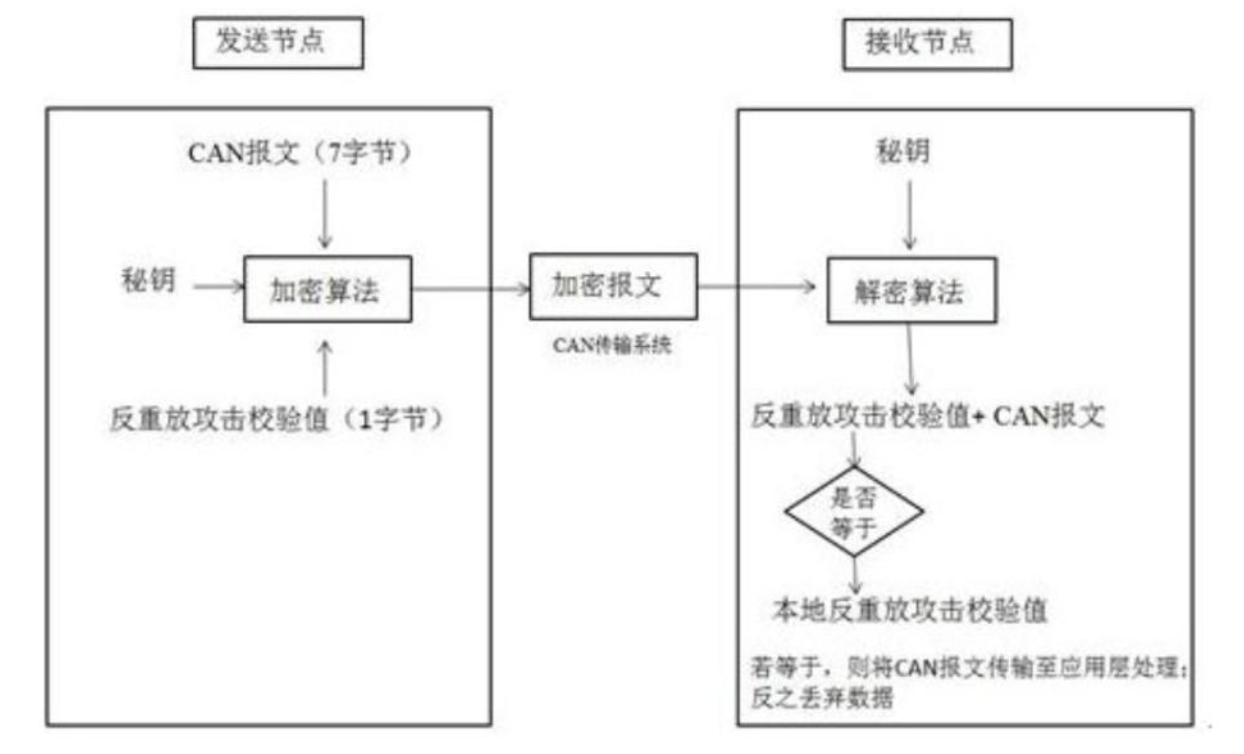
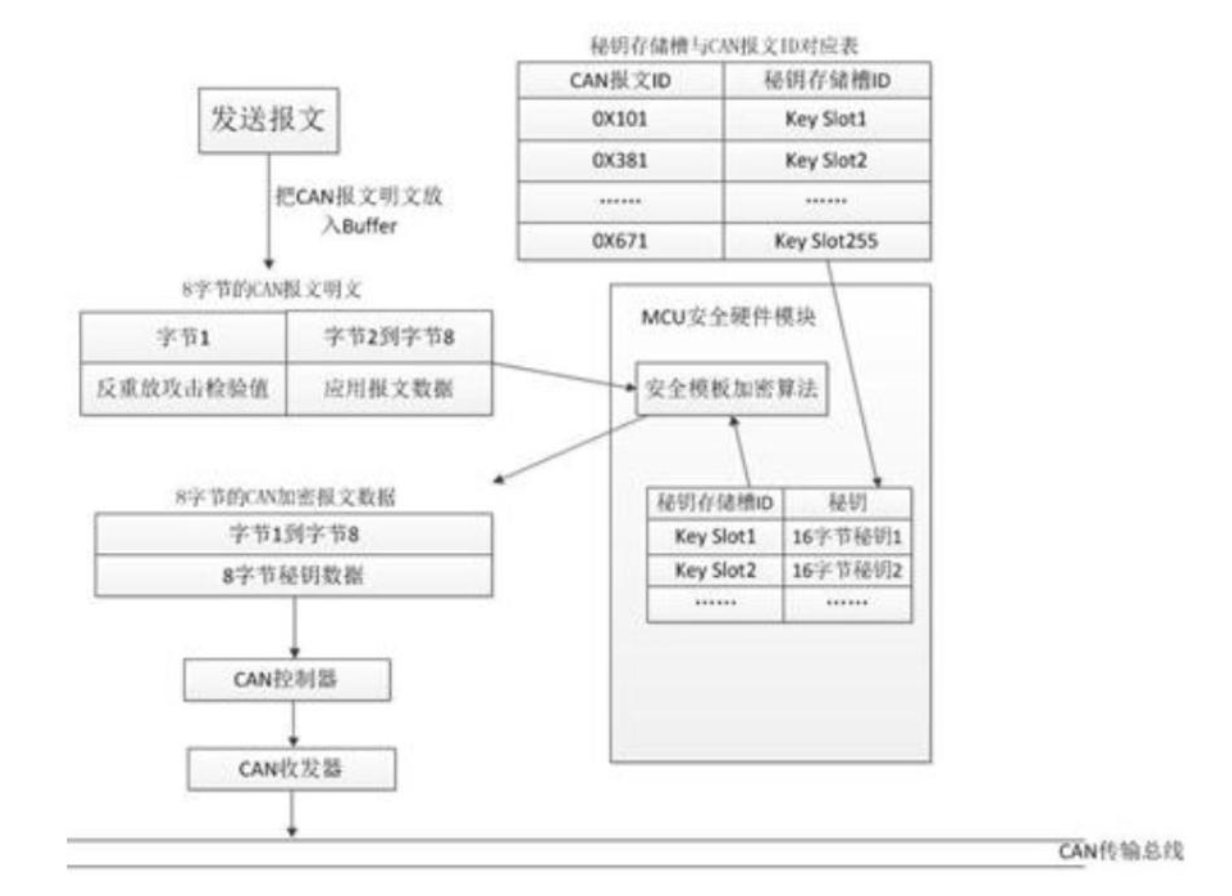
