一种基于国密算法的车载蓝牙门锁解决方案*

程永强 朱雪平 李建**

南宁学院信息工程学院，南宁 530200

摘 要 深入分析蓝牙协议中存在的各种安全风险，研究适用于汽车蓝牙门锁应用场景的安全解决方案。提出一种利用 SM2、SM3、SM4 算法构建蓝牙用户访问认证授权系统以及数据安全的对称和非对称密码系统模型，设计一种没有网络依赖和 CA 证书的公钥信任机制。该技术方案使用密钥以及蓝牙设备地址绑定的方式取代 CA 证书的作用，使得拥有相同的加密密钥和对应的蓝牙设备地址即可信。实验结果验证了所提方案的有效性和可行性，说明了所提方案能够应对身份欺骗、数据流分析、数据窃取、数据篡改、数据回放和通信业务拒绝等安全风险，满足汽车蓝牙门锁的各种安全需求。

关键字 国家商用密码算法，蓝牙通信技术，CA 证书，车载蓝牙门锁

A Solution for Car Bluetooth Door Locks Based on the National Cryptographic Algorithm

Cheng Yongqiang Zhu Xueping Li Jian

School of Information Engineering Nanning University
Nanning 530200,China;
943667593@qq.com

Abstract—This paper analyzes the various security risks in the Bluetooth protocol, ans study the security solution suitable for the application scenario of Bluetooth door locks in cars. We propose a symmetric and asymmetric cryptographic system model using the SM2, SM3, and SM4 algorithms to construct a Bluetooth user access authentication and authorization system and ensure data security, and design a public key trust mechanism that does not depend on a network and CA certificates is proposed. This technique solution uses a method of binding keys and Bluetooth device addresses instead of CA certificates, so that the devices with the same encryption key and corresponding Bluetooth device addresses are trusted. Experiments results verify the effectiveness and feasibility of the proposed solution, and show that the proposed solution can effectively address security risks such as identity fraud, data flow analysis, data theft, data tampering, data replay attacks, and communication business denial, and meet various security requirements of Bluetooth door locks in cars.

Keywords—National commercial cryptographic algorithm, Bluetooth communication technology, CA certificate, Car bluetooth door lock

1 引 言

蓝牙技术已经在物联网、车联网等领域得到广泛应用，它是由爱立信、诺基亚、IBM、东芝、Intel 等五家蓝牙技术联盟成员提出的一种短距离无线数据通信技术。蓝牙在 2.4GHz~2.4835GHz 的频段中划分了几十个信道用于进行通信，在这些信道中通过跳频传输和控制射频链路功率提高了定位和捕捉数据的难度。但是若使用高灵敏度设备周期性扫描物理信道时仍然可以获取到信号的调频序列，可见蓝牙的基本防护手段是不安全的[1]。

针对蓝牙存在的安全问题，文献[2]认为可以利用蓝牙组网中的一些特殊信息计算 SERS 可以提高攻击者破解链路密钥的难度；文献[3]发现了针对蓝牙的 DoS 攻击，并提出了一些预防 DoS 攻击的方法。文献[4]提出了校验用户身份的方式防止攻击者伪装攻击，并设计了一种新的链路密钥产生方案和新的鉴权方案，加大了攻击的难度。文献[5]对低功耗蓝牙的安全模式、配对方式、密钥结构等方面进行了研究。文献[6]提出一种基于低功耗蓝牙的无线安全预警系统。

目前对蓝牙系统的攻击最大的威胁还是来自于对鉴权过程的攻击，攻击者不仅可以针对鉴权过程中不对鉴权次数的限制发起 DoS 攻击，还可以伪装成其他设备的方式通过鉴权，监听信道和截获敏感信息。文献[7]中鲍博武提出了一种无证书的高效认

* **基金资助：** 本文得到南宁学院一流专业培育项目(2020YLZYPY01) 和南宁学院教学质量与教学改革工程项目《网络安全》核心课程（2022BKHXK09）资助.
** 通讯作者：李建，教授，943667593@qq.com

