(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 108944784 B
(45)授权公告日 2020.03.24

(21)申请号 201810871874.2
(22)申请日 2018.08.02
(65)同一申请的已公布的文献号
申请公布号 CN 108944784 A
(43)申请公布日 2018.12.07
(73)专利权人 安徽江淮汽车集团股份有限公司
地址 230601 安徽省合肥市经济技术开发区紫云路99号
(72)发明人 李朋飞 李创举
(74)专利代理机构 北京维澳专利代理有限公司 11252
代理人 周放 贾博雍
(51)Int.Cl.
B60R 25/04(2013.01)
B60R 25/24(2013.01)

审查员 郭啟洪

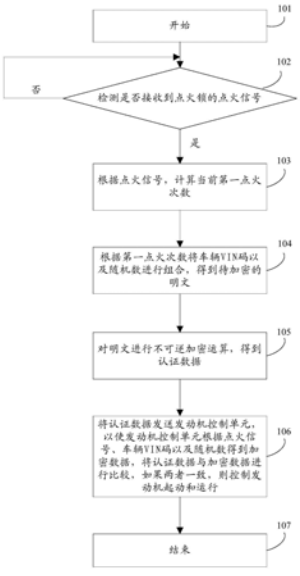
权利要求书3页 说明书9页 附图2页

(54)发明名称

发动机防盗单元的认证方法及系统

(57)摘要

本发明涉及汽车安全领域，具体地涉及一种发动机防盗单元的认证方法及系统，所述方法包括：检测是否接收到点火锁的点火信号；如果是，根据所述点火信号，计算当前第一点火次数；根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；对所述明文进行不可逆加密运算，得到认证数据；将所述认证数据发送给发动机控制单元，以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据后，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。通过本发明，提高了车辆防盗安全级别。



CN 108944784 B

1.一种发动机防盗单元的认证方法,其特征在于,所述方法包括:

检测是否接收到点火锁的点火信号;

如果是,根据所述点火信号,计算当前第一点火次数;

根据所述第一点火次数将车辆VIN码以及随机数进行组合,得到待加密的明文;

对所述明文进行不可逆加密运算,得到认证数据;

将所述认证数据发送给发动机控制单元,以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据,将所述认证数据与所述加密数据进行比较,如果两者一致,则控制发动机起动和运行。

2.根据权利要求1所述的发动机防盗单元的认证方法,其特征在于,所述方法还包括:

根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文之前,获取与所述点火锁连接的点火防盗装置的ID;

检测所述ID是否有效;

如果是,根据所述第一点火次数将车辆VIN码以及随机数进行组合,得到待加密的明文。

3.根据权利要求1所述的发动机防盗单元的认证方法,其特征在于,所述根据所述点火信号,计算当前第一点火次数包括:

检测是否接收到点火锁的点火信号之前,设置16位第一点火计数器;

当接收到所述点火信号后,所述第一点火计数器加8;

检测所述第一点火计数器的值是否等于设定值;如果否,得到当前第一点火次数;

否则,对所述第一点火计数器初始化。

4.根据权利要求3所述的发动机防盗单元的认证方法,其特征在于,所述根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括:

将所述第一点火次数按位平分,将平分完后高设定位和低设定位相加后舍去溢出位,得到设定位的第一移位数;

将所述随机数循环左移或右移所述第一移位数,得到第一同步数;

将所述第一同步数的补码作为新的随机数进行存储;

将车辆VIN码与第一同步数组合得到待加密的明文。

5.根据权利要求4所述的发动机防盗单元的认证方法,其特征在于,所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据具体包括:

设置与所述第一点火计数器相同位的第二点火计数器;

所述发动机控制单元检测是否接收到所述点火锁的点火信号;

如果是,所述第二点火计数器加8;

检测所述第二点火计数器的值是否等于设定值;如果否,得到当前第二点火次数;

将当前第二点火次数按位平分,将平分完后的高设定位和低设定位相加后舍去溢出位,得到设定位的第二移位数;

将所述随机数循环左移或右移所述第二移位数,得到第二同步数;

将所述第二同步数的补码作为新的随机数进行存储;

将车辆VIN码与第二同步数组合后,进行不可逆加密运算,得到所述加密数据。

6.根据权利要求3所述的发动机防盗单元的认证方法,其特征在于,所述根据所述第一

点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括：

将所述第一点火次数按位平均拆分为第一4*4行列矩阵，得到第一移位数矩阵；

将所述随机数按字节平均拆分为第二4*4行列矩阵，将4行的行数据分别循环左移或右移上述第一移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第一同步数；

将所述第一同步数作为新的随机数进行存储；

将车辆VIN码与第一同步数组合得到待加密的明文，其中1≤n≤4。

7.根据权利要求6所述的发动机防盗单元的认证方法，其特征在于，所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据具体包括：

设置与所述第一点火计数器相同位的第二点火计数器；

所述发动机控制单元检测是否接收到所述点火锁的点火信号；如果是，所述第二点火计数器加8；

检测所述第二点火计数器的值是否等于设定值；如果否，得到当前第二点火次数；

将所述第二点火次数按位平均拆分为第三4*4行列矩阵，得到第二移位数矩阵；

将所述随机数按字节平均拆分为第四4*4行列矩阵，将4行的行数据分别循环左移或右移上述第二移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第二同步数；

