研究与开发

一种条件隐私保护的V2G无证书高效聚合签密方案

刘洁，范馨月，何嘉辉
（重庆邮电大学通信与信息工程学院，重庆 400065）

摘　要：针对无证书签名方案不能满足消息机密性，大多数签密方案又存在安全功能不完善、效率低等问题，基于椭圆曲线加密技术提出一种适用于车辆到电网（vehicle-to-grid，V2G）的无证书聚合签密方案。车辆的部分公私钥由自身生成，避免了密钥托管问题。本地聚合器通过聚合解签密，提高了验证效率。通过假名机制提供条件隐私保护，保证合法车辆的匿名性与对恶意车辆的追溯和撤销。采用二元多项式实现车辆假名自主更新。在随机预言机模型下，证明了方案在自适应选择密文攻击下满足不可区分性（IND-CCA2），在自适应选择消息攻击下存在不可伪造性（EUF-CMA）。Scyther形式化分析工具证明了方案的安全性。性能分析表明，与近年签密方案相比，所提方案平均减少了约12.9%的通信开销和84.4%的聚合解签密计算开销，同时具有更高的安全要求。

关键词：无证书；条件隐私保护；二元多项式；聚合签密；可撤销性
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024211

Efficient certificateless aggregate signcryption scheme with conditional privacy protection for V2G networks

LIU Jie, FAN Xinyue, HE Jiahui
School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the issue of message confidentiality in certificateless signature schemes and the shortcomings of most signcryption schemes, such as incomplete security functions and low efficiency, a certificateless aggregate signcryption scheme based on elliptic curve encryption technology was proposed for vehicle-to-grid (V2G) networks. Part of the vehicle's public and private keys were generated by the vehicle itself, avoiding the problem of key escrow. Verification efficiency was improved by the local aggregator through aggregate unsigncryption. Conditional privacy protection was provided by a pseudonym mechanism, ensuring the anonymity of legitimate vehicles and the traceability and revocation of malicious vehicles. Binary polynomials were used to achieve autonomous updating of vehicle pseudonyms. In the random oracle model, the scheme was proven to meet indistinguishability under adaptive chosen ciphertext attacks (IND-CCA2) and existential unforgeability under adaptive chosen message attacks (EUF-CMA). The security of the scheme

收稿日期：2024−06−27；修回日期：2024−09−01
基金项目：国家自然科学基金资助项目（No.62271096）
Foundation Item: The National Natural Science Foundation of China (No.62271096)

was verified by the Scyther formal analysis tool. Performance analysis shows that, compared to recent signcryption schemes, the proposed scheme achieves an average reduction of approximately 12.9% in communication overhead and 84.4% in aggregate unsigncryption computation costs, while also meeting higher security requirements.

Key words: certificateless, conditional privacy protection, binary polynomial, aggregate signcryption, revocability

0　引言

近年来随着可再生低碳设备和车载自组织网络（vehicular Ad Hoc network，VANET）的进步，作为强大储能设备的电动汽车在全球范围内越来越受欢迎。V2G技术能实现电动汽车与电网之间的能量双向流动[1]，助力新一代电网更高效地采用可再生能源，实现削峰填谷，解决电网稳定性问题。但在V2G网络中，由于实体间通信发生在高速开放的无线环境，存在许多潜在安全风险。为实现传输消息的完整性、真实性、不可否认性和数据机密性，已有许多签密方案被提出。Barbosa等[2]结合双线性配对提出了第一个无证书签密方案，但该方案容易受到恶意的密钥生成中心（key generation center，KGC）攻击。Li等[3]提出了一种多接收者的无证书签密方案，该方案可以抵抗恶意KGC攻击，但容易遭受公钥替换攻击。李斌等[4]提出了一种无证书在线/离线签密方案来提高电力系统的鲁棒性，但不满足条件隐私保护。刘德渊等[5]提出了一种基于无证书签密的跨链身份认证方案，但低效的区块生成机制难以满足车联网高实时性要求。

在VANET中，高速的流量会同时产生大量消息，一对一认证会导致接收消息延迟，认证效率低下。无证书聚合签密[6]（certificateless aggregate signcryption，CLASC）是一种混合加密技术，通过将多个签密消息压缩成一个聚合签密消息，结合聚合解签密技术可以提高验证效率，非常适合资源受限的环境。Liu等[7]提出了一种基于雾和双区块链辅助的智能电网CLASC数据共享方案。Yang等[8]提出了一种基于雾计算和云计算的VANET安全预警系统隐私保护聚合认证方案。但这两种方案都是基于双线性配对设计的，由于其计算复杂度高，方案效率低下。Yu等[9]针对资源有限的物联网设备提出了一种基于椭圆曲线的CLASC方案，但该方案容易遭受重放攻击。

条件隐私保护是实现匿名性和可追溯性的有效手段，当车辆有恶意行为时，应揭露其真实身份并撤销其资格。Dai等[10]提出了一种用于车载传感器网络的无配对CLASC方案，但没有提供具体的恶意车辆撤销机制。Dohare等[11]基于双线性配对提出了一种面向云雾中心工业4.0的无证书聚合签密方案，但该方案不满足条件隐私保护，容易泄露用户身份信息。

由上述分析可知，当前大多数基于CLASC的消息验证方案要么缺乏足够的安全性，要么性能不佳，且目前针对V2G网络的CLASC方案很少，因此本文基于二元多项式提出了一种具有条件隐私保护的V2G高效无证书聚合签密方案，具体贡献如下。

（1）本文提出了一种基于椭圆曲线加密和无证书签密的消息签密方案，只有指定的接收者可以验证签密得到秘密信息，保证了消息的完整性、机密性和不可否认性，避免了双线性配对的高计算开销。接收者可以对收到的大量签密聚合后批量验证，提高了解签密的效率。

（2）本文采用假名机制实现条件隐私保护，对有恶意行为的车辆进行身份揭露和撤销，并采用二元多项式技术让合法车辆定期进行假名自主更新，有效减少了KGC的工作负荷，满足匿名性和不可链接性。由于假名具有有效期，假名撤销列表中的假名数量较少，降低了解签密过程中查询撤销列表的计算时延。