证密钥协商协议，在通信和计算开销上具有优势，适用于资源受限的蓝牙设备。

车载蓝牙门锁是一种使用手机等便携式移动设备取代传统的车辆门锁钥匙，可实现车辆解锁、启动等指令的交互[8]。在车载蓝牙门锁系统中，一般都是使用了蓝牙进行通信，因此蓝牙的安全也将会直接影响车辆的安全。然而，蓝牙协议存在的安全风险使其无法直接应用于车载蓝牙门锁，需要探求一种能够实现安全蓝牙通信的解决方案，且该方案需要能够实现车载蓝牙门锁提出的各种需求。目前，有关这方面的演研究成果不多。

本文提出一种用于应对车载蓝牙门锁对蓝牙安全性需求的方案，重点研究蓝牙安全通信问题，使用SM2、SM3、SM4 以及数字签名技术从蓝牙接入验证和授权以及数据安全层面上构建对称和非对称密钥体系，实现数字签名、签名验证、密钥的管理和密钥的协商与公钥的交换。该方案使得移动终端能够安全地完成指令交互，并能够授予次级权限。

2 车载蓝牙门锁的安全需求分析

车载蓝牙门锁是一种使用手机等便携式移动设备取代传统的车辆门锁钥匙，可实现车辆解锁、启动等指令的交互。车载蓝牙门锁要实现的功能是：一是鉴权，明确移动终端具有哪些权限，同时保证指令的交互必须是安全的；二是最高权限的变更，即车主的变更；三是普通权限授予，最高权限拥有者可授予他人普通权限，满足朋友借车及家人用车的需求。为了实现这三大功能，车载蓝牙系统需要具有移动终端应用、车载蓝牙模块、云端服务器三大部分[17]。其中，移动终端用于与车载蓝牙模块完成指令交互、普通权限授予，通信方式为蓝牙通信；也可以与云端服务器进行通信，但是这要求必须处于网络环境，且必须是网络安全通信，用于实现普通权限授予与车辆密钥拉取。车载蓝牙模块与云端服务器的通信必须依赖于安全的网络的通信，其用于实现密钥的同步，而不能用于实现指令的交互。

针对蓝牙的攻击可以被分为主动攻击和被动攻击。主动攻击指非法的未认证的地方通过伪装成合法的设备，对设备间通信的数据进行截获或者修改。这可以是通过身份假冒实现数据窃密、数据篡改、拒绝服务攻击以及中间人攻击。被动攻击指第三方通过对通信双方的信道进行监听，从而获取到敏感信息的方式。这可以是数据流分析的方式。

在链路层安全机制中，第一次通信的双方依赖于 PIN 码用于生成初始密钥和鉴权，而 PIN 码是作为双方通信的唯一互信基础，但是在蓝牙协议中，鉴权完成之前通信双方交换的所有数据都是使用的明文传输的方式，且 PIN 码的验证方式、密钥生成算法等都是公开的，以当前计算机的计算能力极易通过穷举的方式破解。此时攻击者只需要再伪造自己的设备地址将可以轻松实现身份假冒、数据窃密和数据篡改。

在蓝牙中确定一个设备的唯一标识是设备地址，而在公共链路密钥生成之前的所有信息传输都是以明文进行传输的，因此只需要两台设备分别伪造通信的双方进行鉴权过程数据的转发就可以实现数据窃密和篡改，也就是中间人攻击。甚至，因为蓝牙只规定了鉴权失败后需要经过一段时间后才能再次鉴权，却没有规定鉴权的最大次数，攻击者可以利用这点使得合法设备一直无法连接。

