



## 基于身份聚合签名的车载自组网消息认证方案

杨小东,裴喜祯,安发英,李 婷,王彩芬

(西北师范大学 计算机科学与工程学院,兰州 730070)

**摘 要:** 车载自组网(VANET)能提高智能交通系统的安全性和道路通行效率,然而网络通信环境的开放性使其容易遭受攻击进而引发各种安全问题。针对 VANET 中的隐私泄露和签名验证效率较低等问题,结合基于身份的密码体制和聚合签名技术,设计一个面向 VANET 的消息认证方案,将多个消息的认证聚合为一个短签名,车辆只需对聚合后的签名进行验证,即可快速判断所有签名的有效性。分析结果表明,在随机预言模型下,该方案的安全性规约于计算 Diffie-Hellman 困难问题,且能有效缩短车辆对通信消息的认证响应时间。

**关键词:** 车载自组网;聚合签名;基于身份的签名;消息认证;可证明安全性

开放科学(资源服务)标志码(OSID):



**中文引用格式:** 杨小东,裴喜祯,安发英,等. 基于身份聚合签名的车载自组网消息认证方案[J]. 计算机工程,2020,46(2):170-174,182.

**英文引用格式:** YANG Xiaodong, PEI Xizhen, AN Faying, et al. Message authentication scheme for vehicular ad hoc network using identity-based aggregate signature[J]. Computer Engineering, 2020, 46(2): 170-174, 182.

### Message Authentication Scheme for Vehicular Ad Hoc Network Using Identity-based Aggregate Signature

YANG Xiaodong, PEI Xizhen, AN Faying, LI Ting, WANG Caifen

(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

**【Abstract】** Vehicular Ad Hoc Network(VANET) can improve security of intelligent transportation systems and traffic efficiency, but an open network communication environment makes the system vulnerable to attacks, causing various security issues. To address privacy disclosure and inefficient signature verification in VANET, this paper proposes a message authentication scheme for VANET. The scheme integrates an identity-based cryptosystem with aggregate signatures, so as to aggregating authentication of multiple messages into a short signature. Thus vehicles can rapidly assert the validity of all signatures by verifying only aggregated signatures. Analysis results show that under the random prediction model, the security of the proposed scheme can be reduced to the calculation of the difficult Diffie-Hellman problem, and it can efficiently reduce the authentication response time of vehicles to communication messages.

**【Key words】** Vehicular Ad Hoc Network(VANET); aggregate signature; identity-based signature; message authentication; provable security

DOI:10.19678/j.issn.1000-3428.0054961

## 0 概述

车载自组网(Vehicular Ad Hoc Network, VANET)是由车辆行驶信息构成的交互网络(包括车辆位置、车速和路线等)。车辆利用摄像头、传感器或全球定位系统等装置完成各种信息的采集,并通过互联网

和计算机技术将所采集的信息传输到附近的车辆或交通管理中心等机构。交通管理中心收到传输来的消息后,对其进行分析和处理,可以有效解决交通拥堵等问题<sup>[1]</sup>。此外,车载自组网能提供综合的智能交通服务<sup>[2]</sup>。然而,车载自组网面临诸多安全问题<sup>[3]</sup>。在隐私保护和提高计算效率等需求下,利用

