·车联网量子加密通信技术专题·

车载自组织网络下基于区块链与量子密钥的组密钥分发方案*

程腾[1] 刘强[1] 石琴[1] 王川宿[2] 张星[2]

（1.合肥工业大学，自动驾驶汽车安全技术安徽省重点实验室 安徽省智慧交通车路协同工程研究中心，合肥 230009；2.奇瑞汽车股份有限公司，芜湖 241000）

【摘要】为提高车载自组织网络（VANET）的通信效率和安全性，提出了一种基于区块链与量子密钥的匿名身份认证与组密钥分发方案。利用车端随机数与云端随机数共同生成车辆匿名凭证，实现路端对车辆身份认证过程中的隐私保护；使用区块链进行组密钥的安全下发，降低量子密服平台的计算开销，实现车辆身份的撤销与追溯；提出了两段式组密钥生成方式，保证不同场景下组密钥分发的安全性与高效率，同时实现了前向安全与后向安全。信令开销与计算开销分析结果表明，该方案信令开销减少近50%，组密钥分发过程中车端计算开销减少44%，路端计算开销约为对比方案的20%。形式化安全分析结果证明了该方案的安全性和可行性。

主题词：车载自组织网络 匿名身份认证 区块链 组密钥分发 信息安全

中图分类号：TN929.5；TN918.4 **文献标识码：**A **DOI:** 10.19620/j.cnki.1000-3703.20230691

Group Key Distribution Scheme Based on Blockchain and Quantum Keys for VANET

Cheng Teng[1], Liu Qiang[1], Shi Qin[1], Wang Chuansu[2], Zhang Xing[2]

（1. Key Laboratory for Automated Vehicle Safety Technology of Anhui Province, Engineering Research Center for Intelligent Transportation and Cooperative Vehicle-Infrastructure of Anhui Province, Hefei University of Technology, Hefei 230009; 2. Chery Automobile Co., Ltd., Wuhu 241000）

【Abstract】In order to improve the communication efficiency and security of Vehicular Ad-hoc NETwork (VANET), this paper proposed an anonymous identity authentication and group key distribution scheme based on quantum key and blockchain. Anonymous credentials for vehicles were generated by a combination of random numbers on the vehicle side and random numbers in the cloud, which achieved privacy protection for the vehicle during authentication. The utilization of blockchain for secure distribution of group keys has been proposed, which reduced the computational overhead of the Quantum Secret Service platform and enabled vehicle revocation and traceability. A two-stage key generation method was devised to ensure the security and efficiency of group key distribution in various scenarios, as well as achieve forward and backward security. The signaling and computation overheads were calculated, the signaling overhead was reduced by nearly half. During the group key distribution process, the computational overhead at the vehicle was reduced by 44%, while the computational overhead at the roadside is approximately 20% of the overhead in the comparison scheme. The formal security analysis results proved the security and feasibility of this scheme.

Key words: VANET, Anonymous authentication, Blockchain, Group key distribution, Information security

【引用格式】程腾，刘强，石琴，等. 车载自组织网络下基于区块链与量子密钥的组密钥分发方案[J]. 汽车技术，2023(10)：1-8.

CHENG T, LIU Q, SHI Q, et al. Group Key Distribution Scheme Based on Blockchain and Quantum Keys for VANET[J]. Automobile Technology, 2023(10): 1-8.

*基金项目：国家自然科学基金项目（No. 82171012）；安徽省自然科学基金资助项目（No. 2208085MF171）；汽车标准化公益性开放课题资助（No. CATARC-Z-2022-01350）；中央高校基本科研业务费专项资金资助（JZ2023YQTD0073）。

1 前言

车载自组织网络（Vehicular Ad-hoc NETwork，VANET）是以车辆为节点构建的移动通信网络，可以有效改善道路交通状况[1-2]。在VANET中，车辆间及车辆与路端间需交换车辆位置、速度等隐私数据[3-4]，但该网络的拓扑结构极易发生变化，且易受到安全攻击，如分布式拒绝服务（Distributed Denial of Service，DDoS）[5]、女巫（Sybil）攻击[6]，最终造成隐私数据泄露[7-8]。

VANET场景下，车端的计算能力相对较弱，基于大数因子分解的公钥与私钥的加密方式难以适用[9-10]。相较于大数因子分解，基于离散对数问题的椭圆曲线算法[11-13]虽然令计算开销大幅降低，但是仍难以适应VANET复杂场景下低延时的需求。基于数字证书的身份认证方式的拓展性较差，管理、维护成本较高，且存在认证机构（Certification Authority，CA）安全性等问题[14-16]。匿名身份认证仅实现隐私保护，对于匿名车辆的信息无法做到可追溯、可撤销[17-18]。

现阶段，密钥分发方案主要包括集中式密钥分发方案和分布式密钥分发方案。Jiao等[19]提出基于逻辑树的分布式组密钥计算方法，结合组密钥的更新算法，文献[20]对树的结构进行了更新。但上述方案均建立在理想条件下，尚未考虑实际VANET的复杂场景。Shawky等[21]利用智能合约，实现了分布式组密钥的分发。但在组成员更新时，路端需向合约提交一笔交易，因其使用非对称加解密，计算开销较大。为保证数据的隐私和安全，文献[22]提出适用于物联网的认证和密钥管理方案。鉴于VANET是一种特殊的物联网，传统物联网的安全方案的适用性有待商榷。