表 2 协议通信符号说明

符号	说明
uid	一个伪PIN码对应一个uid，一旦连接成功除非身份过期否则一直存在
token	伪PIN码生成的用于初次连接加密的密钥
m_addr	移动终端的蓝牙设备地址
c_addr	车载蓝牙的蓝牙设备地址
m_pub_key	移动终端应用的SM2算法公钥
m_pri_key	移动终端应用的SM2算法私钥
c_pub_key	车载蓝牙的SM2算法公钥
c_pri_key	车载蓝牙的SM2算法私钥
randomA	随机数A
randomB	随机数B
randomC	随机数C
ciphertext	密文
response_code	响应码
msg	响应消息体
cur_tsp	当前时间戳
‖	拼接操作
SM2_sign	SM2算法签名操作

3 车载蓝牙门锁安全解决方案设计

本节将论述一套可用的车载蓝牙门锁安全解决方案。该方案使用这种密钥管理技术实现蓝牙用户接入认证和授权系统应用，并在数据安全层面上构建对称和非对称密钥体系。为了方便方案的论文，表 1 给出了所涉及的一些蓝牙通信协议的一些参数符号及含义。

在蓝牙中，鉴权后的数据传输安全主要依赖加密密钥的对称加密方式，不对加密过后的数据进行有效性验证的，因此是存在数据重放攻击和通信业务否认风险的，如果这种攻击被用于控制车辆，后果对于车载蓝牙门锁系统来说是致命的。因此要实现

一个安全的车载蓝牙门锁系统，要求解决 PIN 码不安全、设备地址对通信的另一方的唯一标识、密钥的交换、鉴权次数不限制带来的无限重试、数据的时效性、数据来源可信六大问题。

3．1 用户接入认证和授权设计

在本文的车载蓝牙门锁系统中，将用户的权限分为两种。一种是普通用户，拥有临时权限，权限可能会有过期时间，不能进行授权操作，只能用于数据通信；另一种是管理员权限，能够创建临时权限，表现为车辆的所有人，拥有将车辆临时外借的权限。蓝牙用户拥有哪种权限取决于用户在连接蓝牙时使用的伪 PIN 码。在本文的系统中，移动终端是通过与车载蓝牙模块交互，完成指令交互、普通权限授予。

在移动终端设备第一次向车载蓝牙模块请求连接时，首先需要拿到车载蓝牙模块预先生成的伪 PIN 码。车载蓝牙模块在生成伪 PIN 码时将伪 PIN 码与权限和移动设备的蓝牙设备地址进行绑定，使用不同的伪 PIN 码在连接后移动终端拥有的权限也会不同，同时一个伪 PIN 码只能被一个终端使用，其在连接认证中对安全的保障发挥了重要的作用。

经过三轮的数据交换后，移动终端和车载蓝牙模块完成了蓝牙设备地址、三个随机数和公钥的交换，且交换过程是加密通信的，避免了蓝牙协议由于生成链路密钥算法的公开和信息明文传输导致的 PIN 码被破解的问题。但是这种加密传输的方式仍然不能确保伪 PIN 码是绝对安全的，攻击者仍然可以通过穷举的方式暴力破解伪 PIN 码。因此，在认证鉴权时需要比对移动终端的蓝牙设备地址，只有比对成功车载蓝牙模块才会进入半连接状态。这样就使得攻击者若要通过暴力穷举破解，就需要同时穷举出正确的伪 PIN 码和其绑定的蓝牙设备地址，且伪 PIN 码应该是只在一定时间范围内有效的，这样就可以极大地提升了暴力破解的难度，且不会造成对拒绝服务攻击抵御能力的下降。后果就是在生成伪 PIN 码时必须传入需要绑定的蓝牙设备地址，但是在这种有上层应用封装的情况下是允许的，在应用的屏蔽下，用户只需要知道伪 PIN 码就可以进行连接认证操作，其他操作对用户都是透明的。