**基金项目:** 国家自然科学基金(61662069);中国博士后科学基金(2017M610817);兰州市科技计划项目(2013-4-22);西北师范大学青年教师科研能力提升计划项目(WNU-LKQN-14-7)。

**作者简介:** 杨小东(1981—),男,副教授、博士、博士后,主研方向为代理重签名、云计算安全;裴喜祯、安发英、李 婷,硕士研究生;王彩芬,教授、博士。

收稿日期:2019-05-20

修回日期:2019-06-27

E-mail: y200888@163.com

密码学技术设计安全高效的消息认证方案是当前车载自组网领域的研究热点之一。

针对传统密码体制的密钥管理复杂等问题,文献[4]提出将身份信息作为公钥的基于身份的密码体制。文献[5]提出方案将多个消息的签名压缩成一个短签名,验证者只需对聚合后的签名进行验证,便可快速判断所有签名的有效性。随后,研究人员相继提出聚合签名方案<sup>[6-8]</sup>。文献[7]设计一个基于身份的聚合签名方案,具有较高的签名验证效率和较长的签名长度。文献[8-9]提出具有固定双线性对运算的基于身份的聚合签名方案,其存在签名长度随签名人数的增加而增长的问题。文献[10]设计一个高效的基于身份的聚合签名方案,由于该方案中的签名可以被伪造,因此安全性较低。文献[11]提出一个签名长度固定的聚合签名方案,其在签名开始前需要预先确定所有参与签名人的集合,不适用于动态车载自组网。文献[12]构造一个面向车联网的聚合签名方案,但签名验证需要大量的双线性对操作。文献[13]提出一个适用于智能电网的基于身份的聚合签名方案,解决了智能电网中存在的隐私泄露问题,但其计算效率和通信效率均较低。文献[14]提出一种新的聚合签名方案,但其无法抵抗联合攻击<sup>[15]</sup>。文献[16]设计一种适用于车载自组织网的聚合签名方案,但其无法抵抗伪造攻击。针对现有方案存在证书管理开销过大、签名验证效率过低等问题<sup>[17-19]</sup>,本文利用基于身份的密码体制和聚合签名技术,构造一个新的车载自组网消息认证方案。

## 1 预备知识

### 1.1 双线性映射

设  $q$  是一个大素数,  $G_1$  和  $G_2$  是阶为  $q$  的两个循环群,  $g$  为  $G_1$  的生成元,  $e: G_1 \times G_1 \rightarrow G_2$  表示一个双线性映射,且具有以下特性:

- 1) 双线性: 对于任意  $a, b \in \mathbb{Z}_q^*$ , 存在  $e(g^a, g^b) = e(g, g)^{ab}$ 。
- 2) 非退化性:  $e(g, g) \neq 1$ 。
- 3) 可计算性: 对于任意  $g_1, g_2 \in G_1$ , 存在一个有效的算法计算  $e(g_1, g_2)$ 。

### 1.2 困难性问题

**定义 1** (计算 Diffie-Hellman 问题)  $G_1$  是阶为素数  $q$  的循环群,  $g$  为  $G_1$  的生成元,  $a, b \in \mathbb{Z}_q^*$ , 给定  $(g, g^a, g^b) \in G_1^3$ , 计算  $g^{ab} \in G_1$  是困难的。

**定义 2** 若对于任意敌手 Adversary, 在多项式时间  $t$  内攻破群  $G_1$  上的 CDH 问题的概率小于  $\varepsilon$ , 则群  $G_1$  上的  $(t, \varepsilon)$ -CDH 假设成立。

## 2 基于身份聚合签名的 VANET 消息认证方案

### 2.1 系统模型

可信的私钥生成中心 (Private Key Generator, PKG)、车辆单元 (On Board Unit, OBU) 和路边单元 (Road Side Unit, RSU) 3 个实体构成本文方案的系统模型 (见图 1)。PKG 主要负责为车辆分发私钥, 同时对于发布虚假消息的车辆, PKG 可以追查其真实身份, 以便对其作出具体的惩罚。OBU 可以利用 DSRC 技术, 完成与 RSU 或其他 OBU 之间的无线通信。RSU 主要为安装在路边的基础设施 (如电线杆等实体), 负责验证车辆单元发送的通信消息的签名以及聚合多个消息的签名等。