（3）基于随机预言机模型下的椭圆曲线离散对数难题证明了本方案的IND-CCA2和EUF-CMA

安全。Scyther形式化证明和安全功能分析表明所提方案可以抵御常见的重放攻击、假冒攻击等网络攻击。性能分析表明本方案具有较低的通信开销和计算开销，尤其在聚合解签密上表现良好。

1 预备知识

1.1 椭圆曲线密码学

Koblitz[12]基于椭圆曲线离散对数问题建立了椭圆曲线密码学（elliptic curve cryptography，ECC），由于其高安全性和轻量性，被广泛应用于加密和认证等安全领域。在有限域F_p上的椭圆曲线E定义为：$y^2=x^3+ax+b \bmod p$，其中$a,b\in F_p$，$4a^3+27b^2\neq 0$，p是一个大素数且为F_p的阶。P为生成元，q阶的椭圆曲线加法群G由曲线上的点和无穷点O构成，具有点的加法和标量乘法运算。

（1）加法：对于$\forall P,Q\in E$，若$P+Q=-R$，则R为P与Q所在直线与E的交点；若$P=-Q$，则有$P+Q=O$。

（2）标量乘法：对于$\forall P\in E$，$m\in Z_q^*$，满足$m\cdot P=P+\cdots+P$。

1.2 二元多项式

二项多项式可用于动态密钥分发和撤销[13]，一个r次二元多项式是有变量M和N的函数，如式（1）所示。

$$F(M,N)=\sum_{i,j=0}^{r} z_{i,j}M^iN^j=$$

$$z_{0,0}+z_{1,0}M+\cdots+z_{r,r}M^rN^r \bmod q \qquad (1)$$

其中，系数$z_{i,j}(0\leqslant i,j\leqslant r)$是从有限域$Z_q^*$中随机选取的，$q$为素数。网络中的每个实体$i$在部署到网络之前都会被分配一个多项式片段$Z_i(N)=F(\mathrm{id}_i,N)$，其中$\mathrm{id}_i\in Z_q^*$代表每个实体$i$的身份。每个实体都会存储该多项式片段$Z_i(N)$的$r$+1个系数$g_j(0\leqslant j\leqslant r)$，$g_j=\sum_{k=0}^{r} z_{kj}\,\mathrm{id}_i^k \bmod q$。

2 系统模型

2.1 系统框架

本文的V2G系统框架主要由电动汽车（electric vehicle，EV）、本地聚合器（local aggregator，LAG）、能源服务提供商（energy service provider，ESP）和密钥生成中心4个实体组成。电动汽车通过无线网络与本地聚合器进行通信，利用V2G网络进行充放电服务。LAG是用于传输消息的本地网关，具有一定的计算存储能力。LAG可以对来自不同EV的签密消息进行解签密，并将验证后的消息发送给ESP。ESP会对收到消息中的服务请求进行响应。KGC是一个可信的实体，负责实体注册、系统初始化和车辆撤销等工作。

2.2 安全威胁

在无证书密码系统中，通常有两类攻击者。第一类攻击者$A1$不知道系统主密钥和车辆的部分私钥，但可以替换车辆的公钥，模拟一个不诚实的用户作为外部攻击者。第二类攻击者$A2$知道系统主密钥和车辆私钥，但无法替换车辆公钥，模拟一个恶意但被动的KGC作为内部攻击者[14]。

CLASC方案要能抵抗安全攻击，在随机预言机模型（random oracle model，ROM）的困难问题假设下，需满足自适应选择消息攻击下的存在不可伪造性（existential unforgeability under chosen message attack，EU-CMA）和自适应选择密文攻击下的不可区分性（indistinguishability under adaptive chosen ciphertext attack，IND-CCA2）。协议的不可伪造性和机密性由敌手A和挑战者C之间进行的2个游戏来说明。敌手A可以在多项式时间内向挑战者C自适应地发起部分私钥查询、公钥查询、公钥替换查询、私钥查询和签密查询。

2.3 困难问题假设

本文提出的V2G无证书聚合签密方案的安全

性依赖于椭圆曲线离散对数计算困难问题，其定义如下。

椭圆曲线离散对数问题（elliptic curve discrete logarithm problem，ECDLP）：已知S和P为椭圆曲线E上的两点，随机数$k\in Z_p^*$，对于$S=k\cdot P$，通过点S和P，计算上很难确定k的值。

3　方案设计

本文所提出的CLASC方案一共包括系统初始化、注册阶段、签密、解签密、聚合解签密、恶意车辆撤销和假名更新7个阶段。系统参数及其定义见表1。

表1　系统参数及其定义

参数	定义
ID_i，ID_j	EV_i和LAG_j的身份标识符
PID_i	EV_i的假名身份
$H(\cdot)$	单向哈希函数
f	部分私钥
SK，PK	完整私钥和完整公钥
T_i，ΔT	当前时间戳和有效期
$F(M,N)$	二元多项式
$Z_i(N)$	二元多项式片段
RL	撤销列表
$\Delta(M)$，$K(M)$	撤销多项式和广播多项式

3.1　系统初始化

输入安全参数λ，KGC产生两个大素数p和q，在椭圆曲线E上生成阶为q，生成元为P的加法循环群G。定义5个单向哈希函数：H_1,H_3:$G\rightarrow Z_q^*$，H_2:$\{0,1\}^*\times G\times G\rightarrow Z_q^*$，$H_4$:$\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\rightarrow Z_q^*$，$H_5$:$\{0,1\}^*\times\{0,1\}^*\times G\rightarrow Z_q^*$。KGC选择一个随机数$s\in Z_q^*$，作为系统主密钥，计算系统公钥$P_{pub}=s\cdot P$，并生成一个$r$阶二元多项式$F(M,N)$，其中$M$和$N$是变量，$r$为撤销车辆的最大数量。KGC公布系统参数$Params=\{p,q,P,G,P_{pub},H_1,H_2,H_3,H_4,H_5\}$。