在这个鉴权流程中，因为移动终端应用持有正确的伪 PIN 码和蓝牙设备地址，因此车载蓝牙模块认为双方拥有互信的基础，双方无条件认为解密后拿到的数据是正确的，在互信的基础下加密传输的公钥也得到了信任，免去了 CA 证书的验证，实现了无 CA 证书的密钥交换。同时，三轮数据交换后，双方都持有了相同三个伪随机数，这三个伪随机被用于生成加密密钥，三个伪随机数的交换过程也就是加密密钥的协商的过程。

在二次连接中，因为车载蓝牙模块和移动终端应用都拥有了对方的公钥以及连接的 uid，因此二次连接可以复用初次连接时生成三个随机数的方式协商出这次连接通信的对称加密密钥。为了保证通信的数据安全，除了加密通信数据外，还必须使用数字签名技术对密文签名，防止数据被篡改。

具体的操作流程如下：

① 移动终端应用发起连接请求，以明文的方式携带上 uid，用 c_pub_key 加密新生成的 randomA 和 cur_tsp，然后将加密后的密文使用 SM3 求出哈希值并使用 m_pri_key 对哈希值签名发送到车载蓝牙模块。

② 车载蓝牙模块收到连接请求，根据 uid 判断是否拥有连接的权限并拿到存储的 m_pub_key 验证签名是否有效，有效则解密拿到 randomA 和 cur_tsp，判断 cur_tsp 是否有效，cur_tsp 有效进入半连接状态并使用 m_pub_key 加密生成的 randomB，求密文的哈希值做签名操作并返回。验签无效或 cur_tsp 无效则快速结束流程。另外，uid 没有连接权限可能是身份过期或者 uid 不存在。

③ 移动终端拿到响应数据使用 c_pub_key 验证签名并解密拿到 randomB，加密 randomC 返回到车载蓝牙模块。

④ 最后车载蓝牙拿到 randomC，生成加密密钥并返回连接成功响应码与消息体，完成这次连接加密密钥的协商。

3．2 通信数据安全设计

连接成功后，双方已经协商出了这次连接通信使用的对称加密密钥，持有了对方的公钥，并且双方持有的公钥是可信的，那么就可以通过数字签名技术使得通信具有防御身份假冒、数据窃密、数据篡改和通信业务否认的能力以及一定的抗数据流分析攻击的能力。到了这一步，在蓝牙通信安全中还需要实现抗重放攻击。

在本文的方案中，要求数据发送方在每一条数据中都必须携带当前时间戳，且这个时间戳是被加密并签名的，以确保这个时间戳不会被篡改。接收者将会为每一个 uid 记录一个最近处理的数据携带的时间戳 recent_timestamp，若发现请求数据所携带的时间戳小于 recent_timestamp 则过滤掉该请求。

设计思路是：使用对称加密与非对称加密来实现数据传输的安全，而非对称加密对于公钥的验证通常的方式是依赖于网络对 CA 证书进行验证。为此，对公钥的交换以及对称加密密钥的协商成为了论文研究的难点。

为解决这一难点，论文使用了一个伪 PIN 码，伪 PIN 码在表现形式与蓝牙的 PIN 码一致，但是在处理上大大不同。伪 PIN 码的产生必须是由被连接者生成，且伪PIN码不能在任何不安全环境中传输。在这个前提下，连接者拿到这一正确的伪 PIN 码生成初次连接的加密密钥并对连接交换的数据进行加密发送到被连接者，被连接者若能够正确解密，则可以认定与之通信的连接者不是不可信的第三方，实现了公钥验证以及防数据窃密的功能。

