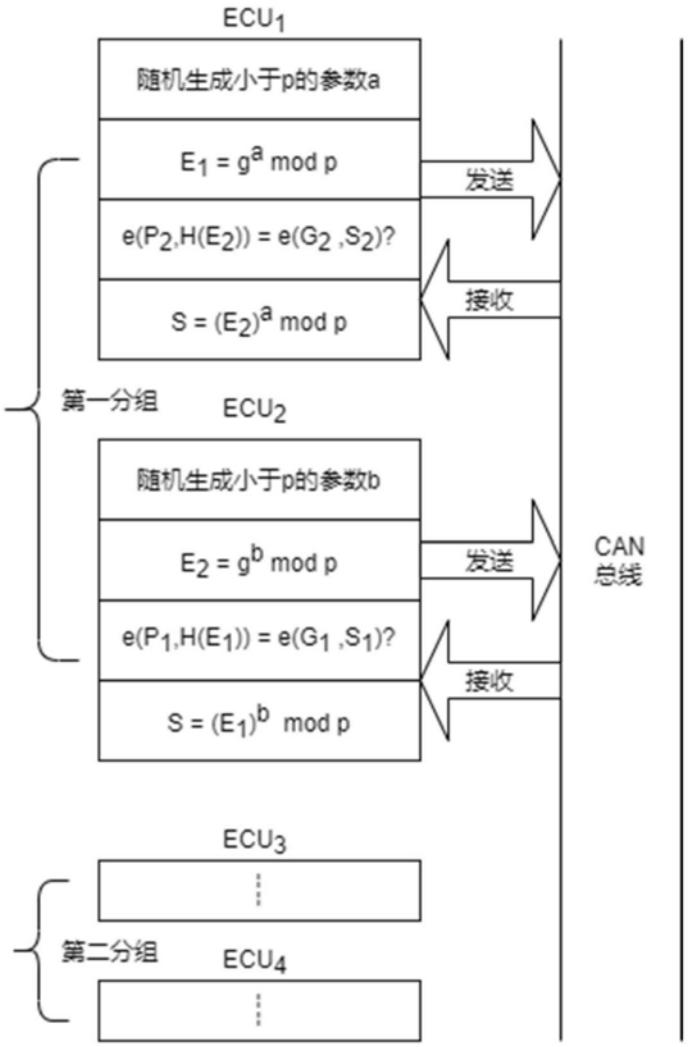

ECU1
随机生成小于p的参数a
E1 = g^a mod p
发送
e(P2,H(E2)) = e(G2 ,S2)?
接收
S = (E2)^a mod p
第一分组
ECU2
随机生成小于p的参数b
E2 = g^b mod p
发送
CAN
总线
e(P1,H(E1)) = e(G1 ,S1)?
接收
S = (E1)^b mod p
ECU3
第二分组
ECU4

图2

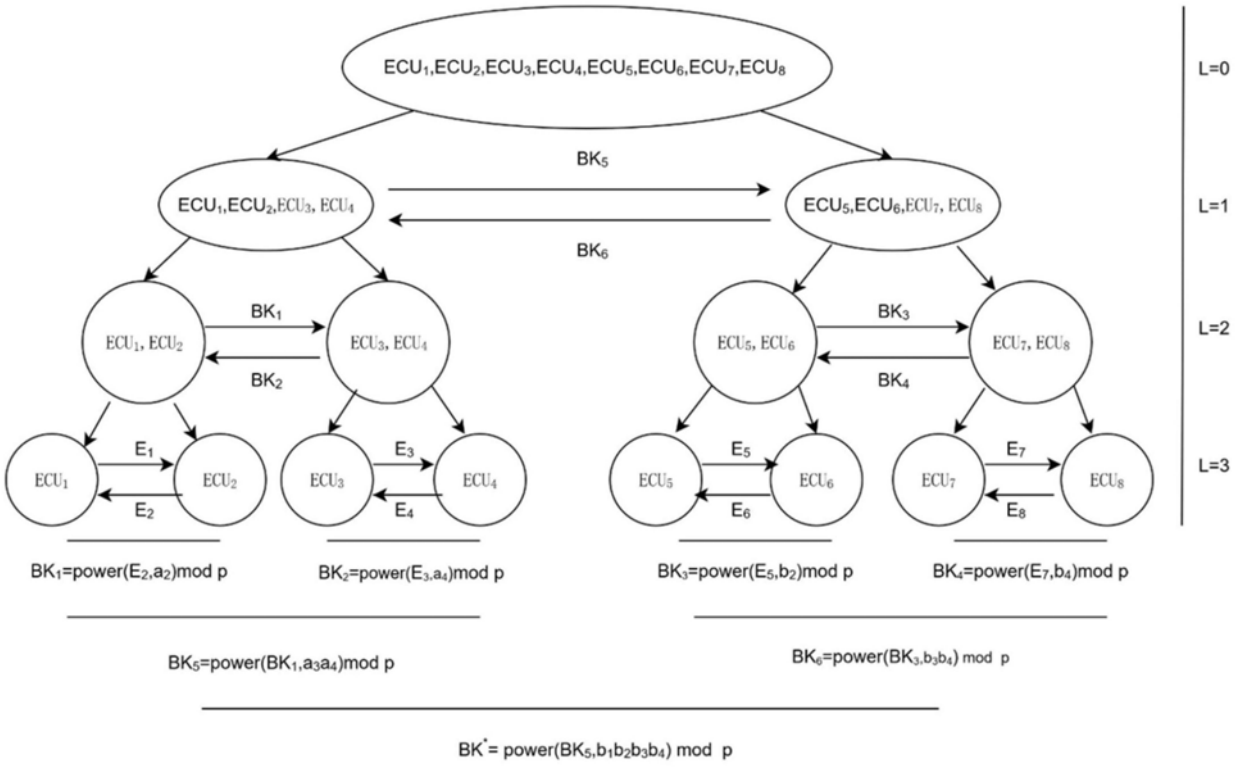

ECU1,ECU2,ECU3,ECU4,ECU5,ECU6,ECU7,ECU8
L=0
BK5
ECU1,ECU2,ECU3, ECU4
ECU5,ECU6,ECU7, ECU8
L=1
BK6
BK1
BK2
BK3
BK4
ECU1, ECU2
ECU3, ECU4
ECU5, ECU6
ECU7, ECU8
L=2
E1
E2
E3
E4
E5
E6
E7
E8
ECU1
ECU2
ECU3
ECU4
ECU5
ECU6
ECU7
ECU8
L=3
BK1=power(E2,a2)mod p
BK2=power(E3,a4)mod p
BK3=power(E5,b2)mod p
BK4=power(E7,b4)mod p
BK5=power(BK1,a3a4)mod p
BK6=power(BK3,b3b4) mod p
BK*= power(BK5,b1b2b3b4) mod p

图3