5G车联网中安全高效的组播服务认证与密钥协商方案

张应辉*① 李国腾① 韩 刚① 曹 进② 郑 东①
①(西安邮电大学网络空间安全学院 西安 710121)
②(西安电子科技大学网络与信息安全学院 西安 710071)

摘 要：5G车联网(5G-V2X)中，内容提供者通过以点对多的传输方式向属于特定区域的一组车辆提供服务消息。针对于车辆获取组播服务遭受的安全威胁与隐私泄露问题，该文提出一种认证和密钥协商方案用于内容提供者与车辆之间的组播服务消息传输。首先，采用无证书聚合签名技术批量验证群组内所有车辆，提高了认证请求的效率。其次，基于多项式密钥管理技术实现安全的密钥协商，使得非法用户或核心网络无法获取共享会话密钥。最后，实现了群组内车辆的动态密钥更新机制，当车辆加入或离开群组时，内容提供者只需要发送1条密钥更新消息即可更新会话密钥。基于形式化验证工具和进一步安全性分析表明，所提方案可以保证匿名性、不可链接性、前向和后向安全性以及抗共谋攻击等安全需求。与现有方案相比，计算效率提高了约34.2%。

关键词：5G车联网；认证；密钥协商；动态群组；组播
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2022)YU-0001-10
DOI: 10.11999/JEIT231118

Secure and Efficient Authentication and Key Agreement Scheme for Multicast Services in 5G Vehicular to Everything

ZHANG Yinghui① LI Guoteng① HAN Gang① CAO Jin② ZHENG Dong①
①(*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121, *China*)
②(*School of Cyber Engineering, Xidian University, Xi'an* 710071, *China*)

Abstract: In 5G Vehicular to Everything (5G-V2X), service messages are provided to a group of vehicles belonging to a specific region by means of point-to-multipoint transmission. To address security threats and privacy leakage, an authentication and key negotiation scheme is proposed for multicast service message transmission between content providers and vehicles. A certificate-less aggregated signature technique is used to batch-verify all vehicles in the group, and improves the efficiency of authentication requests. Secure key negotiation is realized based on the polynomial key management technique, which makes it impossible for illegal users or the core network to obtain the shared session key. Finally, a dynamic key update mechanism for vehicles in the group is implemented, so that when a vehicle joins or leaves the group, the content provider only needs to send a key update message to update the session key. The proposed scheme can guarantee security requirements such as anonymity, unlinkability, forward and backward security, and resistance to conspiracy attacks, as shown by formal verification tools and further security analysis. The computational efficiency is improved by about 34.2% compared to existing schemes.

Key words: 5G Vehicular to Everything (5G-V2X); Authentication; Key agreement; Dynamic group; Multicast

收稿日期：2023-10-17；改回日期：2023-12-22；网络出版：2023-12-27
*通信作者： 张应辉 yhzhaang@163.com
基金项目：国家自然科学基金(62072369, 62072371)，陕西高校青年创新团队基金，陕西省特支计划青年拔尖人才支持计划基金，陕西省重点研发计划 (2021ZDLGY06-02, 2020ZDLGY08-04)，陕西省技术创新引导计划 (2023-YD-CGZH-31)
Foundation Items: The National Natural Science Foundation of China (62072369, 62072371), The Youth Innovation Team of Shaanxi Universities Foundation, The Shaanxi Special Support Program Youth Top-notch Talent Program, The Key Research and Development Program of Shaanxi (2021ZDLGY06-02, 2020ZDLGY08-04), The Technology Innovation Leading Program of Shaanxi (2023-YD-CGZH-31)

1 引言

近年来，随着智能汽车领域的蓬勃发展，车联网(Vehicular-to-Everything, V2X)的概念引起了学术界和工业界越来越多的研究关注。V2X通信指的是车辆可以连接到各种网络实体或设备，可分为车辆到车辆(Vehicle-to-Vehicle, V2V)、车辆到基础设施(Vehicle-to-Infrastructure, V2I)等，可以为车辆用户提供一系列服务，包括互联网接入、舒适服务、视频流和内容共享等[1,2]。

尽管V2X通信拥有巨大潜力，但仍面临许多性能和安全性挑战[3,4]。为解决这些问题，基于蜂窝移动通信网络的蜂窝V2X (Cellular V2X, C-V2X)应运而生。长期演进V2X (Long Term Evolution V2X, LTE-V2X)是第3代合作伙伴项目计划(3rd Generation Partnership Project, 3GPP)在第14版中标准化的第1个C-V2X技术[5]。此外，3GPP已经在第16版中标准化了最新的5G-V2X[1]。但是在第16版中的V2X通信仅支持单播和广播传输，而在面向未来的第17版中正在讨论对5G-V2X中组播传输的支持。其中，广播传输是指在广播覆盖范围中的所有用户设备都可以接收相同的消息，而组播传输中只有经过授权的一组满足特定条件的用户设备(比如组内成员)才可以接收到消息。在车辆获取组播服务的时候，如果1个组播服务报文同时从1个服务提供商发送到特定区域的多辆车辆，则该报文在每条网络链路上只需要传递1次，并且只会在链接分叉时复制[6]。这种机制可以避免相同数据在同一链路上的重复传输，从而有效降低网络资源的消耗[7]。

由于5G-V2X系统具有车辆数量多、机动性强、计算能力有限、车联网设备功耗低、通信信道开放等特点，在5G-V2X网络中的组播服务需要考虑3个重要问题。第一，对于消息来源的可靠性需要进行高效认证；第二，移动车辆的隐私性需要得到保障；最后，当车辆订阅或退订组播服务时需要及时更新会话密钥。组播服务传输目前仍存在许多安全问题，包括相互认证、用户匿名性、不可链接性、抗共谋攻击、完美前向/后向安全性(Perfect Forward/Backward Secrecy, PBS/PFS)、可追溯性、抗重放攻击等。