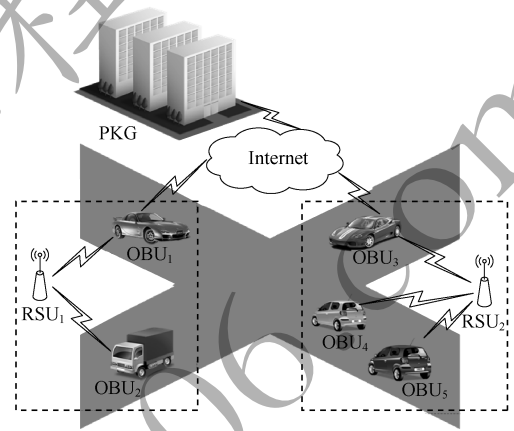


图1 系统模型

Fig. 1 System model

### 2.2 方案描述

基于身份聚合签名的 VANET 消息认证方案具体描述如下:

1) 系统初始化。PKG 首先选择两个阶为素数  $q$  的循环群  $G_1$  和  $G_2$ , 然后随机选择一个  $G_1$  的生成元  $g$ 、一个双线性映射  $e: G_1 \times G_1 \rightarrow G_2$ 、两个安全的 Hash 函数  $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$  和  $H_2: \{0, 1\}^* \rightarrow G_1$ 。PKG 随机选择  $s \in \mathbb{Z}_q^*$  作为主密钥, 计算  $P_{pub} = g^s \in G_1$ , 并公开系统参数  $params = \{\lambda, G_1, G_2, e, q, g, P_{pub}, H_1, H_2\}$ 。

2) 私钥提取。对于车辆单元  $OBU_i (i = 1, 2, \dots, n)$  的身份  $ID_i$ , PKG 确认身份信息  $ID_i$  的合法性后, 计算  $d_{ID_i} = H_1(ID_i, s) + s$ , 并通过安全信道将私钥  $d_{ID_i}$  发送给车辆单元  $OBU_i$ 。

3) 签名。对于消息  $m_i$ , 车辆单元  $OBU_i$  利用私钥  $d_{ID_i}$  进行如下操作:

- (1) 计算  $Q_{ID_i} = g^{d_{ID_i}}$  和  $h_i = H_2(m_i, ID_i, T_i, Q_{ID_i})$ , 其中  $T_i$  为当前时间戳;
- (2) 计算  $S_i = h_i^{d_{ID_i}}$ , 则消息  $m_i$  的签名为  $\delta_i = (S_i, Q_{ID_i})$ ;
- (3) 输出一个关于  $m_i$  和  $T_i$  的签名  $\delta_i = (S_i, Q_{ID_i})$ 。

4) 签名验证。路边单元 RSU 在当前时间  $T'$  收到  $OBU_i$  发送的关于消息  $m_i$  和时间戳  $T_i$  的签名  $\delta_i =$

$(S_i, Q_{ID_i})$  后, 若  $T' - T_i > \tau$ , 则拒绝验证, 其中  $\tau$  表示规定时间差; 否则, RSU 计算  $h_i = H_2(m_i, ID_i, T_i, Q_{ID_i})$ 。若等式  $e(S_i, g) = e(h_i, Q_{ID_i})$  成立, 则接受  $(S_i, Q_{ID_i})$  是一个合法的签名。

5) 聚合签名。对于  $n$  个车辆节点  $OBU_i$  产生的签名  $\delta_i = (S_i, Q_{ID_i})$ , RSU 计算  $\delta = \prod_{i=1}^n S_i$ , 并广播  $n$  个关于消息  $m_i$  和时间戳  $T_i$  的聚合签名  $(\delta, Q_{ID_1}, Q_{ID_2}, \dots, Q_{ID_n})$  给附近的车辆。

6) 聚合签名验证。车辆节点计算  $h_i = H_2(m_i, ID_i, T_i, Q_{ID_i})$ , 若等式  $e(\delta, g) = \prod_{i=1}^n e(h_i, Q_{ID_i})$  成立, 则接受 RSU 广播的  $n$  个通信消息  $m_i$ 。