将所述第二同步数作为新的随机数进行存储；

将车辆VIN码与第二同步数组合后，进行不可逆加密运算，得到所述加密数据，其中1≤n≤4。

8.一种发动机防盗单元的认证系统，其特征在于，所述系统包括：分别与发动机防盗单元、发动机控制单元连接的点火锁；所述发动机控制单元与发动机连接；所述发动机防盗单元通过CAN总线与所述发动机控制单元连接；所述发动机防盗单元与所述发动机控制单元中均存储有车辆VIN码以及随机数；所述发动机防盗单元检测是否接收到点火锁的点火信号；如果是，所述发动机防盗单元根据所述点火信号，计算当前第一点火次数；根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；对所述明文进行不可逆加密运算，得到认证数据，将所述认证数据发送给所述发动机控制单元；所述发动机控制单元检测是否接收到点火锁的点火信号；如果是，所述发动机控制单元根据所述点火信号，计算当前第二点火次数；根据所述第二点火次数将车辆VIN码以及随机数进行组合后进行不可逆加密运算，得到加密数据；所述发动机控制单元将所述认证数据与所述加密数据进行比较，如果所述认证数据与所述加密数据一致，所述发动机控制单元控制所述发动机起动和运行。

9.根据权利要求8所述的发动机防盗单元的认证系统，其特征在于，所述系统还包括：

分别与所述点火锁、所述发动机防盗单元连接的点火防盗装置，所述发动机防盗单元在根据所述第一点火次数将车辆VIN码以及随机数据进行组合得到待加密的明文之前，获取所述点火防盗装置的ID；检测所述ID是否有效；如果是，根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文。

10.根据权利要求9所述的发动机防盗单元的认证系统,其特征在于,所述系统还包括:

生产下线检测设备;所述发动机防盗单元与所述发动机控制单元中均存储的车辆VIN码以及随机数由所述生产下线设备在车辆下线之后写入。

发动机防盗单元的认证方法及系统

技术领域

[0001] 本发明涉及汽车安全领域，具体地涉及一种发动机防盗单元的认证方法及系统。

背景技术

[0002] 随着汽车保有量的快速增长，汽车被盗的案件在全国各地时有发生；据中国保信的统计数据指出，2016年全国有4255辆机动车被盗。汽车防盗装置已经由早期的机械式发展为电子防盗装置；发动机防盗系统主要从控制发动机的起动和运转，并以此达到防盗的目的。

[0003] 发动机防盗系统大致可以分为鉴权和认证两个过程来实现发动机系统的防盗；鉴权即发动机防盗单元对用户的身份进行识别，认证即发动机防盗单元和发动机控制单元之间进行认证；只有当鉴权和认证都完成了，发动机控制单元才允许发动机的起动和运转。

[0004] 鉴权的过程中，发动机防盗单元会通过加密的无线通信方式对用户ID进行识别，以确认用户的身份。鉴权成功后，进入认证的过程，发动机防盗单元会发起认证请求信息，通过CAN总线将认证请求信息发送给发动机控制单元。发动机控制单元对发动机防盗单元发来的信息进行认证，认证完成之后，允许发动机起动和运转。

[0005] 针对发动机控制单元和发动机防盗单元之间的认证过程，现有的技术方案采用了两种技术手段来完成；一是CAN总线技术，二是加密的数据传输。

[0006] CAN总线技术的运用方法为发动机控制单元和发动机防盗单元这两个电子控制单元均包含CAN总线所必须的软硬件接口，并连接到车辆的同一个CAN网络上。

[0007] 在加密的数据传输方面，主要采用的方法为两者使用同一个密钥，分别存储到发动机控制单元和发动机防盗单元中，在每次认证开始，发动机防盗单元使用该密钥和某一种加密算法对明文进行数据加密形成密文，密文经过CAN总线发送给发动机控制单元，发动机控制单元使用同一密钥和对应的解密算法对密文进行解密获得明文，一旦发动机控制单元对密文解密成功，即可判断为认证通过。由于发动机防盗单元和发动机控制单元之间使用了同一个密钥和同一加密算法，所以只要经过匹配两者之间的认证通过。

[0008] 然而上述的加密算法通常是常规的加密算法或整车厂自定义的加密算法，它们的特点都是使用密钥进行加密；但这些加密算法都是公开的或者很容易获得。所以上述加密方法的保密点在于密钥的保密性；而使用密钥进行数据加密存在着密钥的保管和分发的问题，一旦密钥被泄露和窃取，那么该认证过程中的加密就会被破解。

发明内容

[0009] 针对现有技术中的缺陷与不足，本发明提供了一种发动机防盗单元的认证方法，该方法对发动机控制单元和发动机防盗单元之间的通信进行更加严格的加密，提高车辆的防盗安全级别。