为了保证消息传输通道的安全与隐私，身份认证和密钥协商(Authentication and Key Agreement, AKA)协议至关重要。目前针对V2X安全获取组播服务的相关研究较少，但已经有一些身份认证和密钥协商方案用来在车辆与网络与第三方实体之间建立会话密钥。Xu等人[8]提出了一种新的V2X组认证和密钥协商方案，海量车辆构建一个群组，与4G核心网实体完成相互认证。然而，由于使用双线性运算，会产生许多计算开销，另外，所有车辆都可获得归属服务器的主密钥，这非常不安全。Dua等人[9]的方案使用椭圆曲线密码学和哈希函数构建，仅需较低的计算和通信开销，但他们的方案需要假设可信的簇头车辆，并且没有考虑密钥更新操作。Islam等人[10]提出了一种基于密码的组密钥生成协议。但是，此方案存在一些弱点。密钥更新过程需要可信中心(Trusted Authority, TA)保持在线并将加密的组密钥通过单播发送给每辆车，效率非常低。Zhang等人[11]提出了一种安全高效的认证和密钥协商协议，该协议车辆和路侧单元(Road Side Unit, RSU)之间协商共享密钥。然而，他们的方案依赖于双线性配对，并且密钥更新机制需要广播所有车辆的公钥。Xu等人[12]提出了一种基于树的组密钥协议，他们提出的方案支持节点的加入和离开。但是，成员加入或离开群组将改变旧二叉树的结构，因此发起人需要计算并向其他成员广播更新的组密钥，这样车辆可能会伪造要广播更新的组密钥。Cui等人[13]提出了一种针对V2X的安全认证方案，每辆车和第三方都需要在注册机构下完成相互认证，然而，每个认证过程都需要注册机构的参与，这可能导致关键节点的拥塞失败。Wei等人[14]提出了一种经过身份验证的密钥协商机制，用于车辆自组织网络中车辆到基础设施和车辆到车辆通信的安全，基于树实现组密钥建立机制。Ma等人[15]基于组播服务模型提出了一种身份认证和数据传输方案。该方案使用双密钥来分别管理认证密钥和数据流量密钥。然而，由于车辆的移动性，随着车辆数量的增加，组播密钥更新将会变得频繁，导致车辆的跟踪和撤销变得复杂，不利于协议扩展。

此外，上面的大多数方案都需要预先设置用于离线认证的密钥。然而，由于车辆资源有限，很多情况下不可能离线存储所有相关的认证密钥，而且在添加新用户的时候，可能会造成信息泄露等问题。当第三方实体想要为车辆提供组播服务时，为了安全起见，需要在线预设车辆密钥。因此本文利用3GPP TS 33.501 Rel-16[16]标准下5G身份认证和密钥协商(5G-AKA)机制实现组播服务的在线注册，并基于此提出一种5G-V2X场景下组播服务认证和密钥协商方案。具体如下：

(1) 验证车辆群组时，采用无证书聚合签名技术批量验证群组中地所有车辆，减少了认证过程中的信令开销。此外，通过分治法快速定位恶意车辆产生的无效签名，提高群组认证效率。

(2) 具有动态更新机制的高效会话密钥分发，认证成功后，只有合法的车辆才能推导出有效的共享会话密钥。会话密钥更新方法只需要在组播服务提供者中进行少量修改，而只要车辆保持有效，其解密信息就保持不变。此种情况下，无需对剩余车辆进行大量计算即可实现快速密钥更新过程。

(3) 采用形式化验证工具Scyther和进一步安全性分析证明了方案的安全特性。效率分析表明，相较于同类方案，本文方案能有效降低计算与通信开销，提高认证和密钥更新效率。

2　系统模型

如图1所示，组播服务模型主要由3个部分组成，即5G网络，车辆(Vehicle)和组播服务提供者(Multicast Service Provider, MSP)。

5G网络由核心网(Core Network, CN)和接入网(Radio Access Networks, RAN)构成。具体而言，CN分为归属网络(Home Network, HN)、服务网络(Server Network, SN)和用户平面功能(User Plane Function, UPF)。其中HN由认证服务器功能(AUthentication Server Function, AUSF)、统一数据组成管理(Unified Data Management, UDM)构成，为车辆提供认证和授权服务。通常密钥生成中心(Key Generation Center, KGC)可以与AUSF集成，生成系统全局参数并提供密钥给参与者。而SN由接入和移动管理功能(Access and Mobility management Function, AMF)以及会话管理功能(Session Management Function, SMF)组成，为车辆提供接入和通信服务。同时，SMF会配置组播业务到UPF的路径信息，将业务数据路由到正确的实体。UPF，为组播服务提供者提供接入5G网络的接口，基于用户平面将组播业务数据进行路由转发。

接入网(RAN)，通过有线链路连接到5G核心网络，并为车辆提供无线覆盖。此外，配备有边缘云数据库的RAN可以存储组播业务数据，并将组播业务数据安全地转发给车辆。

组播服务提供者(MSP)，位于5G核心网络的内部或外部，负责完成车辆访问组播服务地认证。在与请求组播服务的车辆完成认证后，会将相应的组播业务数据安全传输给相应的RAN。

Vehicle，车辆是不可信任的实体，配备有联网设备，通过无线链路连接到RAN。在同一RAN覆盖范围内的车辆可以构成一个组。在与组播服务提供者通信前，所有车辆都需要在5G核心网络进行注册。只有组播服务提供者认证成功地车辆才能获得组播服务。

除了RAN和车辆之间通过无线链路来进行连接，其他实体之间通过有线链路连接，可以直接通过现有的数据报传输层安全机制直接完成相互认证和密钥协商[17]。因此，RAN和5G网络、组播服务提供者之间或者5G网络内部的连接已经预先建立了安全通道。