### 3 安全性分析

下文通过定理 1 证明 2.2 节提出方案的安全性可归约到 CDH 问题的困难性。

**定理 1** 假定存在一个攻击者 Adversary 发起关于  $H_1$  预言机、 $H_2$  预言机、私钥提取预言机和签名预言机的询问次数分别为  $q_{H_1}$ 、 $q_{H_2}$ 、 $q_E$  和  $q_s$ , 询问的时间分别为  $t_{H_1}$ 、 $t_{H_2}$ 、 $t_E$  和  $t_s$ 。如果 Adversary 在时间  $t$  内以不可忽略的优势  $\varepsilon$  攻破本文方案, 则存在一个挑战者 Challenger 在时间  $t' < t + (q_E t_E + q_s t_s) + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$  内以  $\varepsilon' \geq (\varepsilon - \frac{1}{2^k})(1 - \frac{1}{q_{H_1}})(1 - \frac{1}{q_E})(1 - \frac{1}{q_s})$  的优势解决 CDH 问题。

**证明** 假定 Challenger 获得一个 CDH 困难实例  $(g, g^m, g^n) \in G_1^3$ , 其中  $n, m \in Z_q^*$  是未知的随机数, Challenger 的目标是计算  $g^{mn}$ 。Challenger 运行系统初始化算法, 公布系统参数  $\text{params} = \{\lambda, G_1, G_2, e, q, g, P_{\text{pub}}, H_1, H_2\}$ , 保存系统主密钥  $s$ , 并将系统参数  $\text{params}$  发送给攻击者 Adversary。攻击者 Adversary 向挑战者 Challenger 适应性执行以下随机预言机询问, 并用  $ID^*$  表示目标用户的身份。

1)  $H_1$  询问。当 Adversary 给 Challenger 发送一个身份  $ID_i$  时, 如果在列表  $\text{ListH}_1$  中存在  $(ID_i, a_i)$ , 则 Challenger 将  $a_i$  返回给 Adversary; 否则 Challenger 进行如下操作:

(1) 当  $ID_i = ID^*$  时, Challenger 终止询问, 并输出“FAILURE”(该事件发生用  $E_{\text{event1}}$  表示)。

(2) 当  $ID_i \neq ID^*$  时, Challenger 随机选择  $a_i \in Z_q^*$  发送给 Adversary, 并在列表  $\text{ListH}_1$  中增加记录  $(ID_i, a_i)$ 。

2) 私钥提取询问。当 Adversary 向 Challenger 提交一个身份  $ID_i$  并对其进行私钥提取询问时, Challenger 查询列表  $\text{ListE}(ID_i, d_{ID_i})$ , 如果在列表  $\text{ListE}$  中有对于身份  $ID_i$  的私钥, 则发送给 Adversary; 否则 Challenger 进行如下操作:

(1) 当  $ID_i = ID^*$  时, Challenger 终止询问, 并输出“FAILURE”(该事件发生用  $E_{\text{event2}}$  表示)。

(2) 当  $ID_i \neq ID^*$  时, Challenger 从列表  $\text{ListH}_1$  中获取  $(ID_i, a_i)$ , 并计算  $d_{ID_i} = a_i + s$ , 此时  $P_{\text{pub}} = g^s$ ; 然后将  $(ID_i, d_{ID_i})$  增加到列表  $\text{ListE}$  中, 发送私钥  $d_{ID_i}$  给 Adversary。

3)  $H_2$  询问。当 Adversary 询问关于身份  $ID_i$  的  $H_2$  哈希值时, 如果列表  $\text{ListH}_2$  中存在  $(ID_i, m_i, T_i, Q_i, h_i)$ , 则 Challenger 发送  $h_i$  给 Adversary; 否则 Challenger 执行如下操作:

(1) 当  $ID_i = ID^*$  时, Challenger 设置  $Q^* = g^n$  和  $h_i = H_2(ID_i, m_{ID_i}, T_i, Q_{ID_i}) = g^m$ , 然后将  $g^m$  发送给 Adversary, 并在列表  $\text{ListH}_2$  中增加  $(ID_i, m_{ID_i}, T_i, g^n, g^m)$ 。