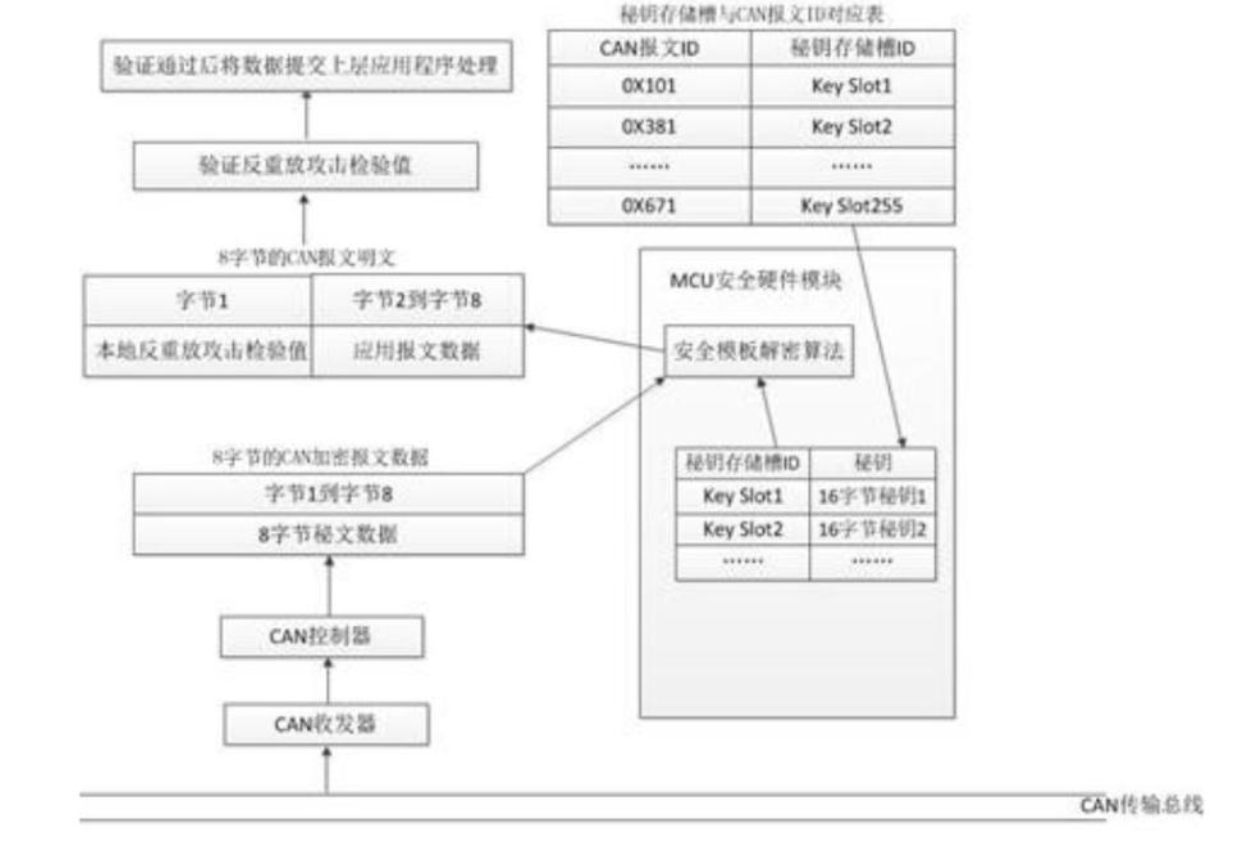
## 搜索关键词——车载CAN总线 AND 通信