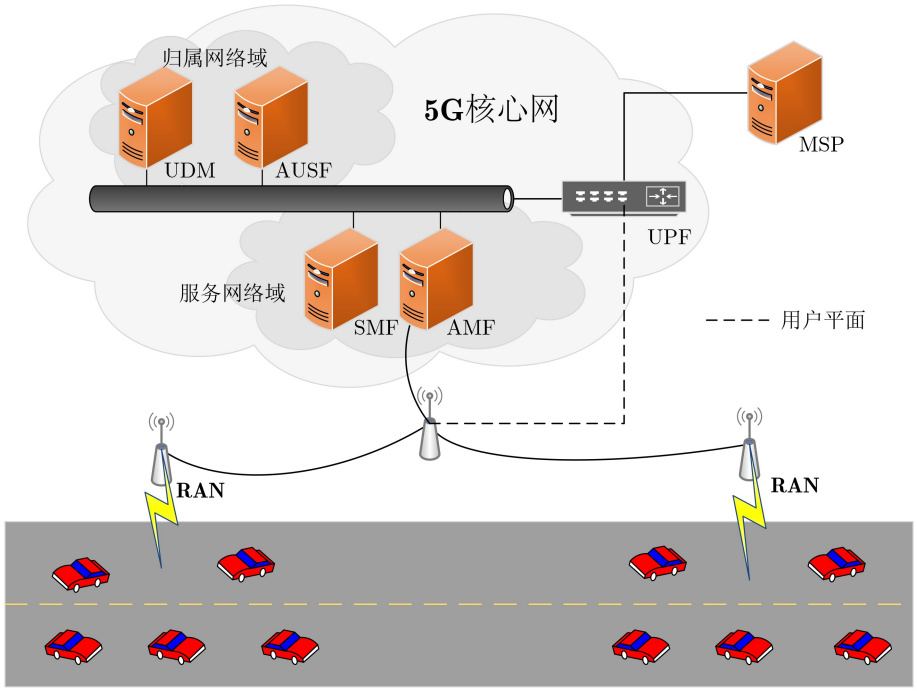

图 1 组播服务模型

3 本文方案

5G-V2X场景下车辆获取组播服务进行身份认证和密钥分发流程包含系统初始化阶段、用户注册阶段、组播服务接入认证阶段、组播服务密钥分发阶段、组会话密钥更新阶段。具体方案描述如下：

3.1 系统初始化阶段

以安全参数k作为输入，AUSF生成两个素数p,q，并计算他们的乘积m。生成阶为q，生成元为P的循环群G。随后选择一个随机数$s\in Z_q^*$作为主密钥，并设置系统公钥为$P_{\text{pub}}=sP$。接下来选择5个哈希函数$H_0:G\times G\to Z_q^*$，$H_1:\{0,1\}^*\times G\times G\to Z_q^*$，$H_2:\{0,1\}^*\times G\times G\times\{0,1\}^*\to Z_q^*$，$H_3:G\to Z_q^*$以及$H_4:\{0,1\}^*\times\{0,1\}^*\times G\to Z_q^*$。最后，AUSF发布系统参数$\text{params}=(q,G,P,P_{\text{pub}},H_1,H_2,H_3,H_4)$，并将主密钥$s$保存到UDM中。

3.2 用户注册阶段

在这个阶段，所有车辆通过RAN漫游到HN域(AUSF/UDM)，并通过5G-AKA协议来完成车辆在线注册，5G-AKA协议执行完后会派生出密钥K_{AMF}。每辆车向HN域提供部分私钥，然后在执行完5G-AKA后使用K_{AMF}向车辆发送另一部分密钥。详情如下：

(1) 车辆V_i生成一个随机数$x_i\in Z_q^*$作为私钥的一部分，并计算对应的部分公钥$X_i=x_iP$。然后V_i向SN发送接入请求消息$\{\text{VID}_i,X_i,\text{ID}_{\text{HN}}\}$，请求消息中包括其真实身份$\text{VID}_i$、部分公钥$X_i$以及HN的身份标识$\text{ID}_{\text{HN}}$。

(2) SN收到请求后，会将认证请求消息转发给HN，并在其中包含自己的身份标识ID_{SN}。

(3) HN收到SN发送的认证请求之后，执行5G-AKA，生成认证向量**AVs**。接下来，HN会生成V_i假名$\text{PID}_i=\text{VID}_i\oplus H_0(sX_i,P_{\text{pub}},t_i)$，其中$t_i$表示假名的有效期。在生成假名后，HN将会选择一个随机数$r_i\in Z_q^*$，并计算$Y_i=r_iP$以及$y_i=r_i+h_is$，其中$h_i=H_1(\text{PID}_i,X_i,Y_i)$。接下来，HN会使用安全通道将认证响应消息$\{\text{PID}_i,Y_i,y_i\}$发送给SN。

(4) 当5G-AKA认证成功后，SN会通过HN派生的会话密钥K_{AMF}将认证响应消息$\{\text{PID}_i,Y_i,y_i\}$发送给车辆V_i。

(5) 在V_i收到认证响应消息后，为了保证响应的正确性，会重新计算$h_i=H_1(\text{PID}_i,X_i,Y_i)$，并通过验证等式$y_iP=Y_i+h_iP_{\text{pub}}$来检查$y_i$的有效性。若等式成立，则将$V_i$的私钥设置为$\text{sk}_i=(x_i,y_i)$，公钥设置为$\text{pk}_i=(X_i,Y_i)$用于后续的过程。

与车辆一样，组播服务提供者可以通过与HN建立的安全通道来获取部分密钥。

(1) 组播服务提供者MSP随机选择一个部分密钥$x_{\text{M}}\in Z_q^*$，计算部分公钥$X_{\text{M}}=x_{\text{M}}P$。然后将身份标识$\text{ID}_{\text{MSP}}$和$X_{\text{M}}$一起提交给HN。

(2) HN选择一个随机数$r_{\text{M}}\in Z_q^*$，计算MSP的部分公钥$Y_{\text{M}}=r_{\text{M}}P$和部分私钥$y_{\text{M}}=r_{\text{M}}+h_{\text{M}}s$，这其中$h_{\text{M}}=H_1(\text{ID}_{\text{MSP}},X_{\text{M}},Y_{\text{M}})$。随后将$\{y_{\text{M}},Y_{\text{M}}\}$通过安全通道安全的发送给MSP。

(3) MSP在收到消息后，会重新计算h_{M}，并验证等式$y_{\text{M}}P=Y_{\text{M}}+h_{\text{M}}P_{\text{pub}}$。若等式成立，则验证成功，将MSP的私钥设置为$\text{sk}_{\text{MSP}}=(x_{\text{M}},y_{\text{M}})$，公钥设置为$\text{pk}_{\text{MSP}}=(X_{\text{M}},Y_{\text{M}})$。

3.3 组播服务接入认证阶段

在此阶段，组播服务提供者MSP首先向RAN发送组播服务通知，同一RAN覆盖范围内且想要订阅特定组播服务的车辆将形成一个RAN组，执行对内容提供者的服务接入认证过程。在接入认证过程中，RAN充当组长。假设一个RAN覆盖的车辆数量为n。