(2) 当  $ID_i \neq ID^*$  时, Challenger 在列表  $\text{ListE}$  中提取  $(ID_i, d_{ID_i})$ , 计算  $Q_i = g^{d_{ID_i}}$ ; 随机选取  $b_i \in Z_q^*$ , 计算  $g^{b_i}$  作为  $h_i = H_2(ID_i, m_{ID_i}, T_i, Q_i)$  的值发送给 Adversary, 同时将  $(m_{ID_i}, ID_i, T_i, Q_i, g^{b_i})$  增加到列表  $\text{ListH}_2$  中。

4) 签名询问。当 Adversary 向 Challenger 询问关于消息  $m_{ID_i}$  和身份  $ID_i$  的签名时, Challenger 先从  $\text{ListH}_2$  提取  $ID_i$  对应的哈希值  $h_i$ , 然后进行以下操作:

(1) 当  $ID_i = ID^*$  时, Challenger 终止询问, 输出“FAILURE”(该事件发生用  $E_{\text{event3}}$  表示)。

(2) 当  $ID_i \neq ID^*$  时, Challenger 从列表  $\text{ListE}$  中获得  $(ID_i, d_{ID_i})$ , 然后计算  $S = h_i^{d_{ID_i}}$ , 并将  $S$  作为  $m_{ID_i}$  的签名返回给 Adversary。

最后, Adversary 输出一个关于消息/身份  $(m_1^*, ID_1^*)$  的有效签名  $\delta^*$ 。若  $ID_1^* \neq ID^*$ , 则输出“FAILURE”; 否则假设  $ID_1^* = ID^*$ , Challenger 从列表  $\text{ListH}_2$  中获得值  $Q^* = g^n$  和  $h_1^* = g^m$ 。由于对于消息  $(m_1^*, m_2^*, \dots, m_n^*)$  的聚合签名  $\delta^*$  是合法的, 因此有  $e(\delta^*, g) = \prod_{i=1}^n e(h_i^*, Q_i^*)$ , 即  $e(\delta^*, g) = e(h_1^*, Q^*) \prod_{i=2}^n e(h_i^*, Q_i^*) = e(g^m, g^n) \prod_{i=2}^n e(h_i^*, Q_i^*) = e(g^m, g^n) \prod_{i=2}^n e(h_i^*, g^{d_{ID_i}}) = e(g^m, g^n) \prod_{i=2}^n e(h_i^{*d_{ID_i}}, g)$ , 得到  $g^{mn} = \delta^* - \prod_{i=2}^n h_i^{*d_{ID_i}}$ 。因此, Challenger 输出  $g^{mn}$  的值作为 CDH 实例的解答。

下文分析 Challenger 成功解决 CDH 问题实例的时间和优势:

1) 对于  $H_1$  和  $H_2$  询问的回答是在  $Z_q^*$  内均匀分布的, 并且该回答也是有效的。

2) 只有当 3 个事件  $E_{\text{event1}}$ 、 $E_{\text{event2}}$  和  $E_{\text{event3}}$  都不发生时, Challenger 才能完成整个询问, 进而解决 CDH 问题实例。

事件  $E_{\text{event1}}$ 、 $E_{\text{event2}}$  和  $E_{\text{event3}}$  都不发生的概率为:

$$\Pr(\neg E_{\text{event1}} \wedge \neg E_{\text{event2}} \wedge \neg E_{\text{event3}}) = \left(1 - \frac{1}{q_{H_1}}\right) \left(1 - \frac{1}{q_E}\right) \left(1 - \frac{1}{q_S}\right).$$

当 Adversary 未询问  $H_2$  却伪造了一个有效的签名时,此事件发生的概率为  $\frac{1}{2^k}$ ,因此 Challenger 在整个

CDH 问题实例中的优势为  $\varepsilon' \geq \left(\varepsilon - \frac{1}{2^k}\right) \left(1 - \frac{1}{q_{H_1}}\right) \left(1 - \frac{1}{q_E}\right) \left(1 - \frac{1}{q_S}\right)$ ,运行时间为  $t' < t + (q_E t_E + q_S t_S) + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$ 。