集中式密钥分发方案的组密钥由密钥分配中心（Key Distribution Center，KDC）选择和分发，用户仅需保存与KDC之间的会话密钥[23-24]。文献[25]提出基于无证书身份认证的组密钥分发策略，但未考虑路端设备的合法性。文献[26]提出的方案实现了匿名与隐私保护，但未提及组密钥的更新方法。集中式密钥分发方案在大规模的网络条件下，KDC需要保存大量密钥，通信量的增加将导致其负担过重。

为弥补量子密服平台的缺陷，本文提出一种匿名身份认证与组密钥分发方案，完成匿名车辆的注销与追溯，同时将计算开销转移到路端，降低量子密服平台的通信量，从而实现组密钥的高效分发。

2 系统架构

本文提出的车联网（Vehicle-to-Everything，V2X）通信场景中，车路云的架构如图1所示，主要由密服平台、路侧单元（Road Side Unit，RSU）、车辆和区块链组成。车辆和RSU均可与密服平台建立点对点通信，路端与车辆、车辆与车辆之间通过PC5广播通信。密服平台由身份认证服务器（AUthentication Server Function，AUSF）、KDC与CA构成。AUSF主要负责车辆匿名凭证的生成与区块链的维护，KDC主要负责车端预充注密钥的无线更新和路端设备量子组密钥参数的管理，CA负责路端设备证书的颁发及撤销列表的维护。

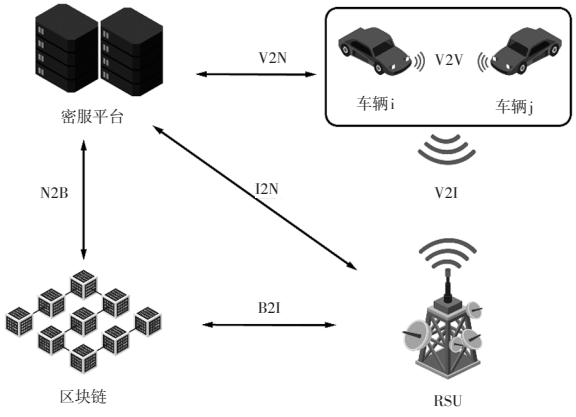


图1 系统架构

V2X场景中，车端已预先充注一定数量的量子会话密钥与量子完整性验证密钥。前期车路、车云之间不互信，双方在真正通信前均需进行身份互认，路端与云端通过安全信道连接。本文使用的符号与定义如表1所示。

3 主体方案

本文提出的方案包括5个阶段：初始化阶段、注册阶段、组密钥分发阶段、组密钥更新阶段以及撤销与追溯阶段。初始化阶段主要完成区块链、路端与车辆的初始化。注册阶段主要完成车辆匿名凭证的生成与车辆信息的记录。车辆与云端进行身份认证，获取车辆的匿名凭证，密服平台生成智能合约并将合约地址告知路端。完成注册后，各车辆与路端通过计算得到一定数量的匿名凭证和与之对应的智能合约的地址。组密钥分发阶段，路端通过智能合约完成对车辆的身份认证，获得预充注到车辆内部的量子密钥。路端计算组密钥参数并使用量子密钥对密钥进行加密，组播给当前合法车辆。在组密钥更新阶段，为保障组通信的前向安全与后向安全，即防止车辆加入或离开路端的组后仍可解密之前的信息，从而进行组密钥更新。追溯与撤销阶段实现对特定车辆的信息追溯与信息撤销。

表1　符号定义

符号	定义
VID_i	车辆i的唯一标识
RID_i	路端设备i的唯一标识
$H()$	单向哈希函数
$HMAC_{key}()$	使用密钥key对内容计算消息验证码
Mac/Mac'	消息验证码
T_v/T_v'	车辆产生的时间戳
T_s/T_s'	云平台产生的时间戳
$GSP-1$	组密钥参数1
$GSP-2$	组密钥参数2
GSK	组密钥
$E_{key}()$	使用密钥key对内容进行加密
$D_{key}()$	使用密钥key对内容进行加密
ANC_i	车辆i的匿名凭证
QSK	预充注量子会话密钥
QIK	预充注量子完整性校验密钥
QSK_{tag}	预充注量子会话密钥标识
QIK_{tag}	预充注量子完整性校验密钥标识
HSM	硬件安全模块
DC	路端数字证书
POS	智能合约地址
σ	数字签名
$\{\}_{i=1}^{n}$	n个参与者的合集

3.1　初始化阶段

3.1.1　唯一ID的赋予

车载单元(On Board Unit,OBU)的硬件安全模块(Hardware Security Module,HSM)中储存OBU的唯一标识VID与预充注的密钥。同理,路侧单元的HSM中储存有RSU的唯一标识RID。