首先，组播服务提供者MSP向RAN发送组播服务通知消息，此消息包含接入组播服务所必须的信息，包括服务提供者的身份ID_{MSP}、其公钥pk_{MSP}等。然后，RAN检查组播服务通知消息的有效性，并广播此消息。

(1) 在收到RAN广播的组播服务通知消息后，每个愿意订阅组播服务的车辆V_i选择一个随机数$a_i\in Z_q^*$，计算$A_i=a_iP$。以及$w_i=H_2(\text{PID}_i,A_i,\text{pk}_i,\text{ID}_{\text{MSP}},T_i)$，其中$T_i$是当前的时间戳。接下来计算$S_i=w_ia_i+y_i$，并设置车辆的签名为$\sigma_i=(S_i,A_i)$。然后将服务接入请求消息$\text{msg}_i=\{\sigma_i,\text{PID}_i,T_i\}$发送给RAN。

(2) 当RAN收到第1个V_i发送的接入认证请求消息后，会等待ΔT以收集组内其他设备的请求消

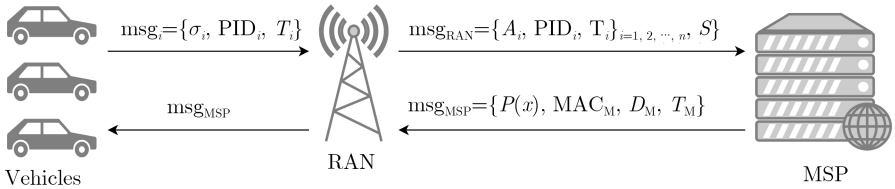

图 2 组播接入认证及密钥分发阶段

息，若在ΔT结束时还没有收集到所有的请求消息，则认证失败。否则，计算

$$S=\sum_{i=1}^{n}S_i \tag{1}$$

然后将组内所有接入认证服务请求消息进行聚合得到$\mathrm{msg}_{\mathrm{RAN}}=\{\{A_i,T_i,\mathrm{PID}_i\}_{i=1}^{n},S\}$，并将$\mathrm{msg}_{\mathrm{RAN}}$发送给UPF, UPF会将$\mathrm{msg}_{\mathrm{RAN}}$转发给MSP。

(3) 当MSP收到RAN发送来的聚合认证请求消息后，首先验证$T_{\mathrm{cur}}-T_i<\Delta T$是否成立，其中$T_{\mathrm{cur}}$为系统当前时间，$\Delta T$为预设的有效时间间隔。若验证失效则拒绝群组接入请求消息。若时间戳在有效范围内，则计算$w_i=H_2(\mathrm{PID}_i,A_i,\mathrm{pk}_i,\mathrm{ID}_{\mathrm{MSP}},T_i)$，并验证等式

$$\mathrm{S.P}=\sum_{i=1}^{n}w_iA_i+\sum_{i=1}^{n}R_i+\sum_{i=1}^{n}h_iP_{\mathrm{pub}} \tag{2}$$

若等式成立，则聚合签名有效，MSP确保接收到的请求消息是有效的，属于合法的车辆V_i。

若等式不成立，基于分治法[18]思想，MSP将组的聚合签名分成两个各包含1/2组成员签名的聚合签名。分别进行验证，若其中一部分失败则说明无效的消息包含在其中，重复此过程，直到找恶意车辆并对合法车辆生成正确的响应。具体如算法1所示。

3.4 会话密钥分发阶段

(1) 在完成组播服务接入认证后，对于所有合法的车辆V_i，MSP选择一个随机数$d_{\mathrm{M}}\in Z_q^*$，并计算$D_{\mathrm{M}}=d_{\mathrm{M}}P$。然后计算$J_i=d_{\mathrm{M}}(X_i+R_i+h_iP_{\mathrm{pub}})$，并将$J_i$存储在数据库中。接着计算$Z_i=H_3(J_i)$。之后，MSP生成一个长度与$Z_i$一样的随机数$Z_{\mathrm{s}}$作为盐值，并选择一个随机数$\varphi\in Z_q^*$作为共享会话密钥，构造一个$n+1$次多项式$P(x)$为

算法 1　聚合签名验证中无效消息查找算法

输入：群组接入请求消息$\mathrm{msg}_{\mathrm{RAN}}=\{\{A_i,T_i,\mathrm{PID}_i\}_{i=1}^{n},S\}$
输出：如果S中有无效请求，则输出无效请求；否则，返回true

```
(1) DetAlg(S):
(2)   if SignatureVerify(S) then
(3)     return true;
(4)   else if Num(S) == 1 then
(5)     return PID_i;
(6)   else
(7)     set S_front = {S_1, S_2,···,S_[n/2]};
(8)     set S_rear = {S_[n/2]+1,S_[n/2]+2,···,S_n};
(9)       DetAlg(S_front);
(10)      DetAlg(S_rear);
(11) end if
```

$$P(x)=\prod_{i=1}^{n+1}(x-Z_i)+\varphi(\mathrm{mod}\ m) \tag{3}$$

随后，MSP计算消息认证码$\mathrm{MAC}_{\mathrm{M}}=H_4(\varphi,\mathrm{ID}_{\mathrm{MSP}},D_{\mathrm{M}},T_{\mathrm{M}})$，其中$T_{\mathrm{M}}$为当前的时间戳。并将组播服务响应消息$\mathrm{msg}_{\mathrm{MSP}}=\{P(x),\mathrm{MAC}_{\mathrm{M}},D_{\mathrm{M}},T_{\mathrm{M}}\}$通过UPF发送给RAN。