[0010] 为了实现上述目的，本发明提供了如下技术方案：

[0011] 一种发动机防盗单元的认证方法，所述方法包括：

[0012] 检测是否接收到点火锁的点火信号；

[0013] 如果是，根据所述点火信号，计算当前第一点火次数；

[0014] 根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；

[0015] 对所述明文进行不可逆加密运算，得到认证数据；

[0016] 将所述认证数据发送给发动机控制单元，以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。

[0017] 优选地，所述方法还包括：

[0018] 根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文之前，获取与所述点火锁连接的点火防盗装置的ID；

[0019] 检测所述ID是否有效；

[0020] 如果是，根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文。

[0021] 优选地，所述根据所述点火信号，计算当前第一点火次数包括：

[0022] 检测是否接收到点火锁的点火信号之前，设置16位第一点火计数器；

[0023] 当接收到所述点火信号后，所述第一点火计数器加8；

[0024] 检测所述第一点火计数器的值是否等于设定值；如果否，得到当前第一点火次数；

[0025] 否则，对所述第一点火计数器初始化。

[0026] 优选地，所述根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括：

[0027] 将所述第一点火次数按位平分，将平分完后高设定位和低设定位相加后舍去溢出位，得到设定位的第一移位数；

[0028] 将所述随机数循环左移或右移所述第一移位数，得到第一同步数；

[0029] 将所述第一同步数的补码作为新的随机数进行存储；

[0030] 将车辆VIN码与第一同步数组合得到待加密的明文。

[0031] 优选地，所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据具体包括：

[0032] 设置与所述第一点火计数器相同位的第二点火计数器；

[0033] 所述发动机控制单元检测是否接收到所述点火锁的点火信号；

[0034] 如果是，所述第二点火计数器加8；

[0035] 检测所述第二点火计数器的值是否等于设定值；如果否，得到当前第二点火次数；

[0036] 将当前第二点火次数按位平分，将平分完后的高设定位和低设定位相加后舍去溢出位，得到设定位的第二移位数；

[0037] 将所述随机数循环左移或右移所述第二移位数，得到第二同步数；

[0038] 将所述第二同步数的补码作为新的随机数进行存储；

[0039] 将车辆VIN码与第二同步数组合后，进行不可逆加密运算，得到所述加密数据。

[0040] 优选地，所述根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括：

[0041] 将所述第一点火次数按位平均拆分为4*4行列矩阵，得到第一移位数矩阵；

[0042] 将所述随机数按字节平均拆分为4*4行列矩阵，将4行的行数据分别循环左移或右移上述第一移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第一同步数；

[0043] 将所述第一同步数作为新的随机数进行存储；

[0044] 将车辆VIN码与第一同步数组合得到待加密的明文，其中1≤n≤4。优选地，所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据具体包括：

[0045] 设置与所述第一点火计数器相同位的第二点火计数器；

[0046] 所述发动机控制单元检测是否接收到所述点火锁的点火信号；如果是，所述第二点火计数器加8；

[0047] 检测所述第二点火计数器的值是否等于设定值；如果否，得到当前第二点火次数；

[0048] 将所述第二点火次数按位平均拆分为4*4行列矩阵，得到第二移位数矩阵；

[0049] 将所述随机数按字节平均拆分为4*4行列矩阵，将4行的行数据分别循环左移或右移上述第二移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第二同步数；

[0050] 将所述第二同步数作为新的随机数进行存储；

[0051] 将车辆VIN码与第二同步数组合后，进行不可逆加密运算，得到所述加密数据，其中1≤n≤4。

[0052] 一种发动机防盗单元的认证系统，所述系统包括：分别与发动机防盗单元、发动机控制单元连接的点火锁；所述发动机控制单元与发动机连接；所述发动机防盗单元通过CAN总线与所述发动机控制单元连接；所述发动机防盗单元与所述发动机控制单元中均存储有车辆VIN码以及随机数；所述发动机防盗单元检测是否接收到点火锁的点火信号；如果是，所述发动机防盗单元根据所述点火信号，计算当前第一点火次数；根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；对所述明文进行不可逆加密运算，得到认证数据，将所述认证数据发送给所述发动机控制单元；所述发动机控制单元检测是否接收到点火锁的点火信号；如果是，所述发动机控制单元根据所述点火信号，计算当前第二点火次数；根据所述第二点火次数将车辆VIN码以及随机数进行组合后进行不可逆加密运算，得到加密数据；所述发动机控制单元将所述认证数据与所述加密数据进行比较，如果所述认证数据与所述加密数据一致，所述发动机控制单元控制所述发动机起动和运行。

[0053] 优选地，所述系统还包括：

[0054] 分别与所述点火锁、所述发动机防盗单元连接的点火防盗装置，所述发动机防盗单元在根据所述第一点火次数将车辆VIN码以及随机数据进行组合得到待加密的明文之前，获取所述点火防盗装置的ID；检测所述ID是否有效；如果是，根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文。

[0055] 优选地，所述系统还包括：

[0056] 生产下线检测设备；所述发动机防盗单元与所述发动机控制单元中均存储的车辆VIN码以及随机数由所述生产下线设备在车辆下线之后写入。

[0057] 本发明的有益效果在于：

[0058] 本发明提供了一种发动机防盗单元的认证方法及系统，发动机防盗单元检测是否接收到点火锁的点火信号；如果是，根据所述点火信号，计算当前第一点火次数，根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；对所述明文进行不可逆加密运算，得到认证数据；将所述认证数据发送给发动机控制单元，以使所述发动机控制单元根据所述点火信号得到加密数据，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。通过本发明，提高了车辆的防盗安全级别。