#### 4 性能分析

本文方案与文献[12-13]方案都利用了基于身份的聚合签名技术,下文对这 3 个方案的通信开销和计算开销进行对比分析。

##### 4.1 通信开销

通信开销主要集中在私钥提取、签名和聚合签名阶段。将本文方案与文献[12-13]方案在私钥提取阶段、签名阶段和聚合签名阶段的通信开销进行对比分析。为便于比较,假设 3 个方案都选取阶为同一个素数  $q$  的群  $G_1$  和  $G_2$ 。在文献[13]方案中,私钥提取阶段需要的通信开销为  $(n+2)G_1 + G_T$ ;签名阶段对  $n$  个消息进行加密需要的通信开销是  $2nG_1$ ,对  $n$  个密文进行签名需要的通信开销是  $nG_1$ ,所以在签名阶段总的通信开销是  $3nG_1$ ;聚合阶段聚合密文需要的通信开销是  $2G_1$ ,同时对聚合密文进行签名需要的通信开销是  $2G_1$ ,所以在聚合阶段总的通信开销是  $4G_1$ 。在文献[12]方案中,私钥提取阶段需要的通信开销是  $2nG_1$ ,签名阶段需要的通信开销是  $2nG_1$ ,聚合阶段需要的通信开销是  $2G_1$ 。在本文方案中,私钥提取阶段

需要的通信开销是  $nG_1$ ,签名阶段需要的通信开销是  $2nG_1$ ,聚合阶段需要的通信开销是  $G_1$ 。各方案的通信开销对比结果如表 1 所示。由此可知,本文方案优化了私钥提取、签名和聚合签名阶段的算法,有效降低了通信开销。

表 1 基于身份的聚合签名方案通信开销比较

Table 1 Comparison of communication costs of identity-based aggregate signature schemes

方案	私钥提取阶段	签名阶段	聚合签名阶段
文献[12]方案	$2nG_1$	$2nG_1$	$2G_1$
文献[13]方案	$(n+2)G_1 + G_T$	$3nG_1$	$4G_1$
本文方案	$nG_1$	$2nG_1$	$G_1$

##### 4.2 计算开销

本文方案、文献[12-13]方案的计算开销比较结果如表 2 所示,其中,Exp 表示 1 次幂运算,Mul 表示 1 次乘法运算、Add 表示 1 次加法运算、H 表示 1 次哈希运算、P 表示 1 次双线性配对运算, $n$  表示车辆数量。

由表 2 可知,在文献[12]方案中,签名阶段执行  $4n$  次乘法运算,签名验证阶段执行  $3n$  次双线性配对运算和  $n$  次乘法运算,聚合签名验证阶段执行  $(n+2)$  次双线性配对运算、 $(n-1)$  次乘法运算和加法运算;在文献[13]方案中,签名阶段执行  $4(n+1)$  次幂运算和  $2(n+1)$  次乘法运算,签名验证阶段执行  $(3n+3)$  次双线性配对运算,聚合签名验证阶段执行  $3n$  次双线性配对运算。但在本文方案中,签名阶段执行  $2n$  次幂运算,签名验证阶段执行  $2n$  次双线性配对运算,聚合签名验证阶段执行  $(n+1)$  次双线性配对运算。因此,本文方案具有较低的签名验证开销和聚合签名验证开销,可以在较短的时间内验证通信消息的有效性。

表 2 基于身份的聚合签名方案计算开销比较

Table 2 Comparison of computational costs of identity-based aggregate signature schemes

方案	私钥提取阶段	签名阶段	签名验证阶段	聚合签名阶段	聚合签名验证阶段
文献[12]方案	$(2n+1)\text{Mul} + 2n\text{H}$	$(4\text{Mul} + 2\text{H} + 2\text{Add})n$	$(3\text{P} + \text{Mul} + \text{Add})n$	$2(n-1)\text{Add}$	$(n+2)\text{P} + (n-1)(\text{Mul} + \text{Add})$
文献[13]方案	$(3+n)\text{Exp} + (2+n)\text{H} + \text{P}$	$(4\text{Exp} + 2\text{Mul} + \text{H})(n+1)$	$(3n+3)\text{P}$	$2(n-1)\text{Mul}$	$3n\text{P}$
本文方案	$\text{Mul} + (\text{H} + \text{Add})n$	$(2\text{Exp} + \text{H})n$	$(\text{H} + 2\text{P})n$	$(n-1)\text{Mul}$	$(n+1)\text{P}$