(2) 当RAN收到组播服务响应消息后，将其广播给组内的车辆。

(3) 当V_i收到中继设备发送来的组播服务响应消息后，首先验证$T_{\mathrm{cur}}-T_{\mathrm{M}}<\Delta T$是否成立，若验证失败则丢弃此消息，若时间戳仍在有效范围内，则计算$J_i'=(x_i+y_i)D_{\mathrm{M}}$，以及$Z_i'=H_3(J_i')$。并通过多项式$P(x)$计算出$P(Z_i')=\varphi$得到会话密钥。在之后，计算消息认证码$\mathrm{MAC}_{\mathrm{A}}'=H_4(\varphi,\mathrm{ID}_{\mathrm{MSP}},D_{\mathrm{M}},T_{\mathrm{M}})$，最后判断等式

$$\mathrm{MAC}_{\mathrm{A}}=\mathrm{MAC}_{\mathrm{A}}' \tag{4}$$

若等式成立，则验证成功。之后组播服务提供者MSP会使用会话密钥来加密组播服务数据，组内车辆在收到发送来的数据后，使用会话密钥解密得到组播服务数据。

3.5 组会话密钥更新阶段

考虑到用户设备的移动性，为了保证群组会话密钥的前后向安全，需要对组会话密钥进行更新。本文考虑了下面两种场景，具体如下：

(1) 车辆加入。对于新加入组播服务的车辆V_{j}，在认证成功后，MSP会使用哈希函数计算新的会话密钥$\varphi'=H_3(\varphi)$，然后向当前所有合法车辆发送更新消息。在收到更新消息后，由于哈希函数是公开的，且组中所有以前的车辆都知道旧的会话密钥φ，因此所有合法用户车辆$i\in[1,n]$通过$\varphi'=H_3(\varphi)$来获得新的会话密钥。而由于哈希函数的单向性，新用户无法从旧的会话密钥获取新的会话密钥。

(2) 车辆离开。对于已离开组播服务的车辆V_{r}，MSP会从数据库中删除相关的Z_{r}。然后选择一个新的群组会话密钥φ'和新的盐值Z_{s}'，并重新构造多项式$P'(x)$

$$P'(x)=(x-Z_{\mathrm{s}}')\prod_{i=1}^{n-1}(x-Z_i)+\varphi'(\mathrm{mod}\ m) \tag{5}$$

然后，MSP将多项式$P'(x)$分配给留在组中的剩余用户$i\in[1,n]/\{r\}$。此种情况下$P(Z_{\mathrm{r}})\neq\varphi'$，离开组播服务后的车辆无法获取更新后的组会话密钥。而对于组内其他车辆$i\in[1,n]/\{r\}$，可以直接使用当前的Z_i推导出更新的组会话密钥$P(Z_i)=\varphi'$。

4 安全性分析

4.1 正确性分析

组聚合签名验证正确性，通过验证式(5)是否成立来确定车辆签名的合法性，因为

$$\begin{aligned}\mathrm{S.P}&=\sum_{i=1}^{n}(w_ia_i+y_i)P\\&=\sum_{i=1}^{n}w_ia_iP+\sum_{i=1}^{n}y_iP\\&=\sum_{i=1}^{n}w_iA_i+\sum_{i=1}^{n}(r_i+h_is)P\\&=\sum_{i=1}^{n}w_iA_i+\sum_{i=1}^{n}r_iP+\sum_{i=1}^{n}h_isP\\&=\sum_{i=1}^{n}w_iA_i+\sum_{i=1}^{n}R_i+\sum_{i=1}^{n}h_iP_{\mathrm{pub}}\end{aligned}\tag{6}$$

所以，正确性成立。

会话密钥正确性，对于每一台车辆V_i，计算

$$\begin{aligned}Z_i'&=H(J_i')=H_3((x_i+y_i)D_{\mathrm{M}})\\&=H_3(d_{\mathrm{M}}(x_i+r_i+h_is)P)\\&=H_3(d_{\mathrm{M}}(x_iP+r_iP+h_iP_{\mathrm{pub}}))\\&=H_3(d_{\mathrm{M}}(X_i+R_i+h_iP_{\mathrm{pub}}))\end{aligned}\tag{7}$$

然后，将Z_i'带入多项式$P(x)$得到

$$\begin{aligned}\varphi&=P(Z_i')\\&=(Z_i'-Z_i)\prod_{j=1,j\neq i}^{n}(Z_i'-Z_j)+\varphi(\mathrm{mod}\ m)\end{aligned}\tag{8}$$

所以，正确性成立。

4.2 使用Scyther进行安全分析

Scyther是一种协议形式化验证工具，可以自动检测协议是否存在潜在的协议攻击，如重放、反射、中间人攻击等[19]。本文所提出的方案模型中，主要的通信实体是车辆与组播服务提供者，即V_i和MSP。由于5G-AKA的过程已被正式验证，则本文方案的注册阶段可认为是安全的，所以只考虑组播服务认证阶段与会话密钥分发阶段。选择Dolev-Yao模型来验证本文方案的安全性，在该模型中，攻击者可以完全控制网络并进行一系列攻击[20]。

基于Scyther的仿真结果如图3所示。可以看出，本文方案满足了所有Scyther机密性和认证属性，且身份信息和新生成的会话密钥也是保密的。

4.3 其他安全性讨论

本节采用非形式化安全性分析的方式，进一步分析说明本文方案如何满足所有安全属性。

车辆身份认证。本文方案中，5G HN在注册阶段将私钥分配给想要订阅组播服务的合法车辆。在组播服务服务接入认证阶段，当希望订阅特定的组播服务时，每个V_i使用私钥生成服务接入请求消息$\mathrm{msg}_i=\{\sigma_i,\mathrm{PID}_i,T_i\}$并发送给附近的接入网RAN，收到消息后RAN将这些消息聚合成一组服务接入请求消息$\mathrm{msg}_{\mathrm{RAN}}=\{\{A_i,T_i,\mathrm{PID}_i\}_{i=1}^{n},S\}$。然后组播服务提供者通过验证式(2)来检查聚合签名的有效性和完整性，只有验证成功时，这些车辆才能被授权订阅特定的组播服务。而对手在不知道私钥y_i和随机数a_i的情况下，无法构造有效的S_i。此外，组播服务提供者需要根据每个车辆V_i对应的J_i来生成响应值，V_i可以通过式(7)来验证组播服务提供者，只有合法的服务提供者才能提供组播服务。综上，本文方案能够实现车辆的身份认证。

会话密钥分发。本文方案采用基于多项式的密钥管理技术来分发密钥，组播服务提供者MSP通过$J_i=d_{\mathrm{M}}(X_i+R_i+h_iP_{\mathrm{pub}})$计算与车辆的私钥，并通过多项式(3)来计算群组成员与组播服务提供者的共享会话密钥而无需任何加密/解密。

匿名性和不可链接性。本文方案中，车辆的真实身份隐藏在假名中，在车辆向HN注册时，会为其生成伪身份$\mathrm{PID}_i=\mathrm{VID}_i\oplus H_1(sX_i,P_{\mathrm{pub}},t_i)$。若攻击者想要提取车辆的真实身份$\mathrm{VID}_i$，必须计算$sX_i$。除了HN之外，任何攻击者都无法从假名中获取车辆的真实身份。此外，车辆随机选择a_i来生