附图说明

[0059] 图1是本发明实施例发动机防盗单元的认证方法的一种流程图。

[0060] 图2是本发明实施例发动机防盗单元的认证系统的一种结构示意图。

具体实施方式

[0061] 为了使本领域技术人员能更进一步了解本发明的特征及技术内容，下面结合附图和实施方式对本发明实施例作详细说明。

[0062] 如图1所示是本发明实施例发动机防盗单元的认证方法的一种流程图，包括以下步骤：

[0063] 步骤101：开始。

[0064] 步骤102：检测是否接收到点火锁的点火信号；如果是，执行步骤103；否则，执行步骤102。

[0065] 需要说明的是，本发明实施例中，不限定于从点火锁获取点火信号，点火信号也可以是汽车机械点火开关或者具备同样功能的电子开关发出的信号。

[0066] 步骤103：根据所述点火信号，计算当前第一点火次数。

[0067] 需要说明的是，根据所述点火信号，计算当前第一点火次数可以通过第一点计数器实现。本发明实施例中，在检测点火锁的点火信号之前，设置16位第一点火计数器；当接收到所述点火信号后，所述第一点火计数器加8；检测所述第一点火计数器的值是否等于设定值；如果否，得到当前第一点火次数；否则，对所述第一点火计数器初始化。

[0068] 需要说明的是，设定值由第一点火计数器的计数最大值确定，比如，设定值为65535；在车辆VIN码写入成功后，第一点火计数器的初始值为0，所述第一点火计数器下电后数据不丢失；当接收到所述点火信号后，所述第一点火计数器加8得到当前第一点火次数。在本发明实施例中，每点火一次，第一点火次数加8，第一点火次数为16位的整数值(0～65535)，当第一点火次数累加超过65535后数值重置为0，第一点火计数器重新累加计数。

[0069] 步骤104：根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文。

[0070] 具体地，所述随机数以及所述车辆VIN码可以是由生产下线检测设备产生，进一步，所述随机数的长度可以是128位。每个车辆对应一个车辆VIN码，所述生产下线检测设备在车辆下线之后将车辆VIN码以及随机数分别写入到发动机防盗单元以及发动机控制单元的存储器中，一经写入，不可擦除也不可由未经整车厂特殊授权的设备修改。

[0071] 进一步，本发明的另一个实施例中，所述随机数也可以是由所述发动机控制单元

产生。所述发动机控制单元在车辆下线后将随机数发送给所述发动机防盗单元。这样发动机防盗单元与发动机控制器单元中具有相同的随机数，便于后续的认证。

[0072] 具体地，所述根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括步骤(A)～(D)：

[0073] (A)将所述第一点火次数按位平分，将平分完后的高设定位和低设定位相加后舍去溢出位，得到设定位的第一移位数；具体地，设定位由第一点火次数的位数标定确定，比如，设定位为8位。

[0074] (B)将所述随机数循环左移或右移所述第一移位数，得到第一同步数。

[0075] (C)将所述第一同步数的补码作为新的随机数进行存储。

[0076] (D)将车辆VIN码与第一同步数组合得到待加密的明文。

[0077] 进一步，为了使待加密的明文保密性更强，本发明的另一个实施例中，所述根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文包括步骤(A')～(D')：

[0078] (A')将所述第一点火次数按位平均拆分为第一4*4行列矩阵，得到第一移位数矩阵。

[0079] (B')将所述随机数按字节平均拆分为第二4*4行列矩阵，将4行的行数据分别循环左移或右移上述第一移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第一同步数。

[0080] (C')将所述第一同步数作为新的随机数进行存储。

[0081] (D')将车辆VIN码与第一同步数组合得到待加密的明文，其中1≤n≤4。

[0082] 下面具体举例如下：比如，第一点火次数为20，即二进制表示为：0000 0000 0001 0100，随机数为00112233445566778899AABBCCDDEEFF，则按字节平均拆分为第一4*4行列矩阵为$\begin{pmatrix}0000\\0000\\0001\\0100\end{pmatrix}$，则随机数按字节平均拆分的第二4*4行列矩阵为$\begin{pmatrix}00112233\\44556677\\8899AABB\\CCDDEEFF\end{pmatrix}$，第二4*4行列矩阵按第一4*4行列矩阵循环右移后，此时第二4*4行列矩阵第一行循环右移0位，第二行循环右移0位，第三行循环右移1位，第四行循环右移4位，得到$\begin{pmatrix}00112233\\44556677\\44CD55DC\\FCCDDEEF\end{pmatrix}$，进行行列置位为$\begin{pmatrix}004444FC\\1155CDCD\\226655DE\\3377DCEF\end{pmatrix}$得到第一同步数为004444FC1155CDCD226655DE3377DCEF。