3.1.2　车辆的密钥预充注流程

量子密服平台在OBU的HSM中预充注一定数量的QSK与QIK,同时预充注了n个用于接收组密钥的QSK。量子密服平台识别OBU内部预充注的密钥,并将密钥与密钥标识匹配。

3.1.3　CA为路端设备颁发数字证书

CA为第三方(车辆与路端均认可)的认证中心,根据路端的唯一标识为路端颁发数字证书,数字证书内包含路端的公钥信息。

3.1.4　区块链初始化

将区块链设置为私有链,量子密服平台为其管理者,且拥有唯一部署智能合约的权限。RSU均为区块链的节点,并被赋予调用智能合约的权限。

3.2　注册阶段

如图2所示,注册阶段,车辆与云端的密服平台进行交互,生成车辆的匿名凭证:

a. 车辆i从HSM获取身份唯一标识VID_i,量子随机数发生器产生n个真随机数RN_{i-c},获取当前时间,并使用车端预充注的量子会话密钥进行加密。同时,使用另一个预充注的量子完整性验证密钥针对加密后的消息计算消息验证码Mac,形成消息体M_1:$\{QSK_{tag},QIK_{tag},E_{QSK}(VID_i,\{RN_{i-c}\}_{i=1}^{n},T_v'),HMAC_{QIK}(E_{QSK}(VID_i,\{RN_{i-c}\}_{i=1}^{n},T_v')),T_v\}$,并将其发送至云端。

b. AUSF收到车辆的身份认证请求后,首先根据时间戳判断消息的有效性。如果时间差过大,则不处理收到的消息。根据收到的消息中的QSK_{tag}与QIK_{tag}找到对应QSK与QIK,计算消息验证码Mac'以验证消息的完整性。若消息完整,则使用QSK对消息进行解密,得到车辆的唯一标识VID_i与车端产生的随机数$\{RN_{i-c}\}_{i=1}^{n}$。AUSF对解密得到的VIN_i与数据库中查询获得的VIN_i进行比较,如果两者相等,则产生n个随机数$\{RN_{c-i}\}_{i=1}^{n}$,对解密后得到的随机数RN_{i-c}进行"加1"操作。通过$ANC_i=H(VIN_i,RN_{i-c},RN_{c-i})$计算车辆的$n$个匿名凭证,云端为车辆的$n$个匿名凭证生成$n$个智能合约与各智能合约的唯一标识,并将唯一标识$POS$与各匿名凭证的哈希值告知车端,通知车端已上传至区块链,量子密服平台从车辆预充注的密钥中选择一个QSK与QIK,并得到对应的QSK_{tag}与QIK_{tag},对消息内容加密并计算Mac,得到M_2:$\{QSK_{tag},QIK_{tag},E_{QSK}(\{RN_{i-c}+1,\ RN_{c-i},\ H(ANC_i),\ POS\}_{i=1}^{n},T_s'),\ HMAC_{QIK}(E_{QSK}(\{RN_{i-c}+1,RN_{c-i},\ H(ANC_i),\ POS\}_{i=1}^{n},T_s')),\ T_s\}$发送给车辆。

c. 车端收到密服平台反馈的消息,通过判断时间戳与本地的时间差进行后续处理。车端i根据消息中QSK_{tag}与QIK_{tag}在车端的安全介质内找到对应的QSK与QIK,计算Mac验证消息的完整性。若所获消息完整,则使用QSK进行解密,得到云端返回的$\{RN_{i-c}+1,RN_{c-i}\}_{i=1}^{n}$。车辆$i$计算得到相应的$n$个匿名凭证$ANC_i=H(VID_i,RN_{i-c},RN_{c-i})$,并计算收到的$POS$的哈希值。车端组装消息,告知云端计算结果,即$n$对$ANC_i$和$POS$,将车端组装消息$M_3$:$\{QSK_{tag},\ QIK_{tag},\ E_{QSK}(VID_i,\ \{H(ANC_i),\ H(POS)\}_{i=1}^{n},\ T_v'),\ HMAC_{QIK}(E_{,QSK}(VID_i,\{H(ANC_i),H(POS)\}_{i=1}^{n},T_v')),T_v\}$发送至云端。

d. 量子密服平台首先根据时间戳判断消息的有效性,决定是否进行进一步处理。AUSF根据所获消息的QSK_{tag}与QIK_{tag},在云端的安全介质内找到对应QSK与QIK,计算Mac'以验证消息的完整性。若消息完整,则

使用QSK对消息进行解密，进而得到ANC_i的哈希值与相应POS的哈希值。将通过云端计算步骤b得到的POS的哈希值与原始消息对比，相同则认为车辆已完成匿名凭证的计算，并获得POS。至此，初始化完成。