3.2　注册阶段

车辆在使用V2G网络的服务前都需在KGC进行注册。车辆EV_i将其真实身份$\{ID_i\}$发送给KGC，KGC检查其是否在撤销列表$RL_1=\{ID_1,ID_2,\cdots,ID_n\}$中，若在则拒绝其注册请求，否则，KGC选择一个随机数$x_i\in Z_q^*$，并计算式（2），为隐藏用户身份，KGC计算车辆假名$PID_i=ID_i\oplus H_1(x_i\cdot P_{pub})$，并计算$f_i=x_i+s\cdot h_i$，$h_i$如式（3）所示。

$$X_i=x_i\cdot P \tag{2}$$

$$h_i=H_2(PID_i,X_i,P_{pub}) \tag{3}$$

KGC还为EV_i生成一个多项式片段$Z_i(N)=F(PID_i,N)$，最后KGC将$\{(PID_i,\Delta T_a),X_i,f_i,Z_i(N)\}$通过安全通道发送给$EV_i$，其中$\Delta T_a$是假名$PID_i$的有效期。

车辆EV_i在收到消息$\{(PID_i,\Delta T_a),X_i,f_i,Z_i(N)\}$后，随机选择$r_i\in Z_q^*$作为私钥，并计算式（4）。

$$R_i=r_i\cdot P \tag{4}$$

最后得到其完整私钥$SK_i=\{r_i,f_i\}$，完整公钥$PK_i=\{R_i,X_i\}$。EV_i将$\{(PID_i,\Delta T_a),Z_i(N)\}$存储在其$OBU_i$中。本地聚合器$LAG_j$的注册过程和$EV_i$的注册过程相似，$LAG_j$向KGC发送注册请求后，KGC为其生成$ID_j$，选择随机数为其生成部分密钥对，$LAG_j$再选择随机数生成完整密钥对，其中$SK_j=r_j+f_j$，$PK_j=SK_j\cdot P$。

3.3　签密

当车辆EV_i需要向V2G网络发送消息时会对消息进行签密，如想发起充电预留申请时，会将充电预留消息$m_i\in\{0,1\}^*$生成签密消息后发送给最近的LAG_j。首先EV_i选择一个随机数$y_i\in Z_q^*$，计算$Y_i=y_i\cdot P$，生成当前时间戳$T_{i,1}\in\{0,1\}^*$，并计算$\mu_i=m_i\oplus H_3(y_i\cdot PK_j)$，$h_4=H_4(\mu_i,PID_i,ID_j,T_{i,1})$，$\delta_i=y_i+(f_i+r_i)h_4$，最后生成签密消息$\sigma_i=\{\mu_i,\delta_i,Y_i\}$，并发送密文$\{\sigma_i,T_{i,1},PID_i,PK_i\}$给$LAG_j$。

3.4　解签密

当LAG_j收到EV_i的密文消息时，首先生成当

前时间戳$T_{i,1}^{*}$，计算$|T_{i,1}^{*}-T_{i,1}|\leqslant\Delta T$是否成立，以此确定消息是否在有效期，若消息在有效期则检查假名PID_i是否未过期，且不在假名撤销列表$\mathrm{RL}_2=\{\mathrm{PID}_1,\mathrm{PID}_2,\cdots,\mathrm{PID}_n\}$中，若成立，则验证签密的合法性。当$\mathrm{LAG}_j$验证单个签密消息时，首先计算$h_i'=H_2(\mathrm{PID}_i,X_i,P_{\mathrm{pub}})$，$h_4'=H_4(\mu_i,\mathrm{PID}_i,\mathrm{ID}_j,T_{i,1})$，$\mathrm{LAG}_j$通过验证式（5）确定签密的合法性。

$$\delta_i\cdot P=Y_i+(X_i+h_iP_{\mathrm{pub}}+R_i)h_4 \tag{5}$$

若式（5）成立，LAG_j则接受消息μ_i，并使用私钥通过式（6）对密文μ_i进行解密，当LAG_j得到明文消息m_i后，LAG_j根据m_i向ESP发送消息，ESP会对被预约的充电站进行电力资源调度和充电桩预留。

$$m_i=\mu_i\oplus H_3(Y_i\cdot\mathrm{SK}_j) \tag{6}$$

式（5）正确性证明如下。

$$\delta_i\cdot P=(y_i+(f_i+r_i)h_4)\cdot P=Y_i+(x_i+sh_i)Ph_4+R_ih_4=$$
$$Y_i+(X_i+h_iP_{\mathrm{pub}}+R_i)h_4 \tag{7}$$

式（6）正确性证明如下。

$$m_i=\mu_i\oplus H_3\left(\mathrm{SK}_j\cdot Y_i\right)=$$
$$m_i\oplus H_3\left(y_i\cdot\mathrm{PK}_j\right)\oplus H_3\left(\mathrm{SK}_j\cdot Y_i\right)=$$
$$m_i\oplus H_3(y_i\cdot\mathrm{SK}_j\cdot P)\oplus H_3(\mathrm{SK}_j\cdot Y_i)=m_i \tag{8}$$

3.5 聚合解签密

本协议还可以对签密消息进行聚合解签密，当LAG_j在一定时间内收到n个车辆发送的密文消息$\{(\mu_i,\delta_i,Y_i,T_{i,1},\mathrm{PID}_i,\mathrm{PK}_i)|i=1,\cdots,n\}$时，$\mathrm{LAG}_j$采用可以抵御中间人攻击的小指数测试技术[15]进行聚合签密，即LAG_j随机选择一个非常小的整数l，计算$\delta=\sum_{i=1}^{n}(c_i\cdot\delta_i)$，其中$c_i=\{c_1,c_2,\cdots,c_n\}$，$c_i\in[1,2^l]$，最后得到聚合签密消息$\sigma=\{\mu_1,\cdots,\mu_n,\delta,Y_1,\cdots,Y_n\}$。随后$\mathrm{LAG}_j$通过验证式（9）来聚合解签密：

$$\delta\cdot P=\sum_{i=1}^{n}c_i\cdot Y_i+$$
$$(\sum_{i=1}^{n}c_i\cdot h_i\cdot h_{4,i})\cdot P_{\mathrm{pub}}+\sum_{i=1}^{n}c_i\cdot(R_i+X_i)\cdot h_{4,i} \tag{9}$$

其中，$h_{4,i}=H_4(\mu_i,\mathrm{PID}_i,\mathrm{ID}_j,T_{i,1})$。

若式（9）成立，则证明聚合签密σ有效，输出明文消息$m_i(1\leqslant i\leqslant n)$。若聚合解签密失败，则采用分治法[16]进行无效签密查找，将聚合签密均分成两组，再分别进行验证，对验证失败的部分重复此过程，直至找出所有非法签密。