[0083] 步骤105：对所述明文进行不可逆加密运算，得到认证数据。

[0084] 需要说明的是，可以使用不可逆加密算法中的MD4或MD5等方法，根据加密要求和

编程单元的处理速率来确定，对待加密的明文进行加密，加密完后，得到128位Hash值，取低64位Hash值作为认证数据。

[0085] 步骤106：将所述认证数据发送发动机控制单元，以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据后，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。

[0086] 具体地，所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据过程如(E)～(L)所示：

[0087] (E)对16位的第二点火计数器初始化，所述第二点火计数器下电后数据不丢失。

[0088] 本发明实施例中，在检测点火锁的点火信号之前，设置与所述第一点火计数器相同位的第二点火计数器；对所述第二点火计数器初始化；比如，在车辆VIN码写入成功后，第二点火计数器的初始值为0，所述第二点火计数器下电后数据不丢失；当接收到所述点火信号后，所述第二点火计数器加8得到当前第二点火次数。在本发明实施例中，每点火一次，第二点火次数加8，当第一点火次数为16位整数值时，第二点火次数也为16位的整数值(0～65535)，当第二点火次数累加超过65535后数值重置为0，第二点火计数器重新累加计数。

[0089] (F)所述发动机控制单元检测是否接收到所述点火锁的点火信号；如果是，执行(G)；否则，执行步骤107。

[0090] (G)所述第二点火计数器加8。

[0091] (H)检测所述第二点火计数器的值是否等于设定值；如果否，执行步骤(I)；否则，返回执行步骤(E)。

[0092] (I)得到当前第二点火次数，将当前第二点火次数按位平分，将平分完后的高设定位和低设定位相加后舍去溢出位，得到设定位的第二移位数；具体地，设定位由第一点火次数的位数标定确定，比如，当第一点火次数为16位时，设定位为8位。

[0093] (J)将所述随机数循环左移或右移所述第二移位数，得到第二同步数。

[0094] (K)将所述第二同步数的补码作为新的随机数进行存储。

[0095] (L)将车辆VIN码与第二同步数组合后，进行不可逆加密运算，得到所述加密数据。

[0096] 需要说明的是，可以使用不可逆加密算法中的MD4或MD5等方法，根据加密要求和编程单元的处理速率来确定，对车辆VIN码与第二同步数组合的数据进行加密后，得到128位Hash值，取低64位Hash值作为加密数据。进一步，发动机控制单元将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。

[0097] 为了是加密数据更加可靠，本发明的另一个实施例中，所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据过程如(E')～(L')所示：

[0098] (E')设置与所述第一点火计数器相同位的第二点火计数器，对16位的第二点火计数器初始化，所述第二点火计数器下电后数据不丢失。

[0099] (F')所述发动机控制单元检测是否接收到所述点火锁的点火信号；如果是，执行(G')；否则，执行步骤107。

[0100] (G')所述第二点火计数器加8。

[0101] (H')检测所述第二点火计数器的值是否等于设定值；如果否，执行步骤(I')；否则，返回执行步骤(E')。

[0102] (I')得到当前第二点火次数，将所述第二点火次数按位平均拆分为第三4*4行列

矩阵，得到第二移位数矩阵

[0103] (J')将所述随机数按字节平均拆分为第四4*4行列矩阵，将4行的行数据分别循环左移或右移上述第二移位数矩阵对应行的移位数；得到新的4*4行列矩阵后，将第n列置换为第n行的方法进行行列置位；得到新的行列矩阵后依照上述拆分方法的逆向方法合并为新的数据，得到第二同步数。

[0104] (K')将所述第二同步数作为新的随机数进行存储。

[0105] (L')将车辆VIN码与第二同步数组合后，进行不可逆加密运算，得到所述加密数据，其中1≤n≤4。

[0106] 需要说明的是，第二同步数的形成过程与第一同步数相同，此处就不再赘述。

[0107] 步骤107：结束。

[0108] 本发明实施例提供的发动机防盗单元的认证方法，发动机防盗单元检测是否接收到点火锁的点火信号；如果是，根据所述点火信号，计算当前第一点火次数，根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；对所述明文进行不可逆加密运算，得到认证数据；将所述认证数据发送给发动机控制单元，以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据后，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。通过本发明，可以在每次点火时，根据点火次数计算待加密的明文，并且每次随机数认证时随机数均不相同，保证了发动机防盗单元与发动机控制单元之外的设备均无法得到随机数。

[0109] 进一步，为了保证认证的安全性，本发明的另一个实施例中，所述方法包括以下步骤：

[0110] 步骤201：开始。

[0111] 步骤202：检测是否接收到点火锁的点火信号；如果是，执行步骤203；否则，执行步骤202。

[0112] 步骤203：根据所述点火信号，计算当前第一点火次数。

[0113] 步骤204：获取与所述点火锁连接的点火防盗装置的ID。

[0114] 需要说明的是，点火防盗装置可以为PEPS或汽车防盗识读线圈；汽车防盗识读线圈起能源传递和防盗识别代码的转发作用。当用汽车钥匙打开车门时，识读线圈把发动机防盗单元电源能量传送到汽车钥匙内的脉冲转发器，然后把汽车钥匙的识别代码传送回发动机防盗单元。识读线圈一般安装在点火锁外面。