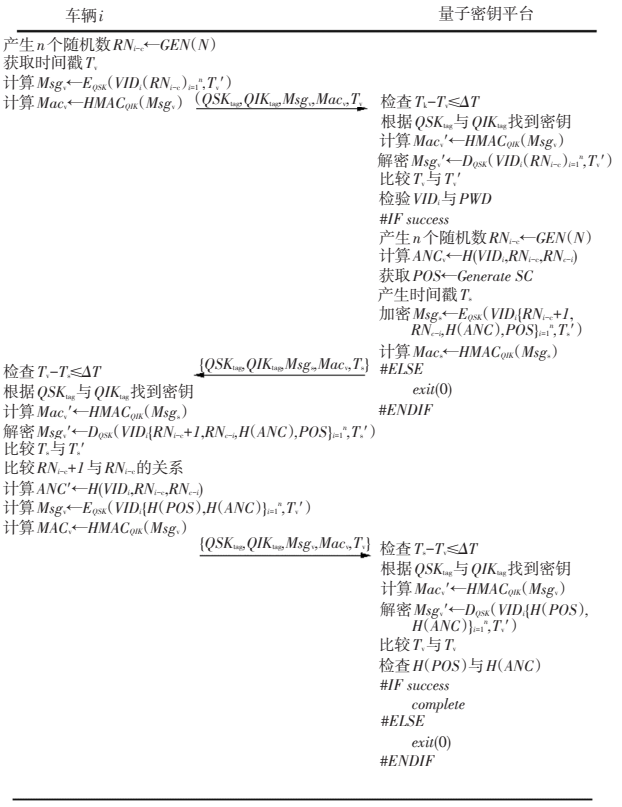


图2　注册流程

3.3　组密钥分发阶段

如图3所示，组密钥分发阶段车辆将与路端交互得到组密钥。流程为：

a. 路端在特定范围内广播所属唯一标识RID与数字证书DC，即M_4:{RID,DC}。

b. 车辆驶入路端通信范围后，通过PC5广播接收路端设备的数字证书，并验证路端身份的合法性。测试车辆确认路端的身份，车辆向路端广播自身的匿名凭证与参数，即M_5:{$E_{PK}(ANC_i,POS,T_v')$,T_v}。

c. 路端首先根据时间戳判断消息的有效性，决定是否进行进一步处理。路端使用私钥SK对消息解密，对比T_v与T_v'。通过解密得到的POS找到并调用智能合约，反馈预充注在车辆中的密钥QSK，则可认证车端身份合法性。路端随机数发生器产生一个随机数作为GSP−1，将调用智能合约所得对称密钥QSK对GSP−1进行加密。RSU循环上述过程，完成所有车辆的认证。路端计算当前所有合法车辆的匿名凭证的哈希值作为GSP−2，使用私钥对消息进行签名得到σ，拼接时间戳后，将T_s组播给当前所有车辆。消息内容为M_6:{GSP−2,{$H(ANC_i)$,QSK_{tag},E_{QSK}(GSP−1,T_s')}$_{i=1}^n$,σ,T_s}。

d. 车端接收组播消息，检查特定的匿名凭证的哈希值，存在即为验证成功，反之验证失败。验证成功的车辆截取消息GSP−2，凭借路端证书获得的公钥对签名进行验证。对消息解密得到GSP−1，根据得到的组密钥GSP−1与GSP−2计算出组密钥GSK=H(GSP−1,GSP−2)。

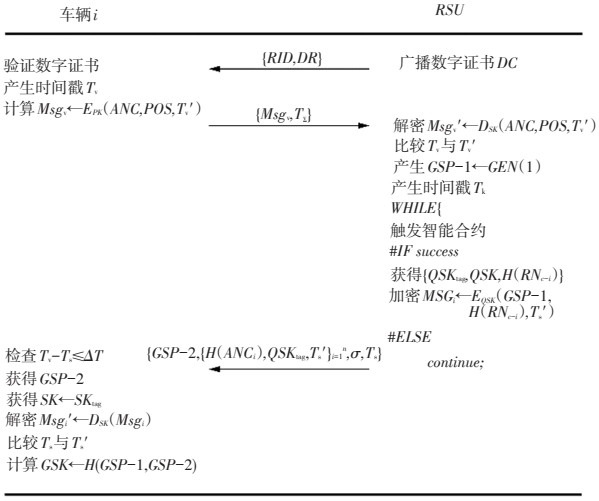


图3　组密钥分发流程

3.4　组密钥更新阶段

由于路端设备固定，路端广播通信范围内的车辆会持续更新。将路端广播通信范围内的车辆视为一个组，路端设备管理的组所面临的车辆更新可分为新成员加入和组成员离开2种情况。