Claim				Status		Comments
MulticastAuth	Vi	MulticastAuth,Vi2	Secret _Hidden_ 1	Ok	Verified	No attacks.
		MulticastAuth,Vi3	Secret n1	Ok	Verified	No attacks.
		MulticastAuth,Vi4	Secret info	Ok	Verified	No attacks.
		MulticastAuth,Vi5	Secret NH	Ok	Verified	No attacks.
		MulticastAuth,Vi6	Secret n2	Ok	Verified	No attacks.
		MulticastAuth,Vi7	Secret K_VM	Ok	Verified	No attacks.
		MulticastAuth,Vi8	Secret ID	Ok	Verified	No attacks.
		MulticastAuth,Vi9	Alive	Ok	Verified	No attacks.
		MulticastAuth,Vi10	Weakagree	Ok	Verified	No attacks.
		MulticastAuth,Vi11	Niagree	Ok	Verified	No attacks.
		MulticastAuth,Vi12	Nisynch	Ok	Verified	No attacks.
	MSP	MulticastAuth,MSP2	Secret _Hidden_ 2	Ok	Verified	No attacks.
		MulticastAuth,MSP3	Secret ID	Ok	Verified	No attacks.
		MulticastAuth,MSP4	Secret n2	Ok	Verified	No attacks.
		MulticastAuth,MSP5	Secret K_VM	Ok	Verified	No attacks.
		MulticastAuth,MSP6	Secret n1	Ok	Verified	No attacks.
		MulticastAuth,MSP7	Secret info	Ok	Verified	No attacks.
		MulticastAuth,MSP8	Secret NH	Ok	Verified	No attacks.
		MulticastAuth,MSP9	Alive	Ok	Verified	No attacks.
		MulticastAuth,MSP10	Weakagree	Ok	Verified	No attacks.
		MulticastAuth,MSP11	Niagree	Ok	Verified	No attacks.

图 3 Scyther仿真结果

成签名，攻击者无法将两个不同的请求消息链接到同一辆车。因此本文方案支持匿名性和不可链接性。

有条件的可追溯性。出现恶意车辆时，HN可以追踪到恶意车辆的真实身份，通过从其安全数据库中检索PID_i，计算$\mathrm{VID}_i = \mathrm{PID}_i \oplus H_1(sX_i, P_{\mathrm{pub}}, t_i)$。由于$s$是HN生成的私钥。因此，只有HN才能追踪到车辆的真实身份，其他实体或攻击者无法追踪到车辆的真实身份。因此，本文方案支持有条件的可追溯性。

抗重放攻击。本文方案的所有消息传输过程中都使用时间戳，在组播接入认证请求消息中包含时间戳T_i和组播响应消息中包含时间戳T_{M}。通过检查时间戳的有效性，参与认证的实体可以发现消息是否发生了重放。

抗拒绝服务(Denial of Service, DoS)攻击。攻击者可能会冒充合法的车辆向组播服务提供者发送虚假信息来破坏组的验证。本文方案中提供了一种检测算法来检测无效请求，检测算法的概念基于分治法。当一批请求验证失败时，MSP可以将该批次分成两个子批次，然后分别检查每个子批次的有效性，如果某个子批次请求数量只剩下1个，并且该请求依然无效，则MSP可以确定该子批次中的该请求无效。

抗共谋攻击。在最坏的情况下，组内n个成员中的$n-1$个人会合作来获取第n个成员的密钥。共谋成员可以计算多项式

$$G(x) = \prod_{i=1}^{n-1}(x - Z_i)(\mathrm{mod}\ m) \tag{9}$$

接下来，他们会对多项式进行因式分解

$$\begin{aligned} g(x) &= \frac{P(x) - \varphi}{G(x)} = \frac{\prod_{i=1}^{n+1}(x - Z_i)}{\prod_{i=1}^{n-1}(x - Z_i)} \\ &= (x - Z_S)(x - Z_n) \end{aligned} \tag{10}$$

由于$g(x)$是1元2次多项式，且Z_n和$(x - Z_S)$的值并未透漏给组内其他共谋成员，因此若想获得密钥他们必须找到以复合整数m为模的单变量多项式的根。而该多项式的因式分解是未知的，这相当于分解m。因此组内成员的密钥对于组内其他成员的共谋攻击是安全的。

前向和后向安全性。当一个车辆V_j加入组，可以访问新的会话密钥φ'，而$\varphi' = H_3(\varphi)$。因此，由于哈希函数的单向性，V_j无法得到旧的会话密钥。而对于一个离开组的车辆V_a，其无法通过多项式推导出新的会话密钥$P(Z_m) \neq \varphi'$，且对于式(11)，由于两个加盐多项式的存在，使得$\prod_{i=1}^{n}(x - Z_i)$的公共乘数是非线性的，如果车辆V_j计算式(7)，无法求得正确的φ'。综上所述，本文方案提供了前向和后向安全性。

$$\begin{aligned} &P(x) - P'(x) \\ &= \left((x - Z_S)\prod_{i=1}^{n+1}(x - Z_i) + \varphi\right) \\ &\quad - \left((x - Z'_S)\prod_{i=1}^{n}(x - Z_i) + \varphi'\right) \\ &= [(x - Z_S)(x - Z_j) - (x - Z'_S)] \\ &\quad \cdot \prod_{i=1}^{n}(x - Z_i) + (\varphi - \varphi') \end{aligned} \tag{11}$$

为了直观展示本文方案的安全和功能性，进一步将本文方案与现有其他认证方案进行了比较，具体如表1所示。可以看到本文方案在抗共谋攻击、抗DoS攻击等安全性方面具有优势。

5　性能分析

本节将基于安全目标对本文方案的计算开销和通信开销方面与文献[11,14,15]进行比较。假设一个RAN覆盖的车辆数量为n。由于车辆注册仅执行1次，因此只将所提出的方案与其它方案就n辆车的服务认证和密钥分发过程中产生的计算开销和通信开销进行比较。此外，由于车辆的消息必须由RAN(比如基站或RSU)进行转发。因此，这些方案的比较中还需要考虑RAN转发带来的开销。