在蓝牙通信中，拒接服务攻击的主要攻击方式有两种，一种是攻击蓝牙使得耗尽资源无法提供服务；若蓝牙对认证次数有次数限制，则可以通过发起大量的认证请求，使得任何设备都无法连接到这一蓝牙达到攻击的目的。因此本论文在设计伪 PIN 码的认证时，要求是不能有连接次数认证且对非法请求能够快速拒绝快速释放连接所需要的资源。在车载蓝牙门锁中，每一个伪 PIN 码的生成都对应着一个使用车俩的人员，但是车俩何时被该用车人初次使用是不确定的，因此在伪 PIN 码的生成到销毁的时间是不确定的，在这个不确定的时间内攻击者就可以通过破解伪 PIN 码来连接到车载蓝牙模块，使得车俩的安全失去保障。在没方案的实现中，伪 PIN 码是一个 16 位的密钥，只用于初次连接，在伪 PIN 码生成到销毁的这个不确定的时间内，16 位密钥不能够给我们对安全足够的信心，因此在设计中要求每一个伪 PIN 码绑定一个蓝牙设备地址，只有在伪 PIN 码和蓝牙设备地址都认证通过的前提下才是连接双方才是互信的。若攻击者使用穷举的方式破解，就要求同时穷举出正确的伪PIN码和蓝牙设备地址，大大提升了破解的难度和成本。

在二次连接以及数据通信中，公钥的交换已经完成，伪 PIN 码不再被使用，身份的验证和数据的防篡改、防窃密都可以加密和数字签名技术来实现。二次连接中，对称加密密钥的协商使用了公钥加密、私钥解密以及对密文签名的方式来保证安全传输。由于非对称加密能够加密的数据长度是受公钥长度限制，在 SM2 中公钥的长度是 64 字节，因此在二次连接中一次加密的数据不超过 64 字节长度，在数据交换中更是不适于使用非对称加密。所以在数据通信中使用的是连接过程中协商出来的密钥使用 SM4 进行对称加密，以及对密文进行摘要后进行签名。

至此，全过程都是在加密环境中进行，使得本文的方案具备了抗身份假冒、抗数据窃密、抗数据篡改、抗拒绝服务、抗通信业务否认风险以及一定的抗数据流分析风险的能力。但是在连接认证和数据通信交换中仍存在数据重放风险，数据重放在连接过程可能造成的后果是使得对拒绝服务攻击的抵御出现缺口，使得蓝牙连接资源耗尽。为此，本文解决问题的方式是对时间戳进行验证的方式堵上这个缺口，当然也可以通过控制一个 uid 只能使用一个连接资源的方式进行抵御。在数据通信过程中，数据重放导致的后果可能是致命的也可能是无关紧要的，本文中是在处理数据之前根据时间戳进行一次过滤的方式抵御。

3．3 方案的安全分析

在蓝牙安全连接的初次连接中，连接流程的开始始于连接者持有正确的伪PIN码和蓝牙设备地址，不存在身份假冒风险，且全流程数据都是加密传输的，对数据流分析有一定抵御能力。由于数据都是加密传输，若攻击者想要窃取数据或者篡改数据，则说明攻击者掌握了正确的伪 PIN 码，这有可能是伪 PIN 码在不安全环境中传输造成的，而这与本论文的基石相悖，即伪 PIN 码只在安全环境传输，因此不成立。那么攻击者只有可能是通过穷举等手段进行破解的，伪 PIN 码在理论上是有可能被穷举破解的，但是需要同时穷举出正确的伪 PIN 码和蓝牙设备地址。进一步提高伪 PIN 码安全，论文提供有两种手段，一种是增加伪 PIN 码的长度，另一种是限制伪 PIN 码的有效时间。尽管在初次连接时使用了 SM4 加密，密钥（token）长度固定为 16 位，但是生成 token 的伪 PIN 码长度是不固定，且伪 PIN 码在生成时需要指定其有效时间区间，在有效时间区别之外即使是合法设备连接也会被拒绝。因此使用者可以根据业务对安全的容忍度灵活调整伪 PIN 码长度和其有效时间区间以应对数据窃密、数据篡改以及身份假冒等风险。在应对数据重放上，伪 PIN 码在使用过一次之后便被销毁，此时数据重放攻击对其无效。因为初次连接只对伪 PIN 码和蓝牙设备地址验证，不对连接另一方身份进行认证，因此不需要考虑通信业务否认攻击。