新成员加入过程的组密钥更新流程为：

a. 当新的车辆完成初始化，准备加入当前路端设备管理的组以获得组通信服务时，为保证前向安全与后向安全，需对组通信加密的密钥进行更新。路端对新加入车辆j发送的信息进行处理，通过POS找到智能合约，并对其进行调用，若返回$H(RN_{c-i})$与密钥QSK，则认为车端身份合法。其中，GSP−1保持不变，路端通过调用智能合约所得密钥QSK对GSP−1加密。新加入车辆身份认证完成后，路端将重新计算当前所有合法车辆的匿名凭证的哈希值作为GSP−2，并使用私钥对消息进行签名得到σ，拼接时间戳后，将T_s组播给当前所有车辆，即{GSP−2,{$H(ANC_i)$,QSK_{tag},E_{QSK}(GSP−1,T_s')}$_{i=1}^1$,σ,T_s}。

b. 对于新加入车辆，执行组密钥获取阶段步骤d。对于组内原有成员，仅需重新获得GSP−2，进而计算GSK。

组成员离开过程的组密钥更新流程为：

a. 路端判断当前车辆是否为当前组成员，若已确认，路端将重新生成GSP−1，并对之前调用智能合约得到的密钥进行加密。此时，重新计算当前组内剩余合法

车辆的匿名凭证的哈希值为GSP-2，并使用私钥对参数进行签名得到σ，拼接时间戳后，将T_s组播给当前所有车辆，即{GSP-2,{$H(ANC_i)$,QSK_{tag_i},E_{QSK}(GSP-1,T_s')}$_{i=1}^{n-1}$,σ,T_s}。

b. 组内剩余车辆接收组播消息，通过检索匿名凭证判断当前位置。组内剩余车辆截取消息GSP-2，利用路端证书获得的公钥对签名进行验证，QSK_{tag}找到密钥QSK，进行解密得到GSP-1。由组密钥GSP-1与GSP-2得到组密钥$GSK=H$(GSP-1,GSP-2)。

3.5 撤销与追溯阶段

3.5.1 撤销

如图4所示，路端或者车辆获取当前时间，随即向量子密服平台上传车辆信息，并使用QSK加密得到(ANC_i,POS)，计算出Mac发送至量子密服平台。云端的身份认证服务器收到车辆的身份认证请求后，首先根据时间戳判断消息的有效性，决定是否进行进一步处理。云端的身份认证服务器根据收到的QSK_{tag}与QIK_{tag}，在云端的安全介质内找到对应的QSK与QIK，计算Mac'以验证消息的完整性。如果消息完整，则继续使用QSK对消息解密，得到车辆的ANC_i与POS，AUSF获取ANC_i对应的VID，判断车辆信息是否泄漏。如果车辆信息发生泄露，量子密服平台立即销毁VID对应的智能合约，从而实现车辆的撤销。

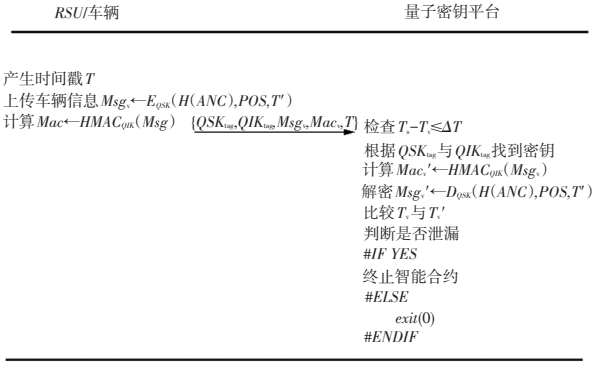


图4 撤销流程

3.5.2 追溯

监管机构欲根据车辆的匿名凭证获取车辆的具体行程，量子密服平台凭借匿名凭证检索其真实身份VID，凭借VID找到其智能合约，通过智能合约的事件日志查看具体行程，同时反馈给监管机构，从而实现车辆信息全生命周期可追溯。

4 形式化安全性证明

Scyther能够对协议模型进行建模、分析和验证，检测协议中可能存在的安全漏洞和缺陷。建模时，需要对协议的安全属性进行声明，描述协议应满足的安全属性，包括协议执行过程中的行为，例如身份认证、密钥交换、消息完整性、机密性等。通过声明和验证这些安全属性，检测协议中可能存在的漏洞和攻击，确保协议的正确性和安全性[27]。本文涉及的安全属性包括：

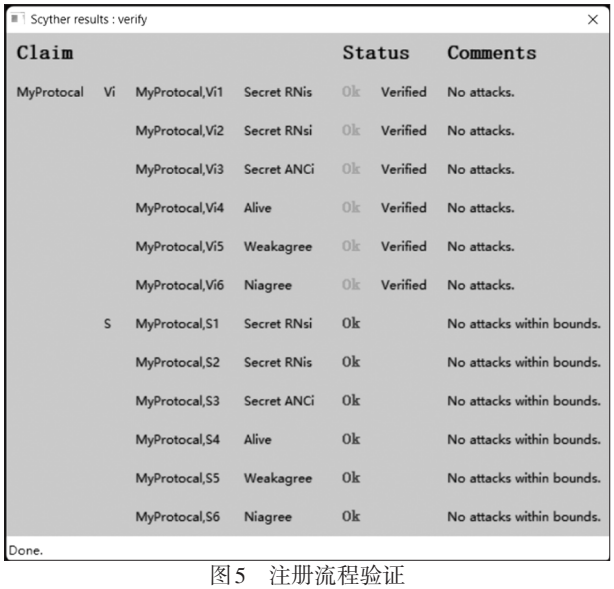
a. 机密性(Secret)，用于指定协议或系统中的机密信息，包括加密密钥、密码等。为保护信息安全，仅支持授权后访问使用。

b. 活性(Alive)，用于验证协议或系统的活性(Liveness)。若该系统或协议具有活性属性，则将于特定时间点执行特定操作或产生特定响应。

c. 弱一致性(Weakagree)，为协议安全属性，指两个或多个实体在协议的某个点上是否达成一致。在Scyther中，该属性用于检查协议中的实体是否达成共识，并不需要与其决策完全相同。

d. 不一致性(Niagree)，同样为协议安全属性，指两个或多个实体在协议的某个点上是否不能达成一致。在Scyther中，该属性用于检查协议中的实体是否不能达成共识。