**发明名称**——一种车载CAN总线报文的加密通信方法

**公开（公告号）**：CN108494725A`







**专利内容：**发送节点与接受节点使用对称加密的方式对报文数据进行加密，密钥有汽车生产厂家提供。

密钥存储： 密钥存储在MCU安全硬件模块中

ECU中保存有密钥存储槽和CANid对应表，

报文格式：1字节反重放校验值（报文计数器）｜7字节加密数据

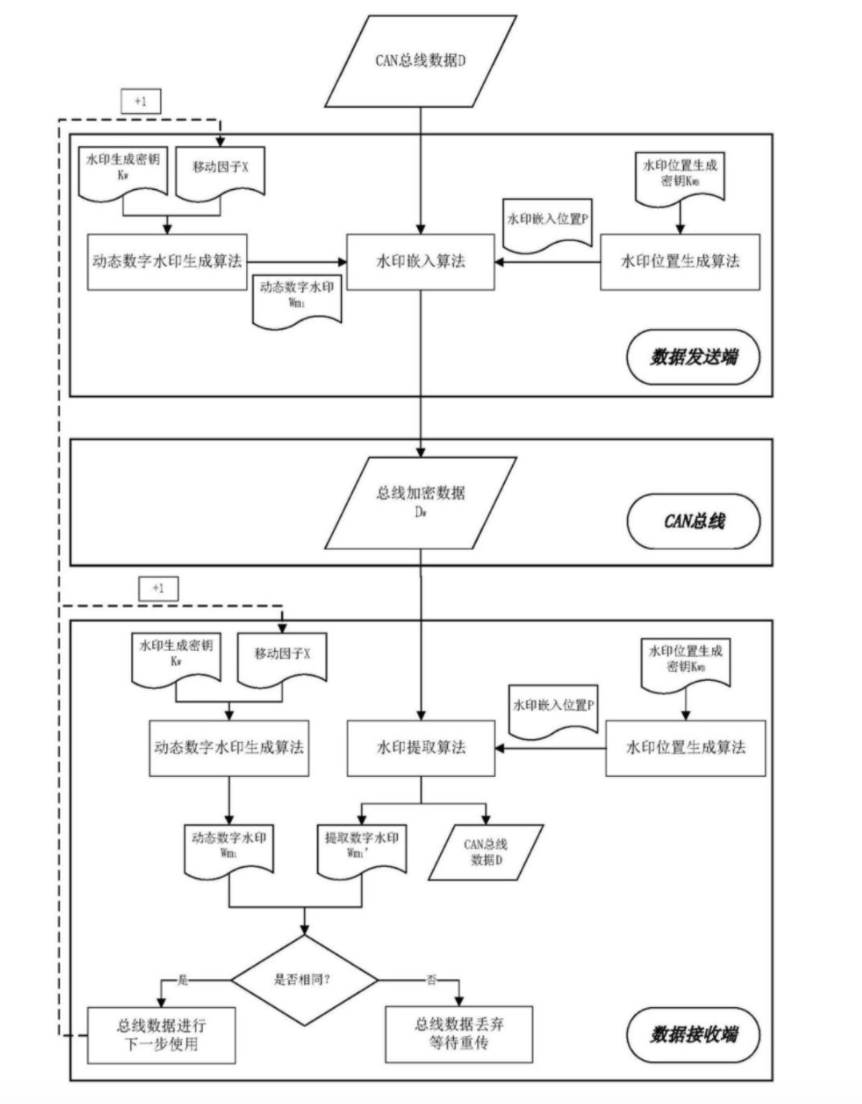
通信过程： 发送方将1字节反重放校验值｜7字节应用数据输入MCU安全硬件模块，同时根据CANid对应表与密钥存储槽之间的关系确定MCU中加密所用的密钥，将8字节明文数据加密得到加密报文。