初次连接主要依赖于 SM4 算法的加密，SM4 算法在加密和解密耗时上明显高于 DES 和 AES 算法，但是在初次连接中交换数据较少、流程较短，对加解密耗时不敏感，且 SM4 算法是采用分组加密的方式，一次处理 128 位数据，加密速度足够快，能够满足本论文要求。另一方面，在初次连接中不再需要访问 CA 服务器即可认证信任公钥，节约了资源并提高了效率。

在二次连接中，数字签名被用作身份的识别鉴定，验签不仅是验证数据的完整性，同时也是验证发送方的身份。此时双方公钥已经完成了交换，且公钥是可信任的。在每一轮交换的数据都会被加密且签名，基于信任的公钥对签名进行验证即可确认通信另一方的身份和保证数据不被篡改不被窃密。并且

在第一轮数据交换中，时间戳被加密且签名，因此时间戳被除发送方外的第二人修改，发送方的身份也被唯一确定，可抵御数据重放攻击。数字签名的天然特性使得数据不可抵赖，可抵御通信业务否认风险。

在二次连接中使用的是非对称加密和数字签名技术，安全性高，其风险来源于公钥的是否可信，在初次连接中已经对次提出了解决方案。也正是因为使用了非对称加密，加解密速度上要比对称加密要慢得多，且加密的数据长度受公钥限制，但是在二次加密中需要交换的数据较少，对加解密速度的容忍性高，因此非对称加密符合本论文要求。

同二次连接过程，在数据通信中数字签名同样被用于身份鉴定，结合对时间戳的验证可抵御数据重放、身份假冒、通信业务否认。在应对数据窃密和数据篡改上同二次连接是一致的。无论是在连接过程还是在数据通信过程，所有数据都是加密传输，可抵御数据流分析。

3．4 方案的代码实现与性能测试

为了验证本文提出的车载蓝牙门锁系统设计方案的可行性和有效性，本文使用 C 语言对设计的连接流程、数据通信进行代码实现。鉴于本文的设计方案是基于蓝牙协议通信的上层应用封装来实现蓝牙安全通信，因此在系统的实现上，本文使用了 socket 作为数据传输的通道进行模拟蓝牙通信。

下面简单介绍具体的代码实现过程。

(1) 初次连接流程代码实现

① 移动终端向车载蓝牙模块发起初次连接请求，即请求者向被请求者发起连接请求：

• 移动终端获取到伪 PIN 码，根据伪 PIN 码生成 uid 和 token，获取到本地蓝牙设备地址和生成一个密码学安全的随机数。然后将 uid 和本地蓝牙设备地址和生成的第一个随机数 A 使用 SM4 算法、token 作为密钥加密并发送到车载蓝牙模块。

• 移动终端接收车载蓝牙模块响应数据，使用 SM4 算法解密，若解密成功且响应码为成功，从响应数据中拿到车载蓝牙模块的公钥、蓝牙设备地址和第二个随机数 B，生成自身的非对称密钥对和第三个随机数 C，并将自身的公钥和随机数 B 加密返回到车载蓝牙模块。

• 接收车载蓝牙模块返回的数据并解密，若响应码为成功，即初次连接成功，通过拿到的三个随机数生成用于数据通信的对称加密密钥。

② 车载蓝牙模块接收到移动终端的初次连接请求，即被请求者接收到请求者发起连接请求：

• 车载蓝牙处理初次连接请求，根据请求中携带的 uid 获取到相应的 token，判断 uid 对应的 token 是否有效，若 token 有效则进入下一步解密，解密成功且密文中携带了正确的蓝牙设备地址，则进入半连接状态，进一步从解密的数据中拿到第一个随机数 A，并生成自身的非对称加密密钥对和第二个随机数 B。将随机数 B、自身的蓝牙设备地址和公钥使用 SM4 加密返回移动终端。若解密失败或携带的蓝牙设备地址不匹配，则快速返回，即快速释放资源，且返回的信息中不能使连接请求者判断出具体是伪 PIN 码错误或是蓝牙设备地址不匹配。