[0115] 步骤205：检测所述ID是否有效；如果是，执行步骤206；否则，执行步骤209。

[0116] 步骤206：根据所述第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文；

[0117] 步骤207：对所述明文进行不可逆加密运算，得到认证数据。

[0118] 步骤208：将所述认证数据发送发动机控制单元，以使所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到加密数据后，将所述认证数据与所述加密数据进行比较，如果两者一致，则控制发动机起动和运行。

[0119] 步骤209：结束。

[0120] 本发明实施例提供的发动机防盗单元的认证方法，在根据所述第一点火次数将车辆VIN码以及随机数进行组合得到待加密的明文之前，获取与所述点火锁连接的点火防盗

装置的ID;检测所述ID是否有效;如果是,根据所述第一点火次数将车辆VIN码以及随机数进行组合,得到待加密的明文。通过本发明,可以在鉴定到ID为无效的用户ID时,不进行加密运算,不发送认证数据到CAN总线上,提高了车辆防盗等级与安全性。

[0121] 针对上述方法,本发明还提供了一种发动机防盗单元的认证系统,如图2,所述系统包括:分别与发动机防盗单元IMMO、发动机控制单元EMS连接的点火锁;所述发动机控制单元与发动机(图中未示)连接;所述发动机防盗单元IMMO通过CAN总线与所述发动机控制单元EMS连接;所述发动机防盗单元IMMO与所述发动机控制单元EMS中均存储有车辆VIN码以及随机数;所述发动机防盗单元IMMO检测是否接收到点火锁的点火信号;如果是,所述发动机防盗单元IMMO根据所述点火信号,计算当前第一点火次数;根据所述第一点火次数将车辆VIN码以及随机数进行组合,得到待加密的明文;对所述明文进行不可逆加密运算,得到认证数据,将所述认证数据发送给所述发动机控制单元EMS;所述发动机控制单元EMS检测是否接收到点火锁的点火信号;如果是,所述发动机控制单元根据所述点火信号,计算当前第二点火次数;根据所述第二点火次数将车辆VIN码以及随机数进行组合后进行不可逆加密运算,得到加密数据;所述发动机控制单元EMS将所述认证数据与所述加密数据进行比较,如果所述认证数据与所述加密数据一致,所述发动机控制单元EMS控制所述发动机起动和运行。

[0122] 需要说明的是,本发明实施例中,不限定于从点火锁获取点火信号,点火信号也可以是汽车机械点火开关或者具备同样功能的电子开关发出的信号。

[0123] 进一步,本发明的另一个实施例中,所述系统还可以包括:分别与所述点火锁、所述发动机防盗单元连接的点火防盗装置,所述发动机防盗单元在根据所述第一点火次数将车辆VIN码以及随机数据进行组合得到待加密的明文之前,获取所述点火防盗装置的ID;检测所述ID是否有效;如果是,根据所述第一点火次数将车辆VIN码以及随机数进行组合,得到待加密的明文。需要说明的是,本发明实施例中可以在鉴定到ID为无效的用户ID时,不进行加密运算,不发送认证数据到CAN总线上,提高了车辆防盗等级与安全性。需要说明的是,点火防盗装置可以为PEPS或汽车防盗识读线圈;汽车防盗识读线圈起能源传递和防盗识别代码的转发作用。当用汽车钥匙打开车门时,识读线圈把发动机防盗单元电源能量传送到汽车钥匙内的脉冲转发器,然后把汽车钥匙的识别代码传送回发动机防盗单元。识读线圈一般安装在点火锁外面。

[0124] 进一步,本发明的另一个实施例中,所述随机数由所述发动机控制单元产生,并由发动机控制单元在车辆下线后将所述随机数发送给所述发动机防盗单元;所述发动机控制单元在车辆下线后将随机数发送给所述发动机防盗单元,使得发动机防盗单元与发动机控制器单元中具有相同的随机数,便于后续的认证。更进一步,所述本发明的另一实施例中,所述系统还可以包括:生产下线检测设备;所述发动机防盗单元与所述发动机控制单元中存储的车辆VIN码以及随机数由所述生产下线设备在车辆下线之后写入。具体地,所述生产下线检测设备在车辆下线之后将车辆VIN码以及随机数分别写入到发动机防盗单元以及发动机控制单元的存储器中,一经写入,不可擦除也不可由未经整车厂特殊授权的设备修改。

[0125] 进一步,本发明的实施例中,所述系统还包括:第一点火计数器与第二点火计数器。

[0126] 所述发动机防盗单元根据所述第一点火次数将车辆VIN码以及随机数进行组合,

得到待加密的明文,进行不可逆加密运算,得到认证数据过程如下:

[0127] 1)对16位的第一点火计数器初始化,所述第一点火计数器下电后数据不丢失。

[0128] 2)所述发动机防盗单元检测是否接收到所述点火锁的点火信号;如果是,所述第一点火计数器加8得到当前第一点火次数。

[0129] 3)将所述第一点火次数的高8位和低8位相加后舍去溢出位,得到8位第一移位数。

[0130] 4)将所述随机数循环左移或右移所述第一移位数,得到第一同步数。

[0131] 5)将所述第一同步数的补码作为新的随机数进行存储。

[0132] 6)将车辆VIN码与第一同步数组合得到待加密的明文。

[0133] 7)对所述明文进行不可逆加密运算,得到认证数据。

[0134] 需要说明的是,可以使用不可逆加密算法中的MD4或MD5,根据加密要求和编程单元的处理速率来确定,对待加密的明文进行加密。

[0135] 所述发动机控制单元根据所述点火信号、所述车辆VIN码以及所述随机数得到所述加密数据过程如下:

[0136] 1)对16位的第二点火计数器初始化,所述第二点火计数器下电后数据不丢失。

[0137] 2)所述发动机控制单元检测是否接收到所述点火锁的点火信号;如果是,所述第二点火计数器加8得到当前第二点火次数。

[0138] 3)将当前第二点火次数的高8位和低8位相加后舍去溢出位,得到8位的第二移位数。

[0139] 4)将所述随机数循环左移或右移所述第二移位数,得到第二同步数。

[0140] 5)将所述第二同步数的补码作为新的随机数进行存储;

[0141] 6)将车辆VIN码与第二同步数组合后,进行不可逆加密运算,得到所述加密数据。

[0142] 需要说明的是,可以使用不可逆加密算法中的MD4或MD5,根据加密要求和编程单元的处理速率来确定,对车辆VIN码与第二同步数组合后进行加密。

[0143] 下面结合图2对本发明实施例的具体流程进行介绍:发动机防盗单元IMMO主要为对ID进行识别和发起认证请求;发动机控制单元EMS,主要为响应IMMO的认证请求和对发动机的起动进行控制;收到点火信号后,发动机防盗单元IMMO和发动机控制单元EMS分别根据点火次数将内部存储的车辆VIN码和随机数进行组合后,形成待加密的明文;发动机防盗单元IMMO和发动机控制单元EMS分别将该明文经过不可逆加密运算(可以进行MD4加密算法或/和MD5加密算法)进行加密;发动机防盗单元IMMO和发动机控制单元EMS分别获得加密后的128位Hash值;发动机防盗单元IMMO取Hash值的低64位,通过CAN总线将该数据发送给发动机控制单元EMS。

[0144] 发动机控制单元EMS取自身运算得到的Hash值的低64位,并与CAN上收到的发动机防盗单元IMMO发送来的数据进行比较;当两者数据完全一致时,判断为认证通过,允许发动机起动和运行。

[0145] 以上对本发明实施例进行了详细介绍,本文中应用了具体实施方式对本发明进行了阐述,以上实施例的说明只是用于帮助理解本发明的系统及方法;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