在本方案建模过程中，共有3种角色，即车端V、路端R与量子密服平台S。车端V与量子密服平台S生成匿名凭证的流程验证结果如图5所示，车端V与路端R的组密钥分发流程的验证结果如图6所示。可以看出，3种角色均可实现机密性、活性、弱一致性、不一致性属性，这意味着实现了相互认证。形式验证的结果表明，本文的组密钥分发方案具有安全性。


Scyther results : verify

Claim				Status		Comments
MyProtocal	Vi	MyProtocal,Vi1	Secret RNis	Ok	Verified	No attacks.
		MyProtocal,Vi2	Secret RNsi	Ok	Verified	No attacks.
		MyProtocal,Vi3	Secret ANCi	Ok	Verified	No attacks.
		MyProtocal,Vi4	Alive	Ok	Verified	No attacks.
		MyProtocal,Vi5	Weakagree	Ok	Verified	No attacks.
		MyProtocal,Vi6	Niagree	Ok	Verified	No attacks.
	S	MyProtocal,S1	Secret RNsi	Ok		No attacks within bounds.
		MyProtocal,S2	Secret RNis	Ok		No attacks within bounds.
		MyProtocal,S3	Secret ANCi	Ok		No attacks within bounds.
		MyProtocal,S4	Alive	Ok		No attacks within bounds.
		MyProtocal,S5	Weakagree	Ok		No attacks within bounds.
		MyProtocal,S6	Niagree	Ok		No attacks within bounds.

Done.

图5 注册流程验证

5 信令开销与计算开销

5.1 信令开销

为定量验证本文方案的实用性，将提出的方案与文

献[21]、文献[28]的方案进行对比。假设车路间组密钥分发场景中共有n辆汽车和1个路端设备。网络通信中维护连接所消耗的资源远大于内容存储消耗的资源，故本文未使用传统方案中计算参与者通信传输所需的数据量，而选择比较发送的消息数量。表2所示为组密钥分发过程中车、路之间的消息发送流程与建立的总连接数量。

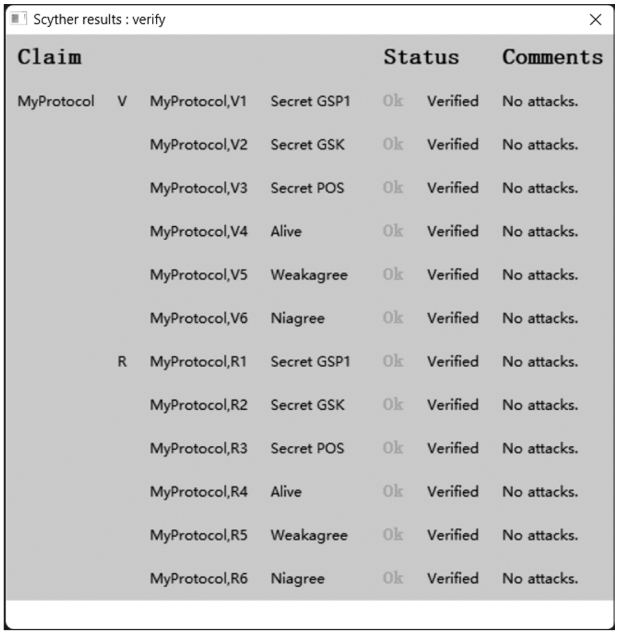


图6　组密钥分发验证

表2　不同方案信令开销　　轮次

方案	消息发送流程	信令开销
文献[21]方案	$OBU\xrightarrow{n}RSU\xrightarrow{n}OBU$	$2n$
文献[28]方案	$OBU\xrightarrow{n}RSU\xrightarrow{n}OBU$	$2n$
本文方案	$OBU\xrightarrow{n}RSU\xrightarrow{1}OBU$	n+1

5.2　计算开销

为保证计算开销的准确性，在内存8 GB的I5-7300HQ平台上计算不同操作所需时间，通过累加方式计算耗时。由于单次操作的耗时较短，计算存在较大误差，本文循环100 000次，计算平均耗时。假定所有方案使用的哈希算法为SHA-256，消息验证采用哈希运算消息认证码（Hash-based Message Authentication Code，HMAC），椭圆曲线密码体制（Elliptic Curve Cryptosystem，ECC）使用相同的椭圆曲线，对称加密算法为SM4，非对称加密使用SM2算法。本文借助OpenSSL库计算各操作的计算开销，测试代码已上传到https://gitee.com/liuqiang112358/timetest。具体计算开销如表3所示。