• 接收移动终端返回的数据，解密拿到第三个随机数 C 和移动终端的公钥，此时连接已成功，使用三个随机数生成用于数据通信的对称加密密钥。

③ 向移动终端返回加密的连接状态码和响应信息，可能是连接失败也可能是连接成功，若连接成功，需要将保存的伪 PIN 码删除，防止伪 PIN 码被第二次使用。

(2) 二次连接流程代码实现

二次连接使用的是非对称加密与数字签名技术，与初次连接在处理在处理上大大不同，初次连接只使用了 SM4 算法，而二次连接使用了 SM2 和 SM3 算法。

① 移动终端向车载蓝牙模块发起二次连接请求：

• 移动终端应用生成第一个随机数 A，将当前时间戳和随机数 A 使用 SM2 算法加密，SM3 算法对加密后的密文做哈希，最后对哈希后得到的摘要值签名并连同密文发送到车载蓝牙模块。

• 接收车载蓝牙模块返回的数据，验签并解密获取到随机数 B。然后生成随机数 C，并将随机数 C 加密并签名返回到车载蓝牙模块。

• 接收车载蓝牙模块响应数据，若返回的响应码为成功，则根据三个随机数生成对称加密密钥。

② 车载蓝牙模块接收到移动终端应用发起的二次连接请求：

• 车载蓝牙拿到请求携带的 uid，先根据 uid 判断该 uid 是否仍然具有连接资格，再拿到相应的所有非对称密钥，然后使用密钥验签并解密。验签解密成功后判断密文携带的时间戳是否有效，若无效需要快速释放连接资源。时间戳验证通过则获取随机数 A，生成随机数 B 并将随机数 B 加密并签名响应给移动终端应用。

• 接收移动终端的响应数据，验签并解密获取到随机数 C，使用三个随机数生成对称加密密钥。给移动终端应用响应连接状态信息。

(3) 数据通信与数据过滤代码实现

移动终端应用向车载蓝牙发起数据通信，发送的数据必须携带当前时间戳，使用连接过程中协商出来的密钥以及 SM4 算法对时间戳和要发送的数据进行加密，然后使用 SM3 算法对加密后的密文做哈希摘要，并使用移动终端应用的私钥对摘要数据进行签名，将签名和密文发送给车载蓝牙模块。具体的实现步骤如下：

• 等待车载蓝牙模块响应，使用车载蓝牙模块的公钥验签并解密，最后打印了响应的响应码和响应信息。

图 1 程序的性能测试运行结果

• 车载蓝牙模块接收到移动终端应用的数据通信后，验签并使用 SM4 解密，从解密后的数据中获取请求携带的时间戳，根据时间戳判断此次通信是否有效，若无效需要过滤此次请求，车载蓝牙模块将不处理此次通信数据。若根据时间戳验证此次通信有效，则更新 recent_timestamp，即更新维护的最近请求时间戳，并将数据交付给上层应用进行处理。

(4) 其他代码的实现

① 密码学安全的随机数生成函数，此函数可以指定要生成的随机数长度，依赖于 OpenSSL，在使用此函数之前，需要先调用 RAND_poll()函数初始化 OpenSSL 的随机数生成器。 密码学安全的随机数生成函数，此函数可以指定要生成的随机数长度，依赖于 OpenSSL，在使用此函数之前，需要先调用 RAND_poll()函数初始化 OpenSSL 的随机数生成器。

② 使用三个随机生成对称加密密钥的函数，此函数将三个随机数进行异或得到加密密钥，增加密钥的随机性。由于输入的随机数本就是密码学安全的，所以在这一步只要求相同的输入必能得到相同的输出就足够了。