#### 5 实验结果与分析

实验环境:CPU 为 Intel Core i7-5500U,内存为 4 GB。基于版本号为 0.4.7 的 PBC 库,对本文方案和文献[12-13]方案进行仿真实验。

##### 5.1 签名验证的计算开销

图 2 展示了 RSU 在仿真实验中执行签名验证

所需的计算开销。仿真实验模拟了从 10 辆 ~ 100 辆车辆生成消息后,RSU 执行签名验证所需的计算开销。3 个方案随着车辆数量的增加,对多个消息进行签名验证所需的时间也逐渐增多。然而,相比文献[12-13]方案,本文方案在签名验证阶段计算开销最小。

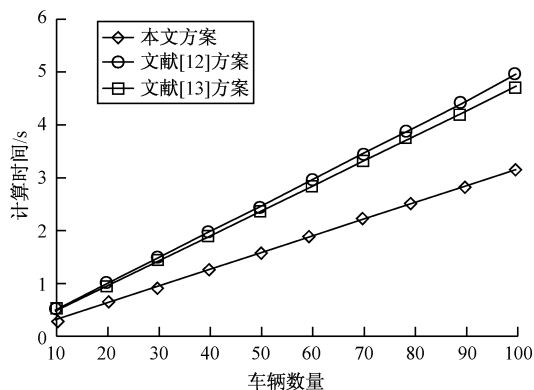


图2 签名验证过程中计算时间与车辆数量的关系

Fig. 2 Relationship between the calculation time and the number of vehicles during signature verification

## 5.2 聚合签名验证的计算开销

图3展示了RSU在仿真实验中执行聚合签名验证所需的计算开销。仿真实验模拟了从10辆~100辆车生成消息后的聚合签名验证所需的计算开销。由图3可知,本文方案在聚合签名验证阶段具有更高的计算效率。

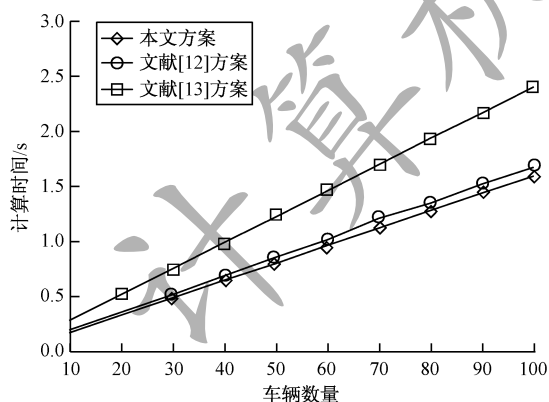


图3 聚合签名验证过程中计算时间与车辆数量的关系

Fig. 3 Relationship between the calculation time and the number of vehicles during aggregate signature verification

## 6 结束语

为降低车辆对通信消息的认证响应时间,本文设计一个基于身份聚合签名的车载自组网消息认证方案,将多个消息的多个签名聚合为一个短签名进行验证。分析结果表明,本文方案具有较高的安全性及较低的通信与计算开销。然而,由于本文方案的安全性规约于计算 Diffie-Hellman 困难问题,无法抵抗量子计算攻击,因此下一步将设计基于格困难问题的车载自组网消息认证方案。

### 参考文献

[1] QIU Tie, CHEN Ning, LI Keqiu, et al. Heterogeneous ad hoc networks: architectures, advances and challenges [J]. Ad Hoc Networks, 2017, 55: 143-152.