式（9）的正确性证明如下。

$$\delta\cdot P=\left(\sum_{i=1}^{n}c_i\cdot(y_i+(f_i+r_i)h_{4,i})\right)\cdot P=$$
$$\sum_{i=1}^{n}c_i\cdot y_i\cdot P+\sum_{i=1}^{n}c_i\cdot f_i\cdot h_{4,i}\cdot P+$$
$$\sum_{i=1}^{n}c_i\cdot r_i\cdot h_{4,i}\cdot P=\sum_{i=1}^{n}c_i\cdot Y_i+$$
$$\sum_{i=1}^{n}c_i\cdot(x_i\cdot sh_i)\cdot P+\sum_{i=1}^{n}c_i\cdot h_{4,i}\cdot R_i=$$
$$\sum_{i=1}^{n}c_i\cdot Y_i+\left(\sum_{i=1}^{n}c_i\cdot h_i\cdot h_{4,i}\right)\cdot P_{\mathrm{pub}}+$$
$$\sum_{i=1}^{n}c_i\cdot h_{4,i}\cdot(R_i+X_i) \tag{10}$$

3.6 恶意车辆撤销

为保护用户隐私，车辆使用不同的匿名身份签署相关消息，当车辆存在恶意行为时，应当揭露其真实身份并撤销其身份资格，保证条件隐私保护。对于匿名身份为PID_i的车辆，KGC可以根据其私钥通过式（11）揭露车辆真实身份。

$$\mathrm{ID}_i=\mathrm{PID}_i\oplus H_1\left(s\cdot X_i\right)=\mathrm{ID}_i\oplus H_1\left(x_i\cdot P_{\mathrm{pub}}\right)$$
$$\oplus H_1(s\cdot x_i\cdot P)=\mathrm{ID}_i \tag{11}$$

并将被撤销的车辆真实身份存储在撤销列表$\mathrm{RL}_1=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$中，将其假名身份存储在假名撤销列表$\mathrm{RL}_2=\{\mathrm{PID}_1,\mathrm{PID}_2,\cdots,\mathrm{PID}_n\}$中，$\mathrm{RL}_1$和$\mathrm{RL}_2$都由KGC进行存储，$\mathrm{RL}_2$中的过期假名会被移除，并且KGC会定期广播$\mathrm{RL}_2$给LAG。

3.7 假名更新

为防止车辆长期使用同一假名被链接攻击，

诚实用户必须定期更新其假名。首先KGC选择一个假名更新随机数$t_i \in Z_q^*$，作为假名更新密钥，生成当前时间戳$T_{i,2}$，并计算$\beta_i = t_i \cdot P$，$\omega = H_5(T_{i,2}, \Delta T_a, \beta_i)$。根据已被撤销的车辆假名身份计算撤销多项式$\Delta(M) = (M - \mathrm{PID}_1) \cdots (M - \mathrm{PID}_n)$和广播多项式$K(M) = t_i \Delta(M) + F(M, \omega)$，最后KGC广播消息$\{\beta_i, K(M), T_{i,2}, \Delta T_a\}$给车辆。

当车辆EV_i收到广播消息后，先生成当前时间戳$T_{i,2}^*$并检查$|T_{i,2}^* - T_{i,2}| \leqslant \Delta T$是否成立，若成立则计算$\omega = H_5(T_{i,2}, \Delta T_a, \beta_i)$，$t_i = \dfrac{K(\mathrm{PID}_i) - Z_i(\omega)}{\Delta(\mathrm{PID}_i)}$，其中$Z_i(N) = F(\mathrm{PID}_i, N)$，是车辆在注册阶段从KGC处秘密获得的。随后$\mathrm{EV}_i$利用获得的$t_i$生成新假名，$\mathrm{PID}_i^* = \mathrm{ID}_i \oplus H_1(t_i \cdot P_{\mathrm{pub}})$。若车辆已被撤销，$\Delta(\mathrm{PID}_i) = 0$则不能计算出$t_i$，无法更新其假名。

4　安全分析

4.1　基于ROM的安全证明

本节在ROM中定义了2个游戏，分别针对$A2$下的EUF-CMA和$A1$下的IND-CCA2进行安全性证明。

定理1　假设一个PPT第二类对手$A2$利用ε的优势攻击本文方案。$A2$通过在多项式时间t中最多执行q_{H_i}次H_i询问(i=2,3,4)、q_{SK}次私钥询问、q_{PK}次公钥询问和q_{S}次签密询问后，则挑战者C可以在时间$t' \leqslant 120\,686 q_{H_2} q_{H_3} q_{H_4} t/\varepsilon'$内以不可忽略优势$\varepsilon' \geqslant 10(q_S + 1)(q_{H_2} + q_{H_3} + q_{H_4} + q_{\mathrm{SK}} + q_{\mathrm{PK}} + q_S)/2^{\lambda}$解决ECDLP。

证明：挑战者C是一个ECDLP的破解者，对于给定的一个ECDLP实例$(P, R_i = r_i \cdot P)$，C的目标是求解出r_i。C以挑战身份PID_i^*，与$A2$交互并将响应记录存储到初始值为空的问答列表L中，C将与$A2$进行GM_1。

（1）初始化：C执行系统初始化算法生成系统参数Params和系统主密钥s，并将两者发送给$A2$。

（2）H_2询问：当C收到$A2$关于PID_i的h_i询问时，C检查PID_i是否在列表L_{H_2}中，若存在则C返回h_i给$A2$，否则C选择一个随机数$x_i \in Z_q^*$，计算式（2）和式（3），并将$(\mathrm{PID}_i, X_i, P_{\mathrm{pub}}, h_i)$插入$L_{H_2}$中，最后返回$h_i$给$A2$。

（3）H_3询问：当C收到$A2$关于PID_i的h_3询问时，若列表L_{H_3}中存在PID_i，则C返回h_3给$A2$，否则C选择一个随机数$y_i \in Z_q^*$，计算$h_3 = H_3(y_i \cdot \mathrm{PK}_j)$，并将$(y_i \cdot \mathrm{PK}_j, h_3)$插入$L_{H_3}$中，返回$h_3$给$A2$。