③ 根据伪 PIN 码生成 token 和 uid 的函数。在本文中，伪 PIN 码被直接用作 token，uid 取伪 PIN 码的前 2Byte。伪 PIN 码是一个 16Byte 的密码学安全的随机数，本身就可以被用作对称加密的密钥，因此伪 PIN 码可直接用作 token。

④ 用于二次连接中的加密和签名函数，先使用 SM2 对数据加密，然后对密文使用 SM3 做哈希摘要，最后对摘要进行签名。

⑤ 用于二次连接的验签和解密函数，先对密文使用 SM3 算法求得哈希摘要，将摘要作为函数进行验签，验签通过后进行解密。

⑥ 用于数据通信的加密和签名函数，先使用 SM4 算法对数据加密，然后使用 SM3 算法对密文求得哈希摘要，最后使用 SM2 算法对摘要进行签名。

⑦ 用于数据通信的验签和解密函数，先使用 SM3 算法对密文求得哈希摘要值，然后使用 SM2 算法进行验签，验签通过后使用 SM4 算法进行解密。

(5) 程序的性能测试

本文方案的性能测试结果如图 1 所示。图中左边为车载蓝牙模块打印的日志，右边为移动终端应用打印的日志。

在程序中，车载蓝牙模块先移动终端应用启动生成伪 PIN 码并打印，移动终端应用启动后输入该伪 PIN 码，然后调用相应函数通过该伪 PIN 码生成对应的 uid 和 token，并使用 token 作为加密密钥完成初次连接的流程。可以看到两个程序打印的公钥信息以及三个随机数完全一致，可以证明车载蓝牙模块对 uid、token、设备地址的校验通过，双方可正常进行加密通信，且密钥是可在加密环境中协商的、双方对接收到的公钥是可信任的。

在二次连接中，可看到双方打印的随机数完全一致，可见双方可通过初次连接中交换的公钥完成非对称加密以及签名、验签流程，密钥可协商，对时间戳的校验无误，程序流程执行正确，代码可执行。

4 结束语

本文介绍了车载蓝牙门锁的安全功能需求，提出了一种车载蓝牙门锁的解决方案。该方案设置了两种通信方式，即加密的网络通信以及安全的蓝牙通信。为了应对车载蓝牙门锁对蓝牙安全的需求，本文使用了国密算法、数字签名技术、时间戳等技术在蓝牙用户接入认证和授权系统应用和数据安全层面上构建对称和非对称密钥体系，并使用 C 语言编程技术实现了论文提出的技术方案的蓝牙认证授权的流程和过期数据的过滤。本文的解决方案实现简单，具有可靠性、有效性和经济性。程序的性能测试说明了本文方案的可行性和有效性。

参 考 文 献

[1] 孙恒.低功耗蓝牙技术安全浅析[J].公安部检测中心,2021,(5):102-106.

[2] Suri P. R., Rani S.. Bluetooth security - Need to increase the efficiency in pairing[C]. IEEE Southeastcon, 2008:607-609.

[3] Iqbal M. M. W., Kausar F., Wahla M. A.. Attacks on Bluetooth Security Architecture and Its Countermeasures[M]. Berlin: Information Security and Assurance, 2010:190-197.

[4] 林韦妍.蓝牙协议分析及改进算法实现[D]. 西安：西安电子科技大学,2015.

[5] 李颖川,王珺吉,姚伟.低功耗蓝牙技术的安全机制研究[J]. 物联网技术. 2020,10(09):45-47

[6] 王建新,苏俊盼,郑一麟.基于低功耗蓝牙 4.0 技术的安全预警系统设计[J].物联网技术. 2019,9(11):98-100, 104

[7] 鲍博武.面向移动语音安全的蓝牙密钥协议关键技术研究[D].郑州：信息工程大学,2020.

[8] 卓宏刚.车载蓝牙门锁系统的研究与设计[D]. 重庆:重庆邮电大学，2018