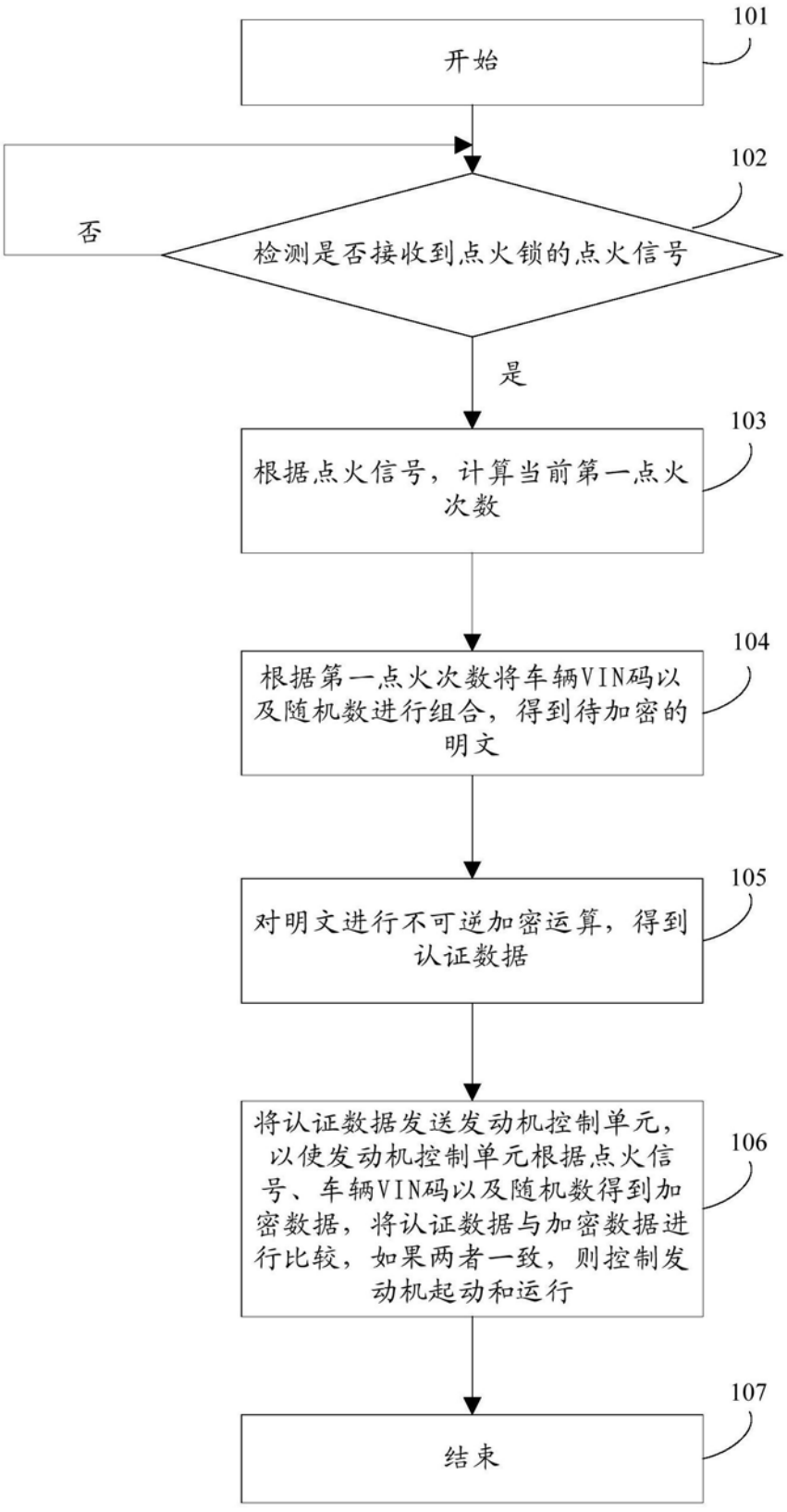

101
开始
102
检测是否接收到点火锁的点火信号
否
是
103
根据点火信号，计算当前第一点火次数
104
根据第一点火次数将车辆VIN码以及随机数进行组合，得到待加密的明文
105
对明文进行不可逆加密运算，得到认证数据
106
将认证数据发送发动机控制单元，以使发动机控制单元根据点火信号、车辆VIN码以及随机数得到加密数据，将认证数据与加密数据进行比较，如果两者一致，则控制发动机起动和运行
107
结束

图1

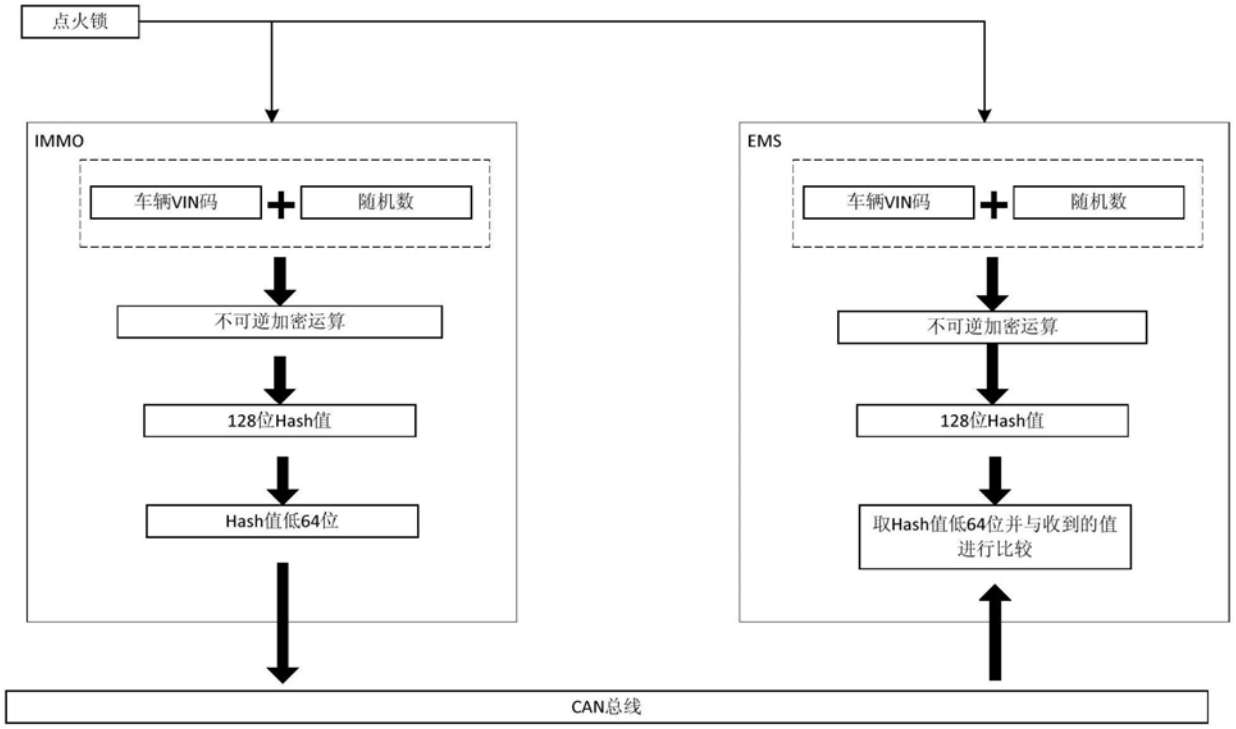

点火锁
IMMO
车辆VIN码
随机数
不可逆加密运算
128位Hash值
Hash值低64位
EMS
车辆VIN码
随机数
不可逆加密运算
128位Hash值
取Hash值低64位并与收到的值进行比较
CAN总线

图2