（4）H_4询问：当C接收到$A2$关于PID_i的h_4询问时，C检查列表L_{H_4}中是否包含元组$(\mu_i, \mathrm{PID}_i, \mathrm{ID}_j, T_{i,1}, h_4)$，若存在，$C$则返回$h_4$给$A2$，否则$C$选择随机数$h_4 \in Z_q^*$，插入$(\mu_i, \mathrm{PID}_i, \mathrm{ID}_j, T_{i,1}, h_4)$到$L_{H_4}$中，并将$h_4$返回给$A2$。

（5）私钥询问：$A2$请求关于PID_i的私钥询问。首先C检查式（12）是否成立，若成立，此次查询终止。

$$\mathrm{PID}_i = \mathrm{PID}_i^* \tag{12}$$

否则C会检查列表L_{SK}中是否包含元组$(r_i, f_i, \mathrm{PID}_i)$，若存在，则$C$返回$(r_i, f_i)$给$A2$，否则$C$选择两个随机数$r_i, f_i \in Z_q^*$，将$(r_i, f_i, \mathrm{PID}_i)$插入$L_{\mathrm{SK}}$中后返回$(r_i, f_i)$给$A2$。

（6）公钥询问：当$A2$向C询问PID_i的公钥时，C首先判断式（12）是否成立，若成立，则C随机选择$r_i, x_i \in Z_q^*$，计算式（4）和式（2），将$(\mathrm{PID}_i, X_i, R_i)$返回给$A2$，并用其更新列表$L_{\mathrm{PK}}$。若不成立，则$C$检查$\{\mathrm{PID}_i, \mathrm{PK}_i\}$是否在$L_{\mathrm{PK}}$中，若在则将$\mathrm{PK}_i$返回给$A2$；否则$C$执行私钥询问得到$r_i$和$f_i$，执行$H_2$询问得到$h_i$，计算式（4）和式（13）。

$$X_i = f_i \cdot P - h_i \cdot P_{\mathrm{pub}} \tag{13}$$

最后C将(X_i, R_i)返回给$A2$，并把$(X_i, R_i, \mathrm{PID}_i)$添加到列表$L_{\mathrm{PK}}$中。

（7）签密询问：当$A2$向C提交发送方为PID_i、接收方为ID_j的消息m_i的签密询问时，C首先判断式（12）是否成立，若不成立，则C执行

签密算法生成签密，因为C知道私钥SK_i。若成立，则C执行私钥询问得到f_i和r_i，并随机选择$y_i \in Z_q^*$，计算$Y_i=y_i \cdot P$，μ_i、h_4和δ_i的计算同签密算法。最后返回签密$\sigma_i=\{\mu_i,\delta_i,Y_i\}$给$A2$，并将其添加到签密列表$L_S$中。

（8）伪造：最后$A2$为PID_i和ID_j提供了一个有效签密$\sigma_i'=\{\mu_i,\delta_i',Y_i\}$且满足$\delta_i' \cdot P=Y_i+X_i+h_iP_{pub}+R_ih_4'$。根据分叉引理[17]，$A2$可以找到另一个有效签密$\sigma_i^*=\{\mu_i,\delta_i^*,Y_i\}$且满足$\delta_i^* \cdot P=Y_i+X_i+h_iP_{pub}+R_ih_4^*$，因此式（14）成立。

$$\delta_i' \cdot P-\delta_i^* \cdot P=\left(Y_i+\left(X_i+h_iP_{pub}+R_i\right)h_4'\right)-\left(Y_i+\left(X_i+h_iP_{pub}+R_i\right)h_4^*\right)\left(\delta_i'-\delta_i^*\right) \cdot P=\left(X_i+h_iP_{pub}+R_i\right)\left(h_4'-h_4^*\right)\frac{\left(\delta_i'-\delta_i^*\right)}{\left(h_4'-h_4^*\right)} \cdot P=\left(x_i+sh_i+r_i\right) \cdot P$$

$$\left(\frac{(\delta_i'-\delta_i^*)}{(h_4'-h_4^*)}-x_i-sh_i\right) \cdot P=r_i \cdot P \qquad (14)$$

所以$A2$将$\left(\frac{(\delta_i'-\delta_i^*)}{(h_4'-h_4^*)}-x_i-sh_i\right)$作为以优势$\varepsilon'$攻破ECDLP的解，而ECDLP在多项式时间内无法解决，因此本方案对ROM中的第二类攻击者$A2$的自适应选择消息攻击具有不可伪造性。

定理2 假设一个PPT第一类对手$A1$利用ε的优势攻击本文方案。$A1$通过在多项式时间t中执行最多q_{H_i}次H_i询问$(i=2,3,4)$、q_{SK}次私钥询问、q_{PSK}次部分私钥询问、q_{PK}次公钥询问和q_{UNS}次解签密询问后，则挑战者C可以以不可忽略的优势$\varepsilon' \geqslant \varepsilon\left(1-\frac{1}{q_{H_2}}\right)^{q_{PSK}+q_{SK}}\left(1-\frac{q_{UNS}}{2^{\lambda}}\right)$解决椭圆曲线离散对数问题。

证明：C是一个ECDLP的破解者，对于给定的一个ECDLP问题实例$(P,Y_i=y_iP)$，C的目标是求解出y_i。C以ID_j^*作为挑战身份，与$A1$交互将响应记录存储到初始值为空的问答列表L中，C将与$A1$进行GM_2。

（1）初始化：挑战者C执行系统初始化算法，为$A1$生成系统参数Params，并秘密保留系统主密钥s。

（2）部分私钥询问：$A1$为PID_i执行该询问。首先C检查式（12）是否成立，若成立，此次查询终止，否则C检查部分私钥列表L_{PSK}中是否包含元组(X_i,PID_i,f_i)，若存在，则C返回$\{X_i,f_i\}$给$A1$，若不存在则C执行一次H_2询问得到h_i，然后选择一个随机数$f_i \in Z_q^*$，计算式（13），最后C将(X_i,PID_i,h_i)存储到L_{H_2}中，将(X_i,PID_i,f_i)插入L_{PSK}中，并将$\{X_i,f_i\}$返回给$A1$。

（3）公钥替换询问：$A1$随机选择一个新公钥$PK_i^*=(R_i^*,X_i^*)$，并将(PID_i,PK_i^*)发送给C。当C收到$A1$对PID_i的公钥替换询问时，C将L_{PK}更新为(R_i^*,X_i^*,PID_i)。