5.1　计算开销

为了便于本文方案与其他现有相关方案之间的计算开销，定义T_{h}, T_{mul}, T_{par}和$T_{\mathrm{e/d}}$分别表示哈希运算、点乘运算、配对运算和加密/解密运算。本

表 1　安全和功能性比较

方案	双向认证	用户匿名	密钥更新	抗重放攻击	不可链接性	抗Dos攻击	可追溯性	PFS/PBS	抗共谋攻击
文献[11]	√	√	√	√	√	×	√	√	×
文献[14]	√	√	√	√	×	×	√	√	×
文献[15]	√	√	√	√	√	√	×	×	×
本文方案	√	√	√	√	√	√	√	√	√

文仿真环境为Windows 11操作系统，处理器Intel(R) Core(TM) i5-8265U 1.60GHz以及16 GB内存的主机上。使用基于配对的密码学库(Java Pairing Based Cryptography, JPBC)[21]测试同一操作环境下不同操作的计算成本$T_{\mathrm{h}}\approx 0.030$ ms, $T_{\mathrm{mul}}\approx 0.726$ ms, $T_{\mathrm{par}}=5.251$ ms, $T_{\mathrm{e/d}}=1.867$ ms。

表2展示了相关方案和本文方案中车辆与网络实体或第三方的计算成本对比。首先，本文分析上述4种方案的计算开销，在文献[14]提出方案的认证和密钥协商阶段，单个车辆需要执行6次点乘运算、5次哈希运算，这意味着当n辆车同时请求时产生的计算开销为$6nT_{\mathrm{mul}}+5nT_{\mathrm{h}}$。对RSU来说，需要执行2次点乘运算和4次哈希运算，这意味着为$2T_{\mathrm{mul}}+4T_{\mathrm{h}}$。同样的方法可以计算出文献[11,15]方案的计算开销。本文方案在组播服务认证和密钥分发过程中单个车辆需要执行3次点乘运算和3次哈希运算，因此当n辆车同时请求组播服务时，产生的计算开销为$3T_{\mathrm{mul}}+3T_{\mathrm{h}}$，而RAN以及组播服务提供者执行$3n+1$次点乘运算以及$3n$次哈希运算，产生的计算开销为$(3n+1)T_{\mathrm{mul}}+3nT_{\mathrm{h}}$。

图4展示出了这些相关方案针对n辆车的计算开销比较结果。结果表明，计算开销随着车辆的增加而增加。将不同方案之间的计算开销画成曲线图来表示，可以看到，本文方案的曲线最平滑。假设$n=100$，即100辆车同时请求组播服务的情况，文献[15]、文献[11]、文献[14]与本文方案，观察到的总计算时间分别为16.58 s,8.05 s,6.89 s和4.54 s。相比文献[14]，本文方案的计算效率提高了约34.15%。而随着车辆数量增加到1 000，计算效率提高了约34.19%。综上，本文方案计算效率与最优方案[14]相比提高了约34.2%。

5.2 传输开销

由于$\bar{p}$和p的大小分别为32字节(Byte)和20字节，因此群G_1和群G的大小分别为64字节和40字节。本文假设时间戳的大小为4字节，哈希函数的输出值大小是32字节，对称加密/解密的大小为16字节，随机数的大小为16字节，身份标识的大小为16字节。

为比较方便，将所有方案的实体分为车辆和服务提供者(SP)。具体而言，通信开销包括两个方面：将数据从车辆传输到SP(V到SP)和从SP传输到请求车辆(SP到V)所产生的传输开销。

各方案在接入认证和密钥协商阶段的通信比较结果如表3所示。本文方案在接入认证阶段的通信成本略高于文献[11]方案，并且低于其他方案。而在密钥分发阶段，本文方案仅需要广播1次组播服务响应消息，每个车辆均可以自行推导出会话密钥。通过图5可以直观看到，随着用户设备数量的增多，本文的方案在通信成本方面具有优势。

由于本文方案使用基于多项式的密钥管理方案，当车辆加入或离开后，可以通过多项式直接推导出更新后的密钥。文献[14]方案和文献[15]方案在成员变动后需要$o(n)$次密钥更新消息，其中n是组内剩余车辆数量。本文方案在车辆加入后，只需要向组内剩余车辆发送更新消息，组内车辆可以通过哈希函数直接推导出新的会话密钥；车辆离开后，组内剩余车辆可以自行推导出新的会话密钥。

表 2 计算开销

方案	n台车辆	网络实体或第三方
文献[11]	$3nT_{\mathrm{mul}}+9nT_{\mathrm{h}}+nT_{\mathrm{e/d}}$	$(2n+3)T_{\mathrm{mul}}+(13n+4)T_{\mathrm{h}}+nT_{\mathrm{e/d}}$
文献[14]	$6nT_{\mathrm{mul}}+5nT_{\mathrm{h}}$	$3nT_{\mathrm{mul}}+7nT_{\mathrm{h}}$
文献[15]	$3nT_{\mathrm{mul}}+5nT_{\mathrm{h}}+3nT_{\mathrm{e/d}}$	$3nT_{\mathrm{mul}}+5nT_{\mathrm{h}}+3nT_{\mathrm{e/d}}+T_{\mathrm{mul}}$
本文方案	$3nT_{\mathrm{mul}}+3nT_{\mathrm{h}}$	$3nT_{\mathrm{mul}}+3nT_{\mathrm{h}}+T_{\mathrm{mul}}$

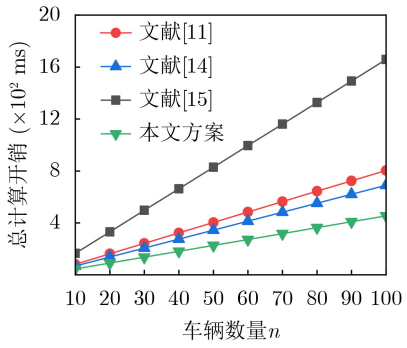

图 4 总计算开销

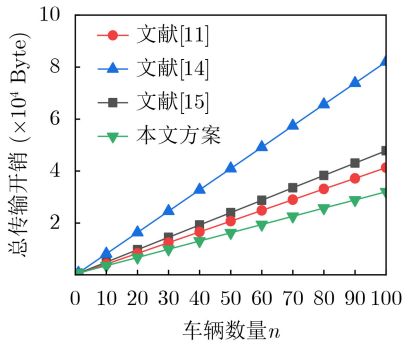

图 5 总传输开销

表 3 传输开销

方案	V到SP	SP到V	总传输开销(Byte)
文献[11]	$112n+132$	$300n$	$412n+132$
文献[14]	$460n$	$360n$	$820n$
文献[15]	$476n+64$	160	$476n+224$
本文方案	$316n+64$	396	$316n+460$