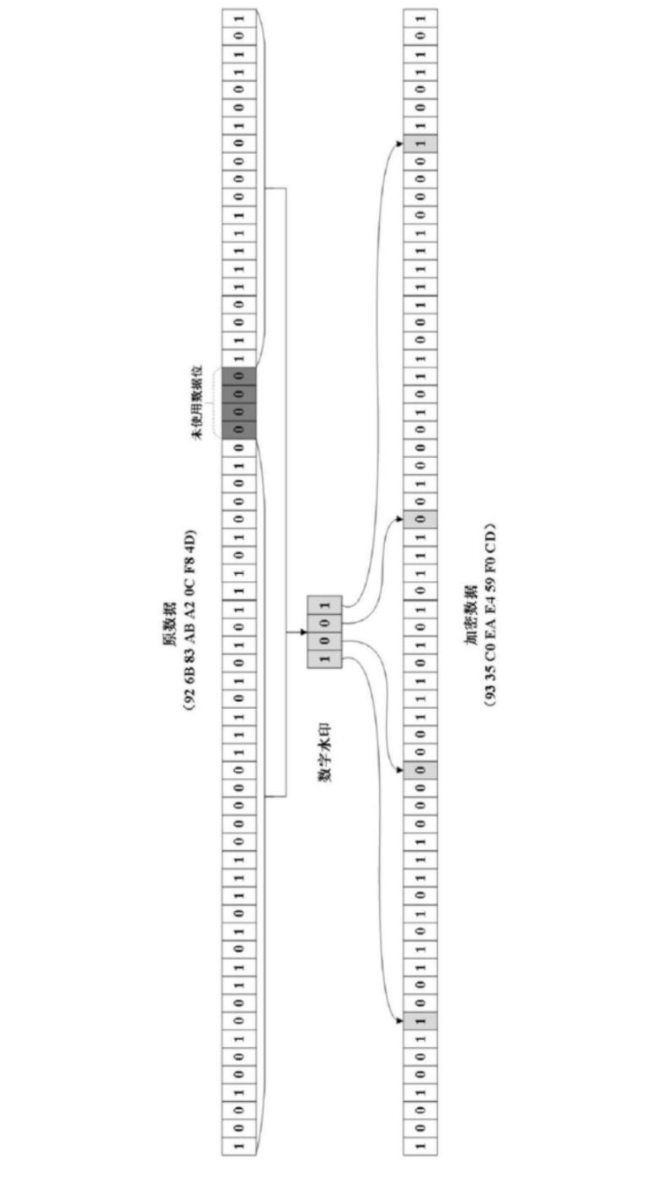
接收方收到加密报文后传入MCU，并根据CANid使用对应的密钥解密，之后再比对反重放校验值是否一致。