阶段1 敌手$A1$可以自适应地完成和定理1中相同的公钥询问、哈希询问和私钥询问。在本阶段，$A1$不对接收方ID_j进行私钥询问、部分私钥询问和公钥替换询问。

（1）解签密询问：$A1$对发送方PID_i和接收方ID_j执行解签密$\sigma_i=\{\mu_i,\delta_i,Y_i\}$询问，$C$检查$ID_j \neq ID_j^*$是否成立，若成立，则$C$获取接收方的私钥$SK_j$来解签密，否则$C$执行以下步骤。

①C选择列表L_{SK}中的第一个元素作为私钥SK_j。

②C通过计算$m_i'=\mu_i \oplus H_3(SK_j \cdot Y_i)$得到消息$m_i'$，并查询列表$L_{H_2}$和$L_{H_4}$得到关于$\{PID_i,ID_j,m_i'\}$的$h_i$和$h_4$。然后$C$验证式（5）是否成立，若成立，则$C$将$m_i'$返回给$A1$，否则$C$依次从$L_{SK}$中选择另一元素作为$SK_j$，并重复此步骤，当列表$L_{SK}$中没有元素使式（5）成立时，则$C$输出错误符号$\perp$给$A1$。在所有解签密询问中拒绝有效密文的概率小于$q_{UNS}/2^{\lambda}$。

（2）挑战：当阶段1结束后，$A1$为选中的挑战

者 ID'_j 选择两条长度相同的消息 m_0 和 m_1。若 $ID'_j \neq ID^*_j$，则 C 停止应答。否则 C 选择两个随机值 $\gamma \in \{0,1\}$，$y_i \in Z^*_q$，并计算 $Y'_i = y_i \cdot P$，$\mu'_i = m'_\gamma \oplus H_3(y_i \cdot PK_j)$，$h'_4 = H_4(\mu'_i, PID'_i, ID'_j, T'_{i,1})$，$\delta'_i = y_i + (f_i + r_i)h'_4$，最后 C 将签密 $\sigma'_i = \{\mu'_i, \delta'_i, Y'_i\}$ 返回给 $A1$。

阶段 2　$A1$ 执行与阶段 1 相同的询问，但 $A1$ 不能对 σ'_i 进行解签密询问。

猜测：$A1$ 输出预测值 γ'。若 $A1$ 可以解决 ECDLP，那 $A1$ 可以从 $Y'_i = y_i \cdot P$ 中得到 y_i，因此根据 $m'_\gamma = \mu'_i \oplus H_3(y_i \cdot PK_j)$，$A1$ 可以通过对 H_3 进行 $y_i \cdot PK_j$ 询问，执行异或操作得到消息 m'_γ。

由上分析可知，在解签密阶段，拒绝有效密文的概率小于 $q_{UNS}/2^\lambda$，在部分私钥询问和私钥询问中，游戏不终止的概率最大为 $\left(1-\frac{1}{q_{H_2}}\right)^{q_{PSK}+q_{SK}}$，因此 $A1$ 解决 ECDLP 具有的优势为 $\varepsilon' \geqslant \varepsilon\left(1-\frac{1}{q_{H_2}}\right)^{q_{PSK}+q_{SK}}\left(1-\frac{q_{UNS}}{2^\lambda}\right)$。可知本方案对 ROM 中的第一类攻击者 $A1$ 的自适应选择密文攻击满足不可区分性。

4.2　基于 scyther 的安全分析

为证明本方案对各种可能的攻击都是安全的，采用 scyther(v1.1.3)形式化安全分析工具[18]在 Dolev-Yao 攻击者模型下对本签密方案进行安全分析，指定 EV 和 LAG 作为方案安全验证的角色。Dolev-Yao 攻击者模型中的攻击者 A 具有通过公共通道获取、窃听、修改、删除或重发实体间传输的消息和进行假冒攻击等安全攻击的能力。scyther 分析结果如图 1 所示，在通信过程中没有检测到任何潜在攻击，本文方案满足 scyther 的安全属性且秘密参数如用户私钥是保密的。

5　性能分析

本节将对本文方案进行计算开销、通信开销及安全功能分析，并与最近提出的无证书聚合签密方案文献[8,11]进行对比。

5.1　计算开销

设置一个 80 位安全级别的双线性配对 e: $G_1 \times G_1 \to G_2$ 和一个加法循环群为 G 的 q 阶椭圆曲线 E:

Scyther results : verify

Claim				Status		Comments
V2GCLAS	EV	V2GCLAS,EV1	Niagree	Ok	Verified	No attacks.
		V2GCLAS,EV2	Nisynch	Ok	Verified	No attacks.
		V2GCLAS,EV3	Alive	Ok	Verified	No attacks.
		V2GCLAS,EV4	Weakagree	Ok	Verified	No attacks.
		V2GCLAS,EV5	Secret ri	Ok	Verified	No attacks.
		V2GCLAS,EV6	Secret add(xi,multiply(s,H2(XOR(IDi,H1(fECM(xi,Ppu...	Ok	Verified	No attacks.
	LAG	V2GCLAS,LAG1	Niagree	Ok	Verified	No attacks.
		V2GCLAS,LAG2	Nisynch	Ok	Verified	No attacks.
		V2GCLAS,LAG3	Alive	Ok	Verified	No attacks.
		V2GCLAS,LAG4	Weakagree	Ok	Verified	No attacks.
		V2GCLAS,LAG5	Secret add(rj,fj)	Ok	Verified	No attacks.

Done.