[2] ZHANG F S, LIU H, LEUNG Y W, et al. CBS: community-based bus system as routing backbone for vehicular ad hoc networks [J]. IEEE Transactions on Mobile Computing, 2017, 16(8): 2132-2146.

[3] MISHRA B, MNAYAK P, BEHERA S, et al. Security in vehicular ad hoc networks: a survey [C]//Proceedings of 2011 International Conference on Communication, Computing and Security. New York, USA: ACM Press, 2011: 59-74.

[4] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1984: 47-53.

[5] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps [C]//Proceedings of the 22th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2003: 416-432.

[6] CHEON J H, KIM Y, YOON H J. A new ID-based signature with batch verification [J]. Trends in Mathematics Information Center for Mathematical Sciences, 2005, 8(1): 119-131.

[7] XU Jing, ZHANG Zhenfeng, FENG Dengguo. ID-based aggregate signatures from bilinear pairings [C]//Proceedings of CANS'05. Berlin, Germany: Springer, 2005: 110-119.

[8] HERRANZ J. Deterministic identity-based signatures for partial aggregation [J]. The Computer Journal, 2006, 3(3): 322-330.

[9] SHIM K A. An ID-based aggregate signature scheme with constant pairing computations [J]. The Journal of Systems and Software, 2010, 83(10): 1873-1880.

[10] DU Hongzhen, WEN Qiaoyan. An efficient identity-based aggregate signature scheme [J]. Journal of Sichuan University (Engineering Science Edition), 2011, 43(1): 87-90. (in Chinese)

杜红珍, 温巧燕. 一个高效的基于身份的聚合签名方案 [J]. 四川大学学报 (工程科学版), 2011, 43(1): 87-90.

[11] YU Yike, ZHENG Xuefeng, SUN Hua. An identity based aggregate signature from pairings [J]. Journal of Networks, 2011, 6(4): 631-637.

[12] DU Hongzhen. An efficient and secure aggregate signature scheme for vehicular ad hoc network [J]. Henan Science, 2016, 34(4): 481-485. (in Chinese)

杜红珍. 一个适用于车载自组织网络的安全高效的聚合签名方案 [J]. 河南科学, 2016, 34(4): 481-485.

[13] WANG Z. An identity-based data aggregation protocol for the smart grid [J]. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2428-2435.

[14] CHENG Ling, WEN Qiaoyan, JIN Zhengping, et al. Cryptanalysis and improvement of a certificateless aggregate signature scheme [J]. Information Sciences, 2015, 295: 337-346.

[15] YANG Xiaodong, LI Yutong, CHEN Chunlin, et al. A short certificateless aggregate signature against coalition attacks [J]. PloS One, 2018, 13(12): 1-18.

(上接第 174 页)

- [16] WANG Daxing, TENG Jikai. Probably secure certificateless aggregate signature algorithm for vehicular ad hoc network[J]. Journal of Electronics and Information Technology, 2018, 40(1): 11-17. (in Chinese)  
王大星, 滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报, 2018, 40(1): 11-17.
- [17] ZUO Liming, CHEN Lanlan, ZHOU Qing. A certificate-based short signature scheme[J]. Journal of Shandong University (Natural Science), 2019, 54(1): 79-87. (in Chinese)  
左黎明, 陈兰兰, 周庆. 一种基于证书的短签名方案[J]. 山东大学学报(理学版), 2019, 54(1): 79-87.
- [18] XU Jinfang, GAO Dezhi, LIU Shudong. Efficient

signature scheme for specified verifier[J]. Application Research of Computers, 2011, 28(1): 298-303. (in Chinese)

许金芳, 高德智, 刘树栋. 高效的具有指定验证者的签名方案[J]. 计算机应用研究, 2011, 28(1): 298-303.

- [19] YANG Lu. Certificateless implicit authentication and key agreement protocol without pairing operation [J]. Computer Engineering, 2012, 38(2): 138-140. (in Chinese)

杨路. 无对运算的无证书隐式认证及密钥协商协议[J]. 计算机工程, 2012, 38(2): 138-140.

编辑 陆燕菲