**疑问：**专利内未写明反重放校验值（报文计数器）的同步机制

**发明名称：**一种基于动态数字水印的车载CAN总线数据加密算法

**公开（公告）号：**CN111404925A





**专利内容：**在发送方ECU和接收方ECU中内置如下两部分内容：

（1）动态数字水印生成算法（水印生成密钥、移动因子、动态数字水印生成算法）

（2）水印位置生成算法（水印位置生成密钥、水印位置生成算法）

通信过程：

发送方：

1. 发送方利用水印生成密钥和移动因子，通过动态数字水印生成算法生成数字水印
2. 发送方利用水印位置生成密钥生成水印潜入位置信息
3. 根据报文中未利用数据位的情况，缩减数据，将水印信息根据水印嵌入位置嵌入到数据中，保证嵌入后的数据长度与原数据长度相同（理解：原数据若为6字节，则还有0填充的2字节）

接收方：

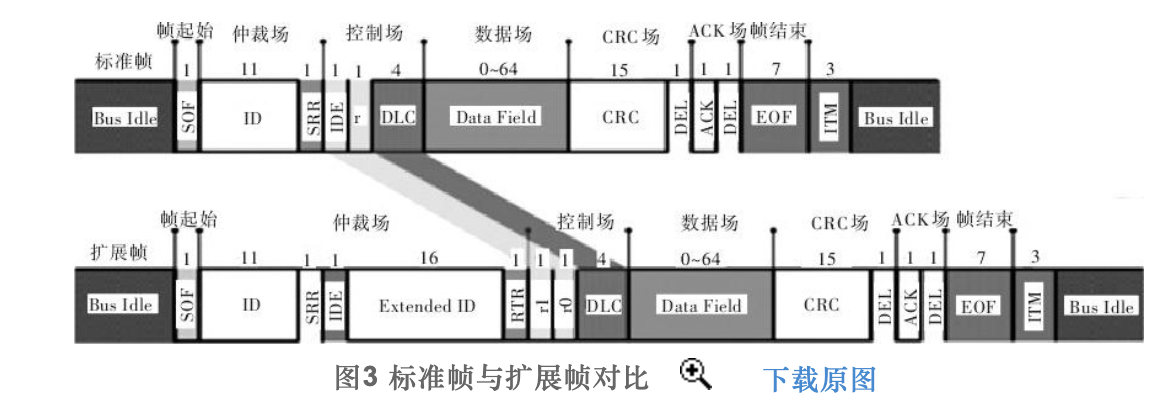
1. 根据水印位置生成密钥声生成水印提取位置信息
2. 根据水印生成密钥和移动因子生成数字水印
3. 根据水印提取位置信息提取接收到数据中的数字水印
4. 核对自己接受的和提取到的数字水印是否一致，若一致则接受，并且发送确认信息至发送端，移动因子递增1；发送端接收到接收端发出的确认信息后，移动因子递增1；

**疑问：**未考虑确认信息丢失的情况，未给出移动因子位数（是否存在移动因子溢出情况），未考虑水印生成密钥的更新问题

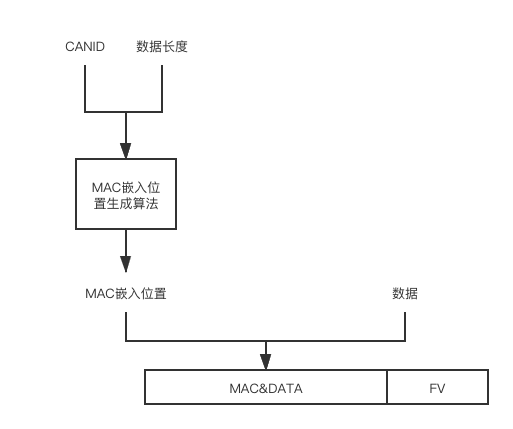
## 专利设想

1. SecOC通信方案，生成的MAC值存放在CRC场中

（CRC替换为MAC是否可行）



1. 类似水印，生成MAC嵌入位置，将MAC值存放在MAC嵌入位置上（此方案是否可以减少MAC长度而不降低安全性）。MAC嵌入位置生成算法可将canid作为输入参数



Canid可否由tbox随机生成，即每次开车都为每个ECU随机生成canid列表（本次行驶canid白名单），发放给各个ecu，

MAC(1byte)

CANID

新鲜值(1byte)

Data(6byte)

空闲位1byte