图 1　scyther 分析结果

$y^2=x^3+ax+b \bmod p$，其中 $a,b\in Z_q^*$，p、q 是两个大素数。本文使用一台配置为 Intel(R) Core(TM) i7-8850U CPU，8.0 G RAM 的计算机在 MIRACL 库中对各种加密原语进行运算，密码学操作符号定义及执行时间见表 2，其中单向哈希、异或和 G_2 中的乘法操作处理时间可忽略不计。

表 2　密码学操作符号定义及执行时间

运算操作	定义	执行时间/ms
T_{BP}	双线性映射	4.211 0
T_{MTP}	映射到点哈希函数	4.406 1
T_{BPM}	双线性映射点乘运算	1.819 2
T_{BPA}	双线性映射点加运算	0.096 4
T_{ECM}	椭圆曲线点乘运算	0.522 4
T_{ECA}	椭圆曲线点加运算	0.002 1
T_M	小指数测试技术乘法运算	0.027 8
T_E	模幂运算	0.027 1

本文方案签密需两次椭圆曲线点乘操作，耗时为 $2T_{ECM}$=1.044 8 ms，解签密需 4 次点乘操作和 3 次点加操作，耗时为 $4T_{ECM}+3T_{ECA}$=2.095 9 ms，聚合解签密需 $2n$+3 次点乘操作、$3n$ 次点加操作和 $2n$ 次小指数测试技术乘法操作，耗时为 $(2n+3)T_{ECM}+3nT_{ECA}+2nT_M$=1.055 3$n$+1.040 6 ms。其他方案的计算开销同理，计算开销对比见表 3。签密与解签密计算开销对比如图 2 所示，本文方案具有最低的计算开销，文献[9]和文献[10]在签密生成上比本文方案多使用一次椭圆曲线点乘操作，虽然在解签密上和本文方案计算成本相近，聚合解签密计算开销比较如图 3 所示，当签密数量大于 1 条时，本文所提方案具有最低的计算时延，且随着签密数量增加，本文方案的性能优势更加明显。而文献[8]和文献[11]由于使用了双线性配对技术和 Map-to-Point 哈希操作，计算开销远高于其他方案。

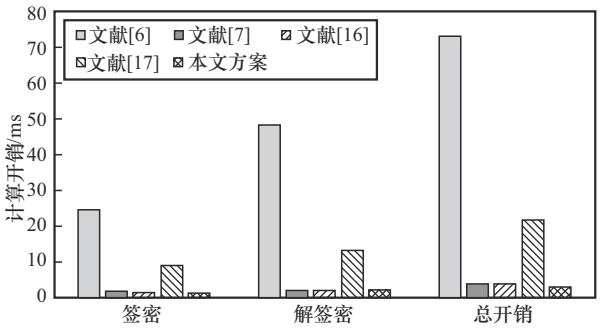

图 2　签密与解签密计算开销对比

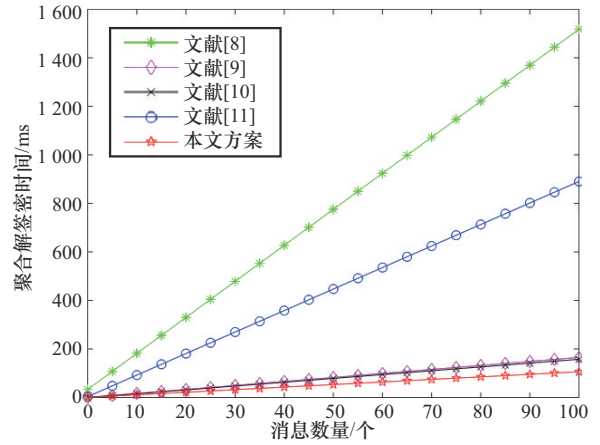

图 3　聚合解签密计算开销比较

5.2　通信开销

为满足 80 位安全级别，设置双线性配对的 p 为 64 byte，ECC 的 p 为 20 byte，因此 G_1 中的元素为 64×2=128 byte，G 中的元素为 20×2=40 byte，Z_q^* 中元素、身份标识符 ID、时间戳 T 和消息 M 的大小分别为 20 byte、20 byte、4 byte 和 100 byte。

在通信开销分析中，主要考虑签密生成后广

表 3　计算开销对比

方案	签密/ms	解签密/ms	聚合解签密/ms
文献[8]	$6T_{BPM}+4T_{BPA}+3T_{MTP}$=24.519 1	$5T_{BP}+3T_{BPM}+5T_{MTP}+T_{BPA}$=48.639 5	$5T_{BP}+3nT_{BPM}+(2n+3)T_{MTP}+(6n-5)T_{BPA}$=14.846 4$n$+33.792 8
文献[9]	$3T_{ECM}+2T_{ECA}$=1.571 4	$4T_{ECM}+3T_{ECA}$=2.095 9	$(3n+1)T_{ECM}+(4n-1)T_{ECA}$= 1.651 2$n$+0.520 3
文献[10]	$3T_{ECM}+T_{ECA}$=1.569 3	$4T_{ECM}+2T_{ECA}$=2.093 8	$(3n+1)T_{ECM}+(3n-1)T_{ECA}$=1.573 5$n$+0.520 3
文献[11]	T_E+2T_{MTP}=8.839 3	$T_{BP}+2T_E+2T_{MTP}$=13.077 4	$T_{BP}+2n(T_E+T_{MTP})$ = 8.866 4n+4.211 0
本文方案	$2T_{ECM}$=1.044 8	$4T_{ECM}+3T_{ECA}$=2.095 9	$(2n+2)T_{ECM}+(3n-2)T_{ECA}+3nT_M$= 1.055 3$n$+1.040 6

播的密文消息，本文方案广播的密文消息为$\{\sigma_i=\{\mu_i,\delta_i,Y_i\},T_{i,1},\mathrm{PID}_i,\mathrm{PK}_i=\{R_i,X_i\}\}$，其中$\{Y_i,R_i,X_i\}\in G$，$T_{i,1}\in T$，$\mu_i\in M$，$\{\delta_i,\mathrm{PID}_i\}\in Z_q^*$，因此本文的通信开销为$2|Z_q^*|+3|G|+|T|+|M|=2\times20+3\times40+4+100=264$ byte。其余方案的通信开销计算同理，通信开销对比见表4。文献[9]和文献[10]均采用椭圆曲线加密技术对消息进行签密，文献[9]密文消息长度小于本文方案，但由于密文消息中未引入时间戳，难以抵抗重放攻击。文献[10]和本文方案通信开销一样，但其聚合解签密效率及安全功能均不如本文方案。本文通信开销低于使用双线性配对的文献[8]和文献[11]，因为ECC中的元素是基于域F_q定义的，大小为$O(\log q)$，而双线性配对中的元素是在扩展域F_{q^k}上定义的，元素大小为$O(k\log q)$。因此，在相同安全级别下，基于ECC的协议比基于配对的协议元素更小。