计算车辆与路端完成组密钥分发过程中所有交通参与者的通信开销，结果如表4与图7所示。

表3　不同操作计算开销　　μs

参数	取值
SHA-256计算时间T_h	0.245 6
HMAC计算时间T_{hmac}	2.016
ECC私钥签名时间T_{sign}	23.48
ECC公钥验证时间T_{veri}	72.39
ECC标量乘法时间T_{mul}	506.3
SM2私钥解密时间T_{sk}	46.13
SM2公钥加密时间T_{pk}	91.81
二次多项式时间T_{poly}	57.34
SM4对称密钥加解密时间T_{sm}	5.100

表4　方案对比　　μs

方案	车端计算开销	路端计算开销
文献[21]	$2T_{sm}+T_{veri}+T_{sign}+T_{mul}\approx547.37$	$N(2T_{sm}+T_{veri}+T_{mul})\approx588.89N$
文献[28]	$4T_h+T_{pk}+T_{veri}+T_{sign}+2T_{poly}\approx303.262\ 4$	$N(4T_h+T_{sk}+T_{veri}+T_{sign}+2T_{poly})\approx257.662\ 4N$
本文方案	$T_{sm}+T_{veri}+T_h+T_{pk}\approx169.545\ 6$	$N(T_{sk}+T_{sm})+T_h+T_{sign}\approx23.725\ 6+51.23N$

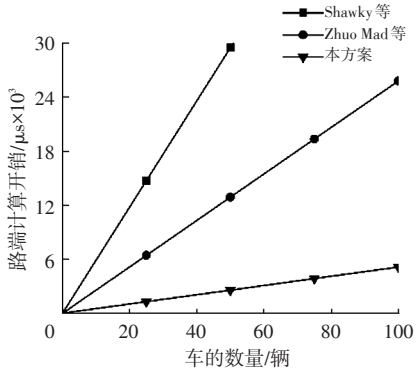


图7　路端计算开销

综上所述，相较于文献[21]、文献[28]，本文方案信令开销减少近50%，相较于文献[28]，车端的计算开销约缩短44%，路端计算开销仅约为该方案的20%，在多车组密钥分发阶段与组密钥更新阶段相较于使用区块链方案更具优势。

6　结束语

本文根据车路所处的环境与通信方式，结合车端与云端的量子随机数发生器和量子密钥，设计了一套适用于车路协同场景的匿名身份认证方案与组密钥分发方案，实现了车辆的隐私保护与组密钥的更新。通过在区块链上部署智能合约，降低了量子密服平台的计算开销，弥补了量子密服平台集中式密钥分发的缺陷，并实现了恶意车辆注销与信息的可追溯。当组成员更新频繁时，可有效减少量子密服平台的计算开销，同时保证

V2V通信的前向安全与后向安全。

参 考 文 献

[1] HAN Y B, SONG W, ZHOU Z B, et al. eCLAS: An Efficient Pairing-Free Certificateless Aggregate Signature for Secure VANET Communication[J]. IEEE Systems Journal, 2021, 16 (1): 1637-1648.

[2] 肖敏, 毛发英, 黄永洪, 等. 基于属性签名的车载网匿名信任管理方案[J]. 网络与信息安全学报, 2023, 9(2): 33-45.
XIAO M, MAO F Y, HUANG Y H, et al. Anonymous Trust Management Scheme of VANET Based on Attribute Signature[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 33-45.

[3] YANG Q, ZHU X Q, WANG X L, et al. A Novel Authentication and Key Agreement Scheme for Internet of Vehicles[J]. Future Generation Computer Systems, 2023, 145: 415-428.

[4] 谢永, 李香, 张松松, 等. 一种可证安全的车联网无证书聚合签名改进方案[J]. 电子与信息学报, 2020, 42(5): 1125-1131.
XIE Y, LI X, ZHANG S S, et al. An Improved Provable Secure Certificateless Aggregation Signature Scheme for Vehicular Ad Hoc NETworks[J]. Journal of Electronics & Information Technology, 2020, 42(5): 1125-1131.

[5] ADHIKARY K, BHUSHAN S, KUMAR S, et al. Hybrid Algorithm to Detect DDoS Attacks in VANETs[J]. Wireless Personal Communications, 2020, 114: 3613-3634.

[6] YU B, XU C Z, XIAO B. Detecting Sybil Attacks in VANETs [J]. Journal of Parallel and Distributed Computing, 2013, 73 (6): 746-756.

[7] AZAM S, BIBI M, RIAZ R, et al. Collaborative Learning Based Sybil Attack Detection in Vehicular Ad- Hoc Networks (VANETs)[J]. Sensors, 2022, 22(18).

[8] 吴武飞, 李仁发, 曾刚, 等. 智能网联车网络安全研究综述[J]. 通信学报, 2020, 41(6): 161-174.
WU W F, LI R F, ZENG G, et al. Survey of the Intelligent and Connected Vehicle Cybersecurity[J]. Journal on Communications, 2020, 41(6): 161-174.