6 结束语

本文针对5G-V2X中的车辆组播服务模型，设计了一种安全高效的组播服务认证方案。方案利用5G-AKA实现车辆部分密钥的在线分发，利用无证书聚合签名技术减轻了组播服务的验证负担，通过多项式密钥管理技术实现了车辆群组共享会话密钥的分发，当车辆订阅或退订组播服务时，实现了会话密钥的动态更新。安全分析表明，本文方案具有匿名性、不可链接性、可追溯性、完美前向/后向安全、抗共谋攻击等安全特性。效率分析表明，本文方案计算效率提升了约34.2%。

参 考 文 献

[1] GARCIA M H C, MOLINA-GALAN A, BOBAN M, *et al*. A tutorial on 5G NR V2X communications[J]. *IEEE Communications Surveys & Tutorials*, 2021, 23(3): 1972–2026. doi: 10.1109/COMST.2021.3057017.

[2] GYAWALI S, XU Shengjie, QIAN Yi, *et al*. Challenges and solutions for cellular based V2X communications[J]. *IEEE Communications Surveys & Tutorials*, 2021, 23(1): 222–255. doi: 10.1109/COMST.2020.3029723.

[3] CHEN Shanzhi, HU Jinling, SHI Yan, *et al*. Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G[J]. *IEEE Communications Standards Magazine*, 2017, 1(2): 70–76. doi: 10.1109/MCOMSTD.2017.1700015.

[4] GANESAN K, LOHR J, MALLICK P B, *et al*. NR sidelink design overview for advanced V2X service[J]. *IEEE Internet of Things Magazine*, 2020, 3(1): 26–30. doi: 10.1109/IOTM.0001.1900071.

[5] SEHLA K, NGUYEN T M T, PUJOLLE G, *et al*. Resource allocation modes in C-V2X: From LTE-V2X to 5G-V2X[J]. *IEEE Internet of Things Journal*, 2022, 9(11): 8291–8314. doi: 10.1109/JIOT.2022.3159591.

[6] SHRIVASTAVA V K, BAEK S, and BAEK Y. 5G evolution for multicast and broadcast services in 3GPP release 17[J]. *IEEE Communications Standards Magazine*, 2022, 6(3): 70–76. doi: 10.1109/MCOMSTD.0001.2100068.

[7] ZHOU Wei, REN Changcheng, MA Chuan, *et al*. Multicast/broadcast service in integrated VANET-cellular heterogeneous wireless networks[C]. 2013 International Conference on Wireless Communications and Signal Processing, Hangzhou, China, 2013: 1–6. doi: 10.1109/WCSP.2013.6677246.

[8] XU Cheng, HUANG Xiaohong, MA Maode, *et al*. GAKAV: Group authentication and key agreement for LTE/LTE-A vehicular networks[C]. 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems, Bangkok, Thailand, 2017: 412–418. doi: 10.1109/HPCC-SmartCity-DSS.2017.54.

[9] DUA A, KUMAR N, DAS A K, *et al*. Secure message communication protocol among vehicles in smart city[J]. *IEEE Transactions on Vehicular Technology*, 2018, 67(5): 4359–4373. doi: 10.1109/TVT.2017.2780183.

[10] ISLAM S K H, OBAIDAT M S, VIJAYAKUMAR P, *et al*. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs[J]. *Future Generation Computer Systems*, 2018, 84: 216–227. doi: 10.1016/j.future.2017.07.002.

[11] ZHANG Jing, ZHONG Hong, CUI Jie, *et al*. SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 1810–1824. doi: 10.1109/TIFS.2020.3044855.

[12] XU Chang, LU Rongxing, WANG Huaxiong, *et al*. TJET: Ternary join-exit-tree based dynamic key management for vehicle platooning[J]. *IEEE Access*, 2017, 5: 26973–26989. doi: 10.1109/ACCESS.2017.2753778.

[13] CUI Jie, ZHANG Xiaoyu, ZHONG Hong, *et al*. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1654–1667. doi: 10.1109/TIFS.2019.2946933.

[14] WEI Lu, CUI Jie, ZHONG Hong, *et al*. Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(9): 3280–3297. doi: 10.1109/TMC.2021.3056712.

[15] MA Ruhui, CAO Jin, ZHANG Yinghui, *et al*. A group-based multicast service authentication and data transmission scheme for 5G-V2X[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(12): 23976–23992. doi: 10.1109/TITS.2022.3197767.

[16] 3GPP. Security architecture and procedures for 5G system (Release16): TS33.501[S]. 2020.

[17] 3GPP. Security architecture and procedures for 5G system (Release 17): TS 33.501[Z]. 2022.

[18] AKTAR S, BÄRTSCHI A, BADAWY A H A, *et al*. A divide-and-conquer approach to Dicke state preparation[J].

IEEE Transactions on Quantum Engineering, 2022, 3: 3101816. doi: 10.1109/TQE.2022.3174547.

[19] CREMERS C J F. The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper[C]. 20th International Conference on Computer Aided Verification, Princeton, USA, 2008: 414–418. doi: 10.1007/978-3-540-70545-1_38.

[20] CERVESATO I. The Dolev-Yao intruder is the most powerful attacker[C]. 16th Annual Symposium on Logic in Computer Science—LICS, Boston, USA, 2001, 1: 1–2.

[21] DE CARO A and IOVINO V. jPBC: Java pairing based cryptography[C]. 2011 IEEE symposium on computers and communications (ISCC), Kerkyra, Greece, 2011: 850–855. doi: 10.1109/ISCC.2011.5983948.

张应辉：男，教授，研究方向为公钥密码学、无线网络安全等.

李国腾：男，硕士生，研究方向为无线网络安全和5G安全.

韩 刚：男，副教授，研究方向为区块链、数据安全共享、访问控制.

曹 进：男，教授，研究方向为应用密码学、天地一体化网络安全等.

郑 东：男，教授，研究方向为编码密码学和网络安全.

责任编辑：余 蓉