表4　通信开销对比

方案	传输消息	通信开销/byte
文献[8]	$3\|G_1\|+\|M\|+\|\mathrm{ID}\|$	500
文献[9]	$\|G\|+\|M\|+\|Z_q^*\|+\|\mathrm{ID}\|$	180
文献[10]	$3\|G\|+\|M\|+\|Z_q^*\|+\|\mathrm{ID}\|+\|T\|$	264
文献[11]	$\|G_1\|+2\|Z_q^*\|+\|M\|$	268
本文方案	$2\|Z_q^*\|+3\|G\|+\|T\|+\|M\|$	264

5.3　安全功能

将本文方案与其他无证书聚合签密方案的安全性和功能进行比较，安全功能对比见表5。本文方案传输的密文中包含时间戳$T_{i,1}$，可抵抗重放攻击。车辆使用假名身份PID_i发送密文消息，满足条件隐私保护，且KGC可以利用私钥揭露恶意车辆的真实身份，并将其假名和真实ID_i加入撤销列表RL中，以撤销其资格。文献[8]不满足不可否认性，且消息中未采用时间戳而易遭受重放攻击，文献[11]虽提出了将时间戳和用户ID共同引入作为公钥，让KGC可以刷新签密密钥来防止用户撤销，但它和文献[9]方案均不满足条件隐私保护，用户使用真实身份进行消息传输，存在隐私泄露风险。文献[10]虽满足条件隐私保护，但没有提供具体的用户撤销机制，且车辆要维护自己的假名池，增加了额外的资源开销。因此本文方案在安全功能上具有一定优势。

6　结束语

针对V2G网络中实体间在公开通道频繁通信带来的隐私和安全问题，本文提出一种具有条件隐私保护的V2G无证书聚合签密方案，实现消息批量验证，提高认证效率。采用无证书签密和椭圆曲线技术，避免了证书管理和密钥托管问题。采用二元多项式实现车辆假名定期自主更新，并提供对恶意车辆的撤销功能。基于ROM证明了方案具有IND-CCA2和EUF-CMA安全性。Scyther形式化分析证明了协议满足不可链接性、抗重放攻击等安全需求。性能分析表明本方案具有较小的计算和通信开销，适用于资源有限的V2G网络。

表5　安全功能对比

安全功能	文献[8]	文献[9]	文献[10]	文献[11]	本文方案
消息认证和完整性	√	√	√	√	√
消息机密性	√	√	√	√	√
不可否认性	×	√	√	√	√
条件隐私保护	√	×	√	×	√
不可链接性	√	√	√	√	√
假冒攻击	√	√	√	√	√
重放攻击	×	×	√	√	√
用户撤销	×	×	×	√	√

参考文献：

[1] MWASILU F, JUSTO J J, KIM E K, et al. Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration[J]. Renewable and Sustainable Energy Reviews, 2014(34): 501-516.

[2] BARBOSA M, FARSHIM P. Certificateless signcryption[C]// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 369-372.

[3] LI H X, WU C H, PANG L J. Completely anonymous certificateless multi-receiver signcryption scheme with sender traceability[J]. Journal of Information Security and Applications, 2022(71): 103384.

[4] 李斌, 吴坡, 王丹, 等. 一种适用于电力终端设备的无证书在线/离线签密方案[J]. 计算机工程, 2023, 49(12): 146-151, 160.
LI B, WU P, WANG D, et al. A certificateless online/offline signcryption scheme for power terminal equipment[J]. Computer Engineering, 2023,49(12): 146-151, 160.

[5] 刘德渊, 张金全, 张鑫, 等. 基于无证书签密的跨链身份认证方案[J]. 计算机应用, 2024. doi: 10.11772/j.issn.1001-9081.2023121824.
LIU D Y, ZHANG J Q, ZHANG X, et al. Cross-chain identity authentication scheme based on certificate-less signcryption[J]. Journal of Computer Applications. 2024. doi: 10.11772/j.issn.1001-9081.2023121824.

[6] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 452-473.

[7] LIU S H, CHEN L Q, CHEN L Q, et al. Integrated and accountable data sharing for smart grids with fog and dual-blockchain assistance[J]. IEEE Transactions on Industrial Informatics, 2023, 20(3): 4940-4952.

[8] YANG Y F, ZHANG L, ZHAO Y L, et al. Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet[J]. IEEE Transactions on Information Forensics and Security, 2022(17): 317-331.

[9] YU H F, REN R T. Certificateless elliptic curve aggregate signcryption scheme[J]. IEEE Systems Journal, 2022, 16(2): 2347-2354.

[10] DAI C, XU Z W. Pairing-free certificateless aggregate signcryption scheme for vehicular sensor networks[J]. IEEE Internet of Things Journal, 2023, 10(6): 5063-5072.

[11] DOHARE I, SINGH K, AHMADIAN A, et al. Certificateless aggregated signcryption scheme(CLASS) for cloud-fog centric industry 4.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6349-6357.

[12] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[13] WANG Y P, WANG X F, DAI H N, et al. A data reporting protocol with revocable anonymous authentication for edge-assisted intelligent transport systems[J]. IEEE Transactions on Industrial Informatics, 2023,19(6): 7835-7847.

[14] WU G, ZHANG F T, SHEN L M, et al. Certificateless aggregate signature scheme secures against fully chosen-key attacks[J]. Information Sciences, 2020(514): 288-301.

[15] ZHONG H, CHEN L, CUI J, et al. Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular Ad Hoc networks[J]. IEEE Internet of Things Journal, 2022, 9(11): 8485-8497.

[16] 张应辉, 李国腾, 韩刚, 等. 5G车联网中安全高效的组播服务认证与密钥协商方案[J]. 电子与信息学报, 2024, 46(2): 1-10.
ZHANG Y H, LI G T, HAN G, et al. Secure and efficient authentication and key agreement scheme for multicast services in 5G vehicular to everything[J]. Journal of Electronics&Information Technology. 2024, 46(2): 1-10.

[17] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000(13): 361-396.

[18] CREMERS C J F. The scyther tool: verification, falsification, and analysis of security protocols: tool paper[C]//Proceedings of the International Conference on Computer Aided Verification. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 414-418.

[作者简介]

刘洁（1999– ），女，重庆邮电大学通信与信息工程学院硕士生，主要研究方向为车联网隐私保护和认证协议。

范馨月（1979– ），女，重庆邮电大学通信与信息工程学院副教授，主要研究方向为网络信息安全、信号处理。

何嘉辉（1999– ），男，重庆邮电大学通信与信息工程学院硕士生，主要研究方向为车联网隐私保护。