[9] FUEYO M, HERRANZ J. On the Efficiency of Revocation in RSA-Based Anonymous Systems[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1771-1779.

[10] MOHAMED T M, AHMED I Z, SADEK R A. Efficient VANET Safety Message Delivery and Authenticity with Privacy Preservation[J]. PeerJ Computer Science, 2021, 7.

[11] ALI I, CHEN Y, ULLAH N, et al. An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle- to- Vehicle Communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1278-1291.

[12] GUO R, XU L, LI X, et al. An Efficient Certificateless Ring Signcryption Scheme with Conditional Privacy-Preserving in VANETs[J]. Journal of Systems Architecture, 2022, 129.

[13] GOUDARZI S, SOLEYMANI S A, ANISI M H, et al. A Privacy- Preserving Authentication Scheme Based on Elliptic Curve Cryptography and using Quotient Filter in Fog-Enabled VANET[J]. Ad Hoc Networks, 2022, 128.

[14] ZHANG L, KANG B R, DAI F F, et al. Hybrid and Hierarchical Aggregation-Verification Scheme for VANET [J]. IEEE Transactions on Vehicular Technology, 2022, 71 (10): 11189-11200.

[15] WASEF A, LU R X, LIN X D, et al. Complementing Public Key Infrastructure to Secure Vehicular Ad Hoc Networks [Security and Privacy in Emerging Wireless Networks][J]. IEEE Wireless Communications, 2010, 17(5): 22-28.

[16] 石琴, 潘廷亮, 程腾, 等. 面向车云网量子加密通信架构的轻量化身份认证方案研究[J/OL]. 汽车技术(2023-08-22) [2023- 08- 31]. https://doi.org/10.19620/j.cnki.1000-3703.20230069.
SHI Q, PAN T L, CHENG T, et al. Research on Light-weight Authentication Scheme for Quantum Encrypted Communication Architecture in Vehicular Cloud Networks [J/OL]. Automobile Technology (2023-08-22)[2023-08-31]. https://doi.org/10.19620/j.cnki.1000-3703.20230069.

[17] 王梦婷, 王伟, 张强, 等. 一种基于身份的车载网消息认证方法[J]. 西安工程大学学报, 2020, 34(6): 86-91+98.
WANG M T, WANG W, ZHANG Q, et al. An Identity-Based Message Authentication Method in VANET[J]. Journal of Xi'an Polytechnic University, 2020, 34(6): 86-91+98.

[18] 吴静雯, 殷新春, 宁建廷. 车载自组网中可撤销的聚合签名认证方案[J]. 计算机应用, 2022, 42(3): 911-920.
WU J W, YIN X C, NING J T. Revocable Aggregate Signature Authentication Scheme for Vehicular Ad Hoc Networks[J]. Journal of Computer Applications, 2022, 42 (3): 911-920.

[19] JIAO R H, OUYANG H, LIN Y K, et al. A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme[J]. Information, 2019, 10(5).

[20] YILDIZ H, CENK M, ONUR E. PLGAKD: A PUF-Based Lightweight Group Authentication and Key Distribution Protocol[J]. IEEE Internet of Things Journal, 2020, 8(7): 5682-5696.

[21] SHAWKY M A, JABBAR A, USMAN M, et al. Efficient Blockchain- Based Group Key Distribution for Secure Authentication in VANETs[J]. IEEE Networking Letters, 2023, 5(1): 64-68.

[22] PANDA S S, JENA D, MOHANTA B K, et al. Authentication and Key Management in Distributed IoT using Blockchain Technology[J]. IEEE Internet of Things Journal, 2021, 8(16): 12947-12954.

[23] HARN L, HSU C F, LI B. Centralized Group Key Establishment Protocol without a Mutually Trusted Third Party[J]. Mobile Networks and Applications, 2018, 23: 1132-1140.

[24] JAISWAL P, TRIPATHI S. An Authenticated Group Key Transfer Protocol Using Elliptic Curve Cryptography[J]. Peer-to-Peer Networking and Applications, 2017, 10: 857-864.

[25] KAMIL I A, OGUNDOYIN S O. A Lightweight Certificateless Authentication Scheme and Group Key Agreement with Dynamic Updating Mechanism for LTE- V- Based Internet of Vehicles in Smart Cities[J]. Journal of Information Security and Applications, 2021, 63.

[26] TAN H W, ZHENG W Y, GUAN Y G, et al. A Privacy-Preserving Attribute- Based Authenticated Key Management Scheme for Accountable Vehicular Communications[J]. IEEE Transactions on Vehicular Technology, 2022, 72(3): 3622-3635.

[27] CREMERS C J F. Scyther: Semantics and Verification of Security Protocols[D]. Netherlands: Eindhoven University of Technology, 2006.

[28] ZHOU X T, HE D B, KHAN M K, et al. An Efficient Blockchain- Based Conditional Privacy- Preserving Authentication Protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2022, 72(1): 81-92.

（责任编辑　斛　畔）

修改稿收到日期为2023